# TechRadar™: Zero Trust Network Threat Mitigation Technologies, Q4 2016

**Road Map: The Security Architecture And Operations Playbook**

by John Kindervag, Jeff Pollard, Joseph Blankenship, and Alexander Spiliotes

October 28, 2016

## Why Read This Report

This TechRadar™, the road map document of the security architecture and operations playbook, defines the use cases, business value, and outlook for the 20 technologies that comprise the most important network threat mitigation technologies. This includes core technologies such as next-generation firewalls and automated malware analysis solutions, but it also includes emerging and growth technologies such as breach simulation and security analytics.

## Key Takeaways

**The Network Is Still A Powerful Enforcement Point**

With the adoption of cloud and mobile technologies, today's corporate perimeter is no longer confined to the four walls of the organization. Deperimeterization does not negate the importance of network security; in fact, the network is more important than ever. It's the only layer in the organization that sees and knows all.

**Alert Volume And Skill Shortages Drive The Need For Advanced Analytics And Automation**

Alert volumes are increasing every year, and adding technologies exacerbates the problem. To become more customer-led, security leaders need to dig their teams out from under the alert deluge, and this necessitates sophisticated analytics and mature workflows executed via automation.

**Breach Avoidance Is Less Expensive Than Breach Response**

The complexities of breaches require firms to suddenly shell out cash for litigation, investigation, notifications, public relations, and fines. The total costs are frighteningly large, and they linger long after the publicity is over. This TechRadar will provide an overview of the technologies available to stop breaches before they happen, and to respond rapidly to attempted attacks.

# TechRadar™: Zero Trust Network Threat Mitigation Technologies, Q4 2016

**Road Map: The Security Architecture And Operations Playbook**

by John Kindervag, Jeff Pollard, Joseph Blankenship, and Alexander Spiliotes
with Stephanie Balaouras, Heidi Shey, Andras Cser, Bill Barringham, and Peggy Dostie

October 28, 2016

## Table Of Contents



## Notes & Resources

Forrester interviewed 48 vendor companies and drew on end user inquiries and research for this report.

## Related Research Documents

The Forrester Wave™: Automated Malware Analysis, Q2 2016

No More Chewy Centers: The Zero Trust Model Of Information Security

Vendor Landscape: Security User Behavior Analytics (SUBA)

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

## Today's Threats Demonstrate The Need For Network Threat Mitigation

The frequency and diversity of major breaches has not abated since our last TechRadar on network threat mitigation technologies. In that time, we've seen hacks that have upended private online communities in the case of Ashley Madison; continued targeting of health insurance organizations, like Anthem and Premera BlueCross BlueShield; and breaches of government and electoral institutions likely perpetrated by nation-state actors as occurred at the US Office of Personnel Management (OPM) and Democratic National Committee (DNC).[1] In addition, the ongoing release of DNC documents by WikiLeaks underscores how a compromised network leads to continuous reputational and operational damage.[2]

### Today's Security Leaders Are Rethinking Network Security Strategy

To combat the increasing sophistication of cybercriminals, hacktivists, and state-sponsored agents, security leaders find themselves on a never-ending quest to maintain the integrity of their networks and to protect their firm's most sensitive data.[3] However, the rapid adoption of cloud and mobile technologies, coupled with new customer engagement and business models, has extended today's network well beyond the concrete walls of the corporation itself. Throwing more security controls at the challenge in a haphazard manner is not the answer; security leaders need to take a step back and take a strategic view. Specifically, we see that:

- **There is a movement to redesign network security.** Vendors didn't design existing enterprise security controls to thwart the types of threats common today. Current attacks are multistage, multi-OS, and multi-application, and enterprise security teams struggle to adapt to morphing attack patterns. Forrester has been working to help define new trust models and security architectures through our Zero Trust (ZT) initiative. A ZT network abolishes the idea of a trusted network inside the corporate perimeter. The entire network is untrusted. Instead, security teams create microperimeters of granular control around an enterprise's sensitive data assets that also provides visibility into how the firm uses this data across its entire business ecosystem.[4]
- **Security teams are seeking to adopt proactive and integrated security.** The advent of next-generation firewall (NGFW) technologies has revolutionized network security by consolidating functions of several security solutions in one multipurpose security appliance. The question for many organizations today is not should they replace their IDS with IPS, but how quickly can they upgrade their gateways to be more proactive and provide more control of applications and users. NGFWs are also critical because they are one way of delivering on the network segmentation and microperimeterization requirements of ZT.
- **Security teams need visibility and analytics.** Many companies are blind to their overall security posture in anything close to a real-time basis. In fact, some consider this "blindness" part of their risk management plan. They avoid discovering the soft spots in their security to avoid expending the money and effort to mitigate them. Forrester advocates the adoption of security analytics (SA) tools to achieve situational awareness across the enterprise — even across hosting models.[5] SA

solutions integrate the traditional log management capabilities of security information management (SIM), with network analysis and visibility (NAV), external threat intelligence, and other security solutions to create real-time security dashboards, and with them, the modern enterprise can have more insight into its real-time security posture.

- **Combatting modern threats requires an integrated arsenal.** A multifaceted approach that blends next-generation firewall, automated malware analysis, NAV, and security analytics is necessary to actively defend modern networks. API-to-API interconnectivity allows these tools to work together. Mature workflows can sit on top of each component and allow the early stages of automation to occur after manual portions of the investigative or containment process is executed with approval by a SOC analyst.
- **Security teams can't ignore the old challenges left unsolved.** Security challenges still remain in areas such as identity and access management, email security, and browser security. We factor those into each mitigation technology category and consider them through the lens of Zero Trust.

## Why The Future Of Zero Trust Network Threat Mitigation Matters

The aftermath of a data breach can be devastating. There are significant costs associated with breach response (discovery, containment, eradication, and recovery), customer notification, lost employee productivity, regulatory fines, and opportunity costs. In addition, enterprises that have suffered a high-profile breach can expect to pay for restitution, additional security and audit requirements, and other liabilities.[6] Security costs and breach fines will only continue to rise. Customers and government bodies are holding organizations accountable for their data breaches and will make companies pay if they are inadequately protected.[7] An enterprise that's the victim of a data breach may be crippled by the seemingly uncapped price tag of cybercrime. The wise enterprise is, therefore, looking to stop breaches before they happen, or at least minimize the impact. This TechRadar is designed to help provide an overview of the numerous technologies available to achieve this laudable goal.

## Overview: TechRadar For Zero Trust Network Threat Mitigation

To help security leaders plan their next decade of investments in network threat mitigation, Forrester investigated the current state of 20 commonly deployed or emerging technologies. We used insight gathered from Forrester client inquiries and industry expert interviews, and combined this with product data to assess four things: 1) the current state of the technology; 2) the technology's potential impact on customers' business; 3) the time experts think the technology will need to reach the next stage of maturity; and 4) the technology's overall trajectory — from minimal success to significant success.[8]

## Why Do These 20 Technologies Appear In The TechRadar?

Forrester believes that it's important to proactively protect against threats, to increase efficiencies, reduce costs, and provide the level of security necessary in today's corporate networks. However, there's a nearly endless number of mitigation technologies that security teams have acquired over the years to combat these threats. To help wade through the landscape, Forrester has culled the list to 20 technologies, which are highlighted in this TechRadar. All are used within an enterprise's extended network to mitigate threats against data and applications. In selecting the technologies to evaluate in this study, Forrester focused on technologies that are:

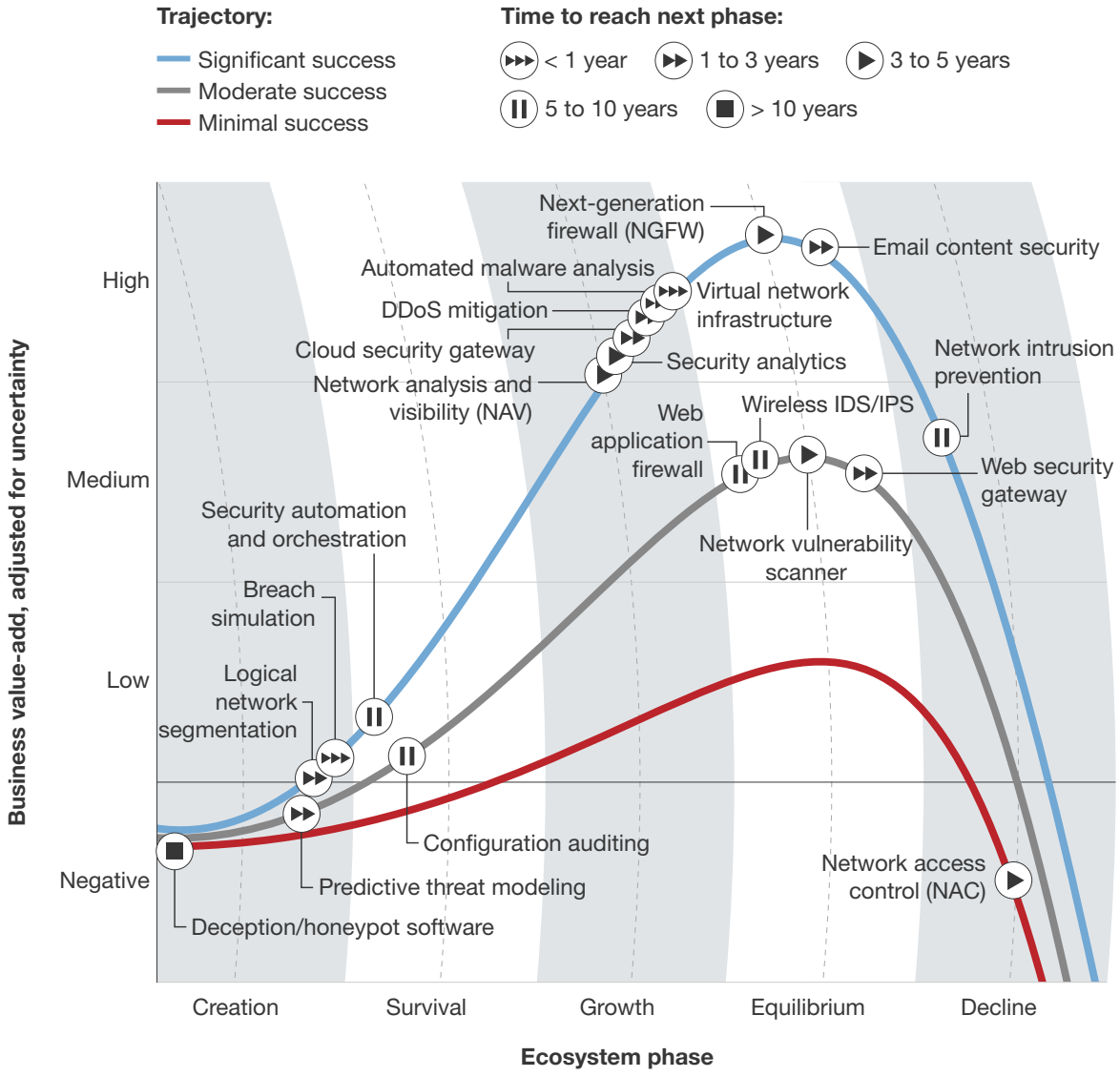
- **Commonly deployed in modern networks to protect against network security threats.** With each new vulnerability, exploit, or attack, security professionals are forced to mitigate the threat by using existing controls whenever possible. As attack vectors expand, however, it becomes clear that attackers have learned how to bypass existing network security controls, forcing security teams to implement new controls that meet the changing threat landscape. Ultimately, there's a large number of controls typically deployed in most enterprise networks, and for this TechRadar, Forrester is focusing on the widely deployed controls.
- **Broad in scope for securing the extended network.** Threat mitigation tools are critical in protecting and securing end-to-end infrastructure and operations. Many of these technologies either sit inline or out of band to the existing network design. However, many of these technologies have a broader scope than just scanning the network; they also help in heuristic and behavioral analysis, modeling threats, and comprehensive reporting that help manage security loopholes. As most modern networks are extending to the cloud, the network perimeter has all but disappeared, requiring new approaches to securing data wherever it resides.
- **Critical to meet compliance requirements.** Many of these technologies were adopted to meet certain compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS). There are various mandates that require organizations to implement security controls to demonstrate that information is protected. These technologies help organizations not only protect data but also report and mitigate anomalies that may exist in the line of communication.
- **Emerging and designed to meet new security criteria.** Research continues in the area of network security, and innovative new vendors have created new and emerging technologies that must be looked at to determine their value in enterprise network security.

## Varied Uses To Secure The Extended Network

Since we last published our TechRadar on network threat mitigation technologies, we found that (see Figure 1):

- **Emerging network security technologies are gaining market traction.** The adoption of security analytics, NAV, and malware analysis tools is continuing to grow as measures to combat APTs and state-sponsored attacks, and anti-DDoS services are proving very useful against disruptive hacktivist attacks. The benefits of cloud services are extremely compelling for organizations, which have in turn prompted increased interest in cloud security gateways to help push cloud initiatives along. The promise of software-defined networking (SDN) and network functions virtualization (NFV) has made virtual network infrastructure (VNI) a very attractive technology segment.[9]
- **Compliance still continues to drive security spending and controls adoption.** The payment card industry data security standard (PCI DSS) continues to be a major driver in network security purchasing, but other compliance initiatives such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) are also powerful purchasing incentives.[10] Multinational companies must plan and implement during the transition period before the European Union's General Data Protection Regulation requirements take effect in May 2018. There's a concerted effort among vendors to position their products in the compliance area.
- **The network is still a powerful enforcement point.** Protecting the network will always be important. Since the network provides transport and access for critical data resources, attackers will continue to target the network to gain access to data that they can then monetize. Therefore, security pros must robustly protect the network. Threat mitigation technologies, such as encryption, firewalls, threat modeling, intrusion prevention, and vulnerability scanners, protect the network, data, and numerous cloud instances that make up current enterprise architectures.

**FIGURE 1** TechRadar™: Zero Trust Network Threat Mitigation Technologies, Q4 '16




## Creation: Risk Management Drives Threat Modeling

Technology in the Creation phase is still finding its footing in the market. We put four technologies in the Creation phase:

› **Breach simulation (see Figure 2).** This new technology is similar to predictive threat modelling, which looks at ways in which an attacker might get inside your network. Breach simulation tools take the opposite approach to try to discover how cybercriminals or malicious insiders might

exfiltrate your toxic data so that it can be monetized or maliciously used. Knowing this information will help security pros prioritize security projects to more proactively protect against data breach vectors. Companies pioneering this space include AttackIQ, Damballa (Core Security), SafeBreach, Stratum Security, and vThreat.

- **Deception/honeypot software (see Figure 3).** Deception technologies help solve the problem of understanding what normal looks like in complex distributed enterprise environments. These technologies mimic real systems and applications to lure an attacker into attempting access. Since they perform no real functions in the environment and don't have direct user input, any attempt to interact with them, by definition, is abnormal. This allows teams to prioritize any events from a deception technology ahead of others. Attackers, not users, are the primary reason why the machine would see any activity leading to a signal-to-noise ratio that acts in favor of security teams. Vendors in this space include Acalvio, Attivo, Illusive Networks, and TrapX.
- **Logical network segmentation (see Figure 4).** These solutions provide ZT network segmentation in software instead of hardware. They often leverage encryption to provide secure segmentation services. By segmenting user traffic away from the rest of the network, they significantly reduce the risk of cybersecurity events from business partners, remote workers, and third-party access. They're also helpful in extending ZT concepts into the cloud and in support of a mobile workforce by providing per-application access for BYOD and other unmanaged device scenarios. There are multiple initial use cases for these technologies. Expect VPN replacement to be an initial use case. Other initial uses cases include providing secure guest or business partner access. Emerging vendors in this space include Akamai (Soha), Blue Cedar Networks (mobile), CDNetworks, Certes Networks, Cryptzone, Dome9, Safe T, Unisys Stealth, Zentera, and Zscaler.
- **Predictive threat modeling (see Figure 5).** Previously called "network threat modeling," this technology models the attack surface of more than just the network. As organizations consolidate data, it will be important to know how cybercriminals can attack that data. Predictive threat modeling technologies allow a type of artificial intelligence to be overlaid on traditional information security strategies. By analyzing vulnerability, device, and network configuration data, it's possible to determine the most likely attack path inside with a computer model that proactively protects against those attacks. The adoption of this technology is important so that security organizations can deliver more-precise risk data. This technology may become part of other tools in the future, such as GRC solutions, security analytics solutions, and vulnerability management tools. RedSeal and Skybox Security are the creators of this space.

**FIGURE 2** TechRadar™: Creation Phase, Breach Simulation, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Breach simulation technologies deploy threat actor tradecraft with automated workflows to assess an environment. The simulation results allow the security team to determine the impact of a potential breach by using actual behaviors based on threat intelligence and incident response. By combining elements of penetration testing, vulnerability assessments, and threat intelligence, a more realistic attack-oriented offering is created that prioritizes attacker results over compliance and patch management. |
| Usage scenarios | | Security practitioners should consider introducing breach simulation technologies to augment existing vulnerability management programs. Breach simulation will provide specific details on the methodology of attackers and the totality of an incident for the security team including the systems, accounts, and data that would be accessed through a successful attack. Example scenarios tested for include: 1) exfiltration of data; 2) privilege escalation; 3) command and control (C&C); and 4) lateral movement, or simulated attacks can mimic nation-state tradecraft or specific breaches such as Target. |
| Vendors | | AttackIQ, Damballa, SafeBreach, Stratum Security, vThreat |
| Estimated cost to implement | | Varies: Pricing is a combination of users, scenarios, and delivery model through a cloud or appliance-based on-premises model. |
| Ecosystem phase | Creation | Breach simulation is a brand new entrant vying for security budget. It seeks to directly apply the lessons and tradecraft learned through threat intelligence and incident response and use that data to assess infrastructure for susceptibility of attack. Vulnerability management's problem expressing the likelihood of an attack, the potential for exploitation of a vulnerability, and the ramifications of an exploit leave a gap that breach simulation can fill. |
| Business value-add, adjusted for uncertainty | Low | Breach simulation is hyper-relevant to security practitioners including incident responders, security operations teams, and threat intelligence-focused personnel. The challenge for those resources will be in taking the data gained via breach simulation and explaining the impact of the findings, along with plans for remediation, to business personnel that are not focused on methodologies and processes. |
| Time to reach next phase | < 1 year | Breach simulation will continue to mature, and we expect it to reach the next phase within a year. |
| Trajectory (known or prospective) | Significant success | As an augmentative measure to a staple of the enterprise security program mainstay, breach simulation has a compelling route to success through expanding existing information gained from vulnerability management. |

**FIGURE 3** TechRadar™: Creation Phase, Deception/Honeypot Software, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Deception technologies mimic a real system and hope to lure an attacker into an intrusion. Since the machine doesn't have a real user or serve a real application, any interaction that occurs is, by definition, anomalous. Additional capabilities can exist, including automated malware analysis and session captures, to better inform the security team of what the attacker attempted during the exploit attempts. |
| Usage scenarios | | Security teams challenged to understand normal behavior patterns in their network can opt to use deception technologies to find abnormal behaviors since any interaction with the deception technology is, by definition, abnormal. It also details the tools and techniques the attacker used when interacting directly with the system. |
| Vendors | | Alcalvio, Attivo, Illusive Networks, Shape Security, TopSpin Security, Trapx |
| Estimated cost to implement | | Varies: Pricing is based on number of operating system types, application types, appliances, or virtual machines used to increase the likelihood of deceiving attackers. Additional capabilities can be added including dynamic malware analysis, which increases costs. |
| Ecosystem phase | Creation | Honeypots aren't new. They have been prevalent in academia and security research for a decade. However, today's deception solutions act as a signaling mechanism that collects the details of threat actor tradecraft, and these enhancements, which are now a part of commercial offerings, are new. Vendors are currently iterating on the right elements of user interface, operating systems available for emulation, and complementary feature sets that should be included to maximize value. |
| Business value-add, adjusted for uncertainty | Negative | The primary benefits of these tools as a warning system for threat presence, along with collection of potential threat actor behaviors, help security personnel monitoring the environment for intrusion or presence of an attacker, but that information isn't relevant to the rest of the organization. |
| Time to reach next phase | > 10 years | These technologies face a challenging competitive landscape, with malware analysis, security analytics, threat intelligence, and network analysis and visibility solutions all attempting to fulfill similar capabilities for security buyers. It will take substantial time and maturity for the vendors and customers considering this technology to determine if it is a foundational product or a possible feature of a more holistic technology set. |
| Trajectory (known or prospective) | Minimal success | Forrester believes this technology makes sense as part of a team's threat detection portfolio. However, today's solutions address only one portion of the attack cycle, whereas security teams are challenged by the entirety of an attack, not just a single stage or portion. Longer term, this should become a feature of advanced threat detection, not a product category existing as a standalone purchase. |

**FIGURE 4** TechRadar™: Creation Phase, Logical Network Segmentation, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Logical network segmentation solutions segment networks into secure enclaves or microperimeters with granular data protection capabilities as recommend by Forrester's Zero Trust model. Segmentation can be achieved using a variety of technologies, including next- generation firewalls or via software-defined networking (SDN). These technologies may leverage encryption to provide secure segmentation services. |
| Usage scenarios | | There are multiple initial use cases for these technologies. Expect VPN replacement to be an initial use case. These tools may also be helpful in providing per-application access for BYOD and other unmanaged scenarios. They may also be helpful in providing secure guest or business partner access. This technology will be very helpful in extending Zero Trust beyond the data center. This is often done on a per-app basis so that a single user is connecting to a single application via an encrypted channel. This effectively logically segments the user traffic away from the rest of the network and may significantly reduce the risk of cybersecurity events from business partners, remote workers, and third-party access. |
| Vendors | | Akamai (Soha), Blue Cedar Networks (mobile), CDNetworks, Certes, Cryptzone, Dome9, Mocana (mobile), Safe-T, Unisys, vArmour, Zentera, Zscaler |
| Estimated cost to implement | | Varies: This is a startup market that has not yet stabilized, but it will probably be priced on a per-user basis. |
| Ecosystem phase | Creation | Venture capitalists have just now begun to invest in this type of technology, and there are only a small number of early adopters who are using these tools for specific use cases. |
| Business value-add, adjusted for uncertainty | Low | These technologies may signal a new trend in network access and segmentation, but there are not enough large scale deployments yet to have enough data to judge the overall efficacy of the solutions. |
| Time to reach next phase | 1 to 3 years | If these tools prove effective, easy to deploy and use, and cost efficient, then there could be compelling reasons for organizations to adopt this technology very quickly. If the tech proves successful, expect the space to explode. |
| Trajectory (known or prospective) | Significant success | Given the overarching trends toward mobile and BYO-anything usage scenarios, coupled with the shift to more cloud services and a greater number of third-party partnerships, logical network segmentation tools should prove to be a significant success. |

**FIGURE 5** TechRadar™: Creation Phase, Predictive Threat Modeling, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Predictive threat modeling is a methodology that analyzes the architecture and design of an application to find potential design flaws that have security consequences. It can also help in firewall auditing. |
| Usage scenarios | | Predictive threat modeling allows organizations to take a very high-level and strategic view of their network security architectures, configurations, and policy. By analyzing network data and modeling threat vectors and attack scenarios, security and risk professionals can more accurately determine where to place controls and how to define policy and configure devices. |
| Vendors | | Cigital, Coverity, Microsoft, RedSeal, Skybox Security |
| Estimated cost to implement | | Highly variable: It depends on the number of devices and the type of threat modeling to be done. |
| Ecosystem phase | Creation | Predictive threat modeling is a concept that can be used to enhance software and network security. The evolution away from purely perimeter-centric security controls means that threat modeling tools may become more necessary to determine how to properly protect important data. These tools will also need to evolve and become more user-friendly and cost-effective if this market is to survive and grow. |
| Business value-add, adjusted for uncertainty | Negative | This market is at the Creation phase and will take some time before it can provide value. However, it can be useful in auditing capabilities by P modeling threats and can provide control for various compliance requirements. |
| Time to reach next phase | 1 to 3 years | Much of the intellectual property created from early threat modeling tools is being leveraged in other ancillary spaces, such as firewall auditing products. The offshoots of threat modeling will have enhanced growth, as they are more targeted to specific problems. The costs and complexity of current threat modeling tools work as a barrier to adoption of this new technology. |
| Trajectory (known or prospective) | Moderate success | Predictive threat modeling could become moderately or even significantly successful if it can reduce risks by providing insight that can be used to more efficiently design and manage security infrastructures. |

## Survival: Compliance Drives Configuration Auditing, While VNI Holds Promise

Configuration auditing technology has been around for some time but has had varying degrees of success. Its adoption has been fueled primarily by compliance, whereas VNI shows promise to reach the next stage. The Survival technologies are:

- **Configuration auditing (see Figure 6).** Configuration auditing technology automates network device configuration tasks, such as finding unused rules and objects, and optimizing the rule base to increase device performance. Auditing tools are important in a dynamic network environment because security pros continually add new rules to support business processes. Network device configurations are generally filled with old and unnecessary rules that only impede device performance and provide attackers with potential avenues for attack. Because network configuration errors lead to data breaches and network downtime, Forrester advises our customers to adopt these technologies where possible in order to automate their processes. Solutions for heterogeneous networks include AlgoSec, FireMon, and Tufin.
- **Security automation and orchestration (see Figure 7).** The security talent shortage and the volume of incidents have overcome historical reluctance to automate security functions. Early use cases for automation and orchestration solutions are incident investigation and response. Most solutions use playbooks containing a series of automated actions that human analysts normally take in different scenarios. Analysts without much technical ability can deploy prepackaged playbooks, but creating customized playbooks may require some programming skill. As detection solutions continue to improve, analysts will still need to conduct investigations and decide remediation actions. We expect that future automation solutions will take automated remediation steps independent of human analysts. Notable vendors include Demisto, FireEye (Invotas), IBM (Resilient Systems), Phantom, RiskSense, and Swimlane.

**FIGURE 6** TechRadar™: Survival Phase, Configuration Auditing, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Also known as firewall auditing tools, configuration auditing tools automate the process of reviewing firewall, router, and other device/system rule sets. These tools gather configuration and log information from firewalls and, using sophisticated algorithms, look for insecure, unused, conflicting, or redundant rules in the firewall configuration. This tool can then be used to modify the configuration so that the firewall rule sets are more secure and efficient. |
| Usage scenarios | | Auditing tools are important in firewall rule creep. There is often a formalized process for adding new firewall rules, but rarely is there a formal process for removing rules that are no longer needed. Additionally, the Payment Card Industry Data Security Standard (PCI DSS) requires maintenance of firewall configurations and reviews at least every six months. |
| Vendors | | AlgoSec, Check Point, FireMon, Proofpoint (NetCitadel), Skybox Security, SolarWinds, Tufin, VMware (Arkin) |
| Estimated cost to implement | | These tools are generally licensed on a per-firewall basis. The cost per firewall is low, so in environments with many firewalls the total investment could be large. However, even in a large enterprise with numerous firewalls, the total cost will typically be much smaller than for other security controls. Given both the short-term and long-term benefits from locking down firewall and router configurations, the value of these tools in reducing business risk is notable. |
| Ecosystem phase | Survival | Configuration auditing tools are in the Survival phase. The overall size of the market remains small. |
| Business value-add, adjusted for uncertainty | Low | The business value is considered low, because although there is positive security impact and the overall costs are low compared with other security controls, the targeted nature of these tools limits their value to a single aspect of security instead of affecting the entire security program. Forrester believes that these tools provide tangible value that may drive growth of this space longer term. However, not all organizations see this tool as a necessity. |
| Time to reach next phase | 5 to 10 years | Given the increasing number of data breaches, the current regulatory environment, and the fact that firewalls and routers are misconfigured in most networks that have been compromised, Forrester anticipates that both regulatory compliance and the changed threat landscape will drive the configuration auditing space to the next level within the next five to 10 years. |
| Trajectory (known or prospective) | Moderate success | Configuration auditing tools have the potential to become common in enterprise security organizations. Security managers have already discovered that meeting compliance mandates, such as PCI, are too burdensome to do manually, and in today's changed threat environment, network configuration errors lead to breaches. |

**FIGURE 7** TechRadar™: Survival Phase, Security Automation And Orchestration, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Security automation and orchestration solutions provide agile network programmability powered by centralized management. This allows security operations teams to enable security workflows and decisions to be automated, making security operations more efficient and using security resources more effectively. Automation may start with simple repetitive tasks but will evolve to include autonomous response and orchestration as necessary for the real-time detection of and response to threats that characterize a Zero Trust network. |
| Usage scenarios | | Security is one of the last parts of the enterprise to employ automation. Many processes in the security operations center (SOC) remain dependent on repetitive manual tasks. Employing security automation and orchestration solutions promises to increase efficiency and allow analysts to focus on higher-value activities. The well-documented shortage of trained, experienced security professionals is pushing S&R teams to find ways to increase their effectiveness without adding additional staff. |
| Vendors | | Ayehu Software, CyberSponse, FireEye (Invotas), Hexadite, Hexis Cyber Solutions, IBM (Resilient Systems), Phantom, Proofpoint, Swimlane |
| Estimated cost to implement | | Low. Solutions don't require a complex technical implementation but must work with existing technologies and processes. Security pros may find that their rules of engagement and processes need revamping in order to take full advantage of automation tools. Programming skills may be necessary to create custom playbooks for some solutions, but most provide prebuilt templates. |
| Ecosystem phase | Survival | Security pros remain reluctant to automate security functions due to previous poor experiences with automated blocking technologies and the belief that human analysts must be involved in every stage of a security investigation. Few players currently focus on security automation and orchestration, and there are signs that the functionality will be included as part of security platforms as larger vendors acquire smaller vendors. |
| Business value-add, adjusted for uncertainty | Low | Current solutions provide automated playbooks for repetitive functions, which does provide some efficiency gains. As the technology matures and security pros gain confidence in the technology to automate response as well as investigative tasks, enterprise value will increase significantly. |
| Time to reach next phase | 5 to 10 years | It will take time for solutions to advance significantly enough that security pros will trust them to automate remediation activities and for the technology to become an integral part of security operations. |
| Trajectory (known or prospective) | Significant success | As solutions improve and become part of operations, they will have a significant impact, improving response times and easing the strain on security teams. |

## Growth: Advanced Threats Call For A New Breed Of Tools

Attacks have become more sophisticated, and new controls have evolved to meet their growing threats. Additionally, compliance has forced the adoption of technology that peers deeply into the packet and has the ability to block attacks before they can damage critical resources. Technologies in the Growth phase are:

- **Automated malware analysis (see Figure 8).** Malware analysis tools analyze malware in virtual sandboxed environments, looking for signs of malicious code. They're designed to improve the catch rate of zero-day attacks. Some platforms combine malware analysis with technologies that also look for command and control (C&C) activity of botnets and related attacks. This technology may move from a standalone product to a feature embedded into other security gateways or antimalware controls. Look for increased merger and acquisition activity in this space. Blue Coat Systems, Check Point Software Technologies, Cisco (FireAmp and ThreatGrid), FireEye, Lastline, and Palo Alto Networks are players in this space.
- **Cloud security gateway (see Figure 9).** Both business leaders and CIOs are eager to adopt various types of cloud services for flexibility and speed. However, security, privacy, and other third-party risk concerns have sometimes dampened adoption appetite.[11] Cloud security gateways (CSGs) provide enterprises with the ability to control traffic and data to a cloud service and report the usage to auditors and other stakeholders to ensure proper security controls are in place and enforced. CSG capabilities can range from DLP and monitoring to encryption and tokenization to anomalous behavior detection. We first covered cloud encryption gateways in our TechRadar on data security and have since seen massive growth and interest in additional cloud security functions.[12] As firms look to adopt more cloud services, expect CSGs to see continued success in enabling better visibility and policy in cloud environments. Interesting vendors in this space include Bitglass, CipherCloud, Cisco Systems (CloudLock), Imperva (Skyfence), Microsoft (Adallom), Netskope, Oracle (Palerra), Skyhigh Networks, Symantec (Blue Coat Systems, Elastica, Perspecsys), and Vaultive.
- **DDoS mitigation controls (see Figure 10).** Cybercriminals and hacktivists use DDoS attacks as a protest and cyberterrorist tool, which is increasing the need for DDoS mitigation services. DDoS mitigation solutions reduce the impact of attacks as well as ensure the availability of critical services and applications. While not every enterprise views hacktivist-based DDoS attacks as a huge risk, in the event that an attack occurs, the business impact could be immense, especially for companies that rely significantly on the revenue from eCommerce. These solutions can also include the capability to mitigate application-level DoS attacks. Arbor Networks and Radware provide anti-DDoS hardware, and there is anti-DDoS capability in most network IPS and NGFW products, but they don't protect upstream. Look for an increased adoption of DDoS-as-a-service from companies such as Akamai Technologies, Imperva (Incapsula), Neustar, and Verizon.

- **Network analysis and visibility (NAV) (see Figure 11).** NAV tools will help the entire network function like a fighter pilot on alert, constantly scanning the network for malicious activity, behaviors, and potential attacks to provide situational awareness. These tools include: 1) network discovery tools for finding and tracking assets; 2) data flow analysis tools to analyze traffic patterns and user behaviors; 3) packet capture and analysis tools that function like a network DVR; 4) network metadata analysis; and 5) network forensics tools that assist incident response and criminal investigation. Blue Coat Systems; Lancope (Cisco); Narus; Niksun; and RSA, the security division of EMC, are among the varied players in this space.
- **Security analytics (see Figure 12).** SA solutions combine the correlating and reporting functions of SIM together with information feeds from DLP, NAV, endpoint, IAM, external threat, and even fraud solutions. SA gives security pros context and situational awareness about threats to sensitive data and provide a higher level of visibility to behavior inside the network, giving security pros additional context for decision-making and investigations. Traditional SIM vendors are adding SA features to their products, and standalone vendors are building compelling offerings that can function with or without a SIM. Notable vendors in this space include BAE Systems, Bay Dynamics, E8 Security, Rapid7, and Securonix, in addition to traditional SIM vendors like IBM (QRadar); LogRhythm; and RSA, the security division of EMC, among others.
- **Virtual network infrastructure (see Figure 13).** Current networking infrastructures are too rigid and old to support the orchestration of services needed to optimize a user's experience or adapt to the changing threat environment. VNI encompasses multiple technologies, including network functions virtualization (NFV) and software-defined networking (SDN).[13] VNI architecture and associated technologies are important to the continued adoption of Zero Trust networking, as the virtual networks themselves help by segmenting traffic easily and the use of virtual firewalls enforce ZT policy.[14] Vendors in this space include Big Switch Networks, Embrane, and VMware, as well as traditional networking companies such as Cisco Systems and Juniper Networks.

**FIGURE 8** TechRadar™: Growth Phase, Automated Malware Analysis, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Automated malware analysis tools analyze malware in virtual sandboxed environments, looking for signs of malicious code. |
| Usage scenarios | | Malware analysis tools are designed to improve the catch rate of targeted attacks. Some platforms combine malware analysis with technologies that also look for command and control (C&C) activity of botnets and related attacks. |
| Vendors | | Check Point, Cisco Systems, Cyphort, Damballa, Fidelis Cybersecurity, FireEye, Forcepoint, Fortinet, Intel Security (McAfee), Lastline, Palo Alto Networks, Symantec (Blue Coat Systems), Trend Micro, Zscaler |
| Estimated cost to implement | | Pricing varies, but generally it is based on the size of the appliance necessary to support the traffic it analyzes. Prices can range from $25,000 to several hundred thousand dollars. |
| Ecosystem phase | Growth | This technology may move from a standalone product to a feature embedded into other security gateways or antimalware controls. Look for increased merger and acquisition activity in this space. |
| Business value-add, adjusted for uncertainty | High | Malware analysis tools are valuable, but as the market continues to be saturated with vendors offering malware analysis capabilities, integration into other technologies is key for these tools to deliver value. |
| Time to reach next phase | < 1 year | The advent of targeted attacks requires more than signature-based protection, which is driving the adoption of malware analysis tools. Forrester believes that the market for malware analysis will reach the next level in less than one year. |
| Trajectory (known or prospective) | Significant success | Malware analysis tools provide valuable information that can be used for incident response and threat intelligence. As solutions make it easier and faster to conduct such analysis without the need for specialized staff or resources to maintain, the adoption of such tools is expected to rise. |

**FIGURE 9** TechRadar™: Growth Phase, Cloud Security Gateway, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Cloud security gateways provide security teams with visibility into how data moves to and from cloud services. Additionally, they offer the ability to enforce policy regarding cloud usage by proxying the traffic so that policy such as access control rules or encryption can be applied to the traffic or the data. |
| Usage scenarios | | The use of cloud security gateways gives security teams the ability to control traffic and data to a cloud service and then report on that usage so that auditors and other stakeholders can be confident that proper security controls are in place and enforced. Cloud security gateway capabilities can range from DLP and monitoring to encryption and tokenization to anomalous behavior detection. |
| Vendors | | Bitglass, CipherCloud, Cisco Systems (CloudLock), FireLayers, IBM, Imperva (SkyFence), Microsoft (Adallom), Netskope, Oracle (Palerra), Perspecsys, Skyhigh Networks, Symantec (Blue Coat Systems/Perspecsys), Vaultive |
| Estimated cost to implement | | Varies: Cloud security gateway vendors tend to price based on a per-user subscription and per service being protected. Average deal sizes are around $250,000 to $300,000. |
| Ecosystem phase | Growth | Business executives and the CIO charge S&R pros with protecting the firm's sensitive data — no matter if it's stored on-premises or in the cloud. To protect data in the cloud, security pros have had to invest in a variety of solutions: solutions that discover cloud usage, solutions that encrypt data, solutions that provide insight into user behavior and access, and so on. Many cloud security gateways combine these key capabilities into a single offering. |
| Business value-add, adjusted for uncertainty | High | Cloud services have many proven benefits for businesses, such as reduced operational and investment costs and increased business agility. However, handing over data to another provider to manage can be a difficult decision when considering security and privacy. Cloud security gateways can help enable organizations to embrace cloud deployments through increased control over their data and reduction of risk. |
| Time to reach next phase | 1 to 3 years | Forrester believes the time to reach the next phase for cloud security gateways is one to three years. |
| Trajectory (known or prospective) | Significant success | Forrester sees significant success for this market as the use of cloud services increases and the capabilities for these solutions continue to advance. |

**FIGURE 10** TechRadar™: Growth Phase, DDoS Mitigation, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Distributed denial of service (DDoS) mitigation solutions reduce the impact from DDoS attacks, ensuring availability of critical services and applications. These solutions can also mitigate application-level DoS attacks. |
| Usage scenarios | | Hacktivists use DDoS attacks as a protest and cyberterrorist tool, which is increasing the need for DDoS mitigation services. Financially motivated cybercriminals can also use DDoS as a means to distract the security team from other suspicious activity in the environment. Financial institutions in particular use this tool to mitigate the effects of DDoS attacks on the online banking sites — sites which demand high availability. |
| Vendors | | Akamai, CenturyLink, CloudFlare, Corero Network Security, DOSarrest Internet Security, F5 Networks, Imperva, Level 3 Communications, NetScout (Arbor Networks), Neustar, Radware, Verisign, Verizon |
| Estimated cost to implement | | Varies: Vendors can deliver these DDoS solutions as appliances, services, or as a hybrid of the two. |
| Ecosystem phase | Growth | Although many anti-DDoS solutions have been on the market for some time, until recently the market size has been relatively small. |
| Business value-add, adjusted for uncertainty | High | In the event that an organization suffers a DDoS attack, the business value is high, particularly for industries that rely on a significant amount of revenue from eCommerce/online transactions. These solutions can ensure that eCommerce sites maintain high availability, protecting not only the brand of the organization, but also revenue-generating transactions. However, not every enterprise views hacktivist-based DDoS attacks as a huge risk and DDoS mitigation controls as a necessity. |
| Time to reach next phase | 1 to 3 years | Forrester believes that the market for DDoS protection will reach the next level within the next one to three years. |
| Trajectory (known or prospective) | Significant success | Given the increase in hacktivism and DDoS as a smokescreen for more devastating attacks, the market for DDoS protection is poised for significant success. |

**FIGURE 11** TechRadar™: Growth Phase, Network Analysis And Visibility (NAV), Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Network analysis and visibility (NAV) is a category of products that includes: 1) network discovery tools for finding and tracking assets; 2) flow data analysis tools to analyze traffic patterns and user behaviors; 3) packet capture and analysis tools that function like a network DVR; and 4) network forensics tools that assist incident response and investigations. |
| Usage scenarios | | By continuously scanning the network for malicious activity, behaviors, and potential attacks, NAV tools give security pros important situational awareness regarding the firm's security posture. |
| Vendors | | • Network discovery: Cisco Systems, Lumeta<br>• Flow analysis: Arbor Networks, Cisco Systems (Lancope), Riverbed Technology, Vitria Technology<br>• Packet capture and analysis: AccessData Group, Niksun<br>• Network metadata analysis: Fidelis Cybersecurity, Symantec (Blue Coat Systems, Narus), Vectra Networks<br>• Network forensics: Damballa, RSA |
| Estimated cost to implement | | The cost of these tools varies significantly because of the broad range of categories. The biggest challenge and cost to implementation is the network itself; inspecting and logging all network data can create a significant burden on current networks. |
| Ecosystem phase | Growth | Many factors drive NAV adoption. Insider threats remain the most significant, but others include:<br>• Custom malware designed to avoid traditional detection techniques. Highly skilled coders specialize in creating customized malware packages for a specific attack or attacker.<br>• Advanced persistent threats (APTs). Today's more sophisticated attacks require the type of enhanced vigilance that comes from properly deployed NAV tools.<br>• Compliance initiatives (PCI DSS or HIPAA/HITECH) that require advanced reporting. Most auditors or assessors will demand reports that provide detail on internal user behaviors such as audit trails. NAV tools are uniquely positioned to provide this type of compliance information in an on-demand manner.<br>• Government requirements that mandate continuous monitoring of security controls. For example, NIST 800-37 is a risk management framework that mandates a function similar to NAV called "continuous monitoring." |
| Business value-add, adjusted for uncertainty | High | In today's constantly mutating threat landscape, NAV tools provide security pros with the insight they need to prevent and detect insider and external threats as well as help meet compliance requirements. |
| Time to reach next phase | 3 to 5 years | Forrester believes that the market for standalone NAV tools is currently in the Growth stage, and, given its importance combating advanced security threats and achieving compliance, we expect to see strong growth during the next three to five years. |
| Trajectory (known or prospective) | Significant success | Forrester recommends that clients invest in NAV tools as they redesign their networks and enhance the capabilities of their security operations centers. |

**FIGURE 12** TechRadar™: Growth Phase, Security Analytics, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Security analytics (SA) platforms are built on big data infrastructure, and they ingest and correlate a variety of system logs, network flow data, threat intelligence, and other data from a variety of sources. The SA platform uses this data and machine learning techniques to provide real-time monitoring and rapid incident detection, analysis, and response. |
| Usage scenarios | | Security pros deploy SA solutions to: 1) better predict and prepare for specific threats to their firm; 2) identify, prioritize, and address vulnerabilities with real-world exploits; and 3) identify and respond to the tell-tale signs of malicious activity in progress. |
| Vendors | | BAE Systems, FICO, Forcepoint, HPE (Arcsight), Huntsman, IBM, Intel Security (McAfee), LogRythm, RSA, SAS, Splunk |
| Estimated cost to implement | | High. Commercial solutions usually have connectors to ingest logs and data from other systems; otherwise, these connectors need to be built. It's also difficult to ingest external threat intelligence in a useful format and structure. Finally, even with better statistical and behavioral modeling and predictive analytics, skilled human intervention is required to configure, adjust, and tune the platform. Otherwise, most will find the collected data volumes to be overwhelming and not very useful. To date, only large enterprises have been able to afford implementations. |
| Ecosystem phase | Growth | Despite the challenges, due to the continuous threat of a ruinous data breach, security pros, particularly those in large enterprises and in industries such as financial services, retail, energy, and defense, are prioritizing investment. |
| Business value-add, adjusted for uncertainty | High | High. The business impact of a breach can be significant. It can damage reputations for years, making it more expensive to win new customers, borrow money, and enter into new business opportunities. For large enterprises, the cost of a major customer breach can reach hundreds of millions due to the cost of remediation, customer response, lawsuits, and regulatory fines. If the breach involves IP theft, it can permanently erode competitive advantage. |
| Time to reach next phase | 3 to 5 years | Today's security information management (SIM) tools are transforming themselves into SA tools by collecting and correlating more than just system log data. They are also improving their modeling and predictive analytics. However, this has only just begun. Meanwhile, large enterprises with more expertise have been using other analytic platforms for SA, and new entrants are entering the market. |
| Trajectory (known or prospective) | Significant success | Vendors are improving interfaces, predictive analytics, reporting, etc., and developing more workflow and automation for detection and response. These improvements, together with efforts to simplify implementation and data integration, will propel SA to significant success. |

**FIGURE 13** TechRadar™: Growth Phase, Virtual Network Infrastructure, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Forrester's virtual network infrastructure (VNI) is built on five tenets that encompass multiple technologies, such as network function virtualization (NFV) and software-defined networking (SDN). NFV technology is software versions of network hardware (switches, routers, load balancers, firewalls, VPN gateways, etc.). Unlike the hardware counterpart, virtual instances of network functions can be spun anywhere there is an x86 compute platform. SDN technology uses orchestration/operating systems to easily and programmatically control flows throughout the network (physical and virtual). Additionally, SDN technology provides a place where security services can be inserted via software on the network to enhance and enforce the organization's security posture. For example, security functions can be inserted into the flow as needed by either automatically redirecting a flow to firewall hardware or spinning up a virtual firewall in the middle of flow. |
| Usage scenarios | | Primary usage scenario is for the deployment of next-generation data centers. This technology also provides value for network agility and the ability to make changes to the network based upon business demands. VNI also provides ease of deployment for segmented Zero Trust networks. |
| Vendors | | Big Switch Networks, Brocade, Cisco Systems (Embrane), Cumulus Networks, HPE, Juniper Networks, Nokia (Nuage Networks), PlumGrid, vArmour, VeloCloud, VMware |
| Estimated cost to implement | | Varies widely: differs from hardware and software technologies. |
| Ecosystem phase | Growth | Although this is a very new technology (less than one year), the market has fragmented into four areas: 1) centralized control plane with distributed data plane architecture; 2) traditional approach (smart network and controller/management); 3) hybrid approach; and 4) overlay approach (bypass the network). Overlays have passed through the Creation phase and are exiting the Survival phase. The other groups are still in the Survival phase. |
| Business value-add, adjusted for uncertainty | High | VNI architecture and associated technologies are important to the continued adoption of Zero Trust networking, as the virtual networks themselves help by segmenting traffic easily, and the use of virtual firewalls can serve as virtual segmentation gateways (VSGs) to support Zero Trust network policy. VNI also helps reduce the complexity and costs of networking, allowing for easier flexibility for business agility. |
| Time to reach next phase | < 1 year | Massive customer demand is driving increased vendor investment. We expect to see wide deployments of overlays in virtualized data centers in the next year. |
| Trajectory (known or prospective) | Significant success | VNI is a significant part of the future of networking and holds the promise to make networks easier to deploy and reconfigure and improve resource efficiency. |

## Equilibrium: NGFW Dominates While Vulnerability Scanners Are Mature

There are several important technologies that are integral to most large organizations. Forrester sees these as having reached a state of equilibrium because they're so widely deployed that their success has somewhat constrained their growth. Technologies in the Equilibrium phase are

- **Email content security (see Figure 14).** Inbound cloud filtering eliminates malicious content and spam before it ever reaches the enterprise, and because malware and spam are such large problems, these solutions are now universally deployed in most enterprises. Most email content security technologies will exist in the cloud or in a hybrid cloud/on-premises format within the next one to three years. The saturation of the technology means that most purchases are for replacement, but advancements in cloud-based alternatives and the necessity of staying ahead of the native email security features of Microsoft Office 365 will keep this technology evolving; expect another three years to reach the next stage. Major players in this space are Barracuda, Cisco Systems, Forcepoint, Proofpoint, and Symantec.[15]
- **Network vulnerability scanners (see Figure 15).** Proactive network protection includes the ability to identify risks and vulnerabilities before cybercriminals can exploit them. As a result, many security teams now scan internal and external networks on a regular basis to discover new vulnerabilities. The goal? Patch systems to protect them before they can be exploited. This market will mature over the next three to five years as app scanners and network scanners merge into a single solution. While the scanning market has become saturated with similar solutions, vulnerability scanning is transitioning to vulnerability management in order to help security teams prioritize risks and remediate them. We expect to see continued integration and improvements to improve operational efficiency and ease remediation. Vendors include BeyondTrust, Core Security Technologies, Digital Defense, Qualys, Rapid7, Tenable Network Security, and Tripwire.
- **Next-generation firewall (NGFW) (see Figure 16).** NGFWs have replaced network firewall (FW) and IPS in most instances. There will still be a small market for standalone FWs and IPS. NGFW forms the technology foundation for Zero Trust network architecture design. NGFWs are already serving as network segmentation solutions in Zero Trust networks. This space was pioneered by Check Point Software Technologies and Palo Alto Networks, but Cisco Systems, Forcepoint (Stonesoft), and Fortinet also offer competitive solutions.
- **Web application firewall (WAF) (see Figure 17).** WAF has reached equilibrium. It has almost reached its full compliance-driven capacity of PCI 6.6. Now it's a fight for best-practice web security space. The issue with WAF is that the technology is almost self-limiting. That is, a single cluster of WAFs can protect a large number of websites. WAFs provide application-level protection against known web attacks. PCI remains a critical business driver in this space, but most teams without PCI obligations understand the value of application-layer protection of mission-critical websites, and adoption will continue to grow as web-centric attacks continue to evolve over time. Akamai Technologies, Citrix, F5 Networks, Imperva, and Radware are well-known WAF players.

- **Web security gateway (see Figure 18).** Security teams use web security gateways to enforce acceptable use policies, defend against content-borne threats, manage HTTP bandwidth, and prevent data leaks. As this traffic is destined for a cloud, it makes sense to filter it there. Expect more widespread adoption of cloud-based solutions over the next one to three years. Large enterprises may still opt for a hybrid deployment model. Also, vendors will embed these capabilities into NGFWs and cloud security gateways, which will continue to impact demand for standalone appliances. Major players in this space are: Blue Coat Systems, Cisco Systems, Forcepoint (Websense), McAfee, Symantec, and Zscaler.
- **Wireless intrusion detection/prevention system (WIDS/WIPS) (see Figure 19).** Wireless networks remain an attractive target for attackers; hackers can steal credentials or attack wireless infrastructure and gain access to protected internal networks. WIDS/WIPS provides dedicated sensors or radios that continuously monitor the air for these types of attacks. Additionally, these tools monitor for rogue devices and may even have the ability to contain or shut down rogue access points. The PCI DSS mandates wireless scanning. Sadly, compliance remains the primary driver of adoption, and those mandated by compliance have already rolled it out. In addition, vendors have embedded these capabilities into most wireless infrastructure systems. Expect this technology to stall until hackers devise some new ways of exploiting wireless networks. Major players in this space are Cisco Systems, Fortinet, and Zebra Technologies.

**FIGURE 14** TechRadar™: Equilibrium Phase, Email Content Security, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Email content security technology monitors the inbound and outbound email traffic for spam, viruses, worms, Trojans, and other malware. Features include antispam, antimalware, data leak prevention (DLP), and encryption techniques. |
| Usage scenarios | | These solutions can help against spam, phishing attacks, and denial of service by monitoring inbound messages. Security pros can use DLP to control outbound mail messages and secure sensitive data during transmission. |
| Vendors | | BAE Systems, Barracuda Networks, Cisco Systems, Clearswift, Forcepoint, Fortinet, Kaspersky Lab, Microsoft, Mimecast, Proofpoint, Retarus, SonicWALL, Sophos, Symantec, Trend Micro, Trustwave |
| Estimated cost to implement | | Varies: The price will depend on the features on the appliance or service. With a few exceptions, pricing is based on a per-user pricing model, with pricing ranging from $8 per user on the low end to $26 per user at the high end. |
| Ecosystem phase | Equilibrium | The solutions can be deployed on-premises, in the cloud, or in a hybrid of the two with inbound filtering performed in the cloud and outbound filtering performed on-premises. The ability to detect and prevent phishing attacks drives vendor replacement. On-premises gateways are being disrupted by the migration to Office 365 and Google Apps, which eliminate the need for on-premises and favors cloud deployments. |
| Business value-add, adjusted for uncertainty | High | Email content security technologies can filter out unwanted and/or malicious content without burdening internal infrastructure. This not only leads to direct cost savings and operational efficiencies but helps to protect the organization from phishing attacks — one of the most common means by which cybercriminals successfully attack organizations. |
| Time to reach next phase | 1 to 3 years | This is a relatively mature technology that will continue to add even more advanced threat prevention features. During the next several years, hosted cloud email providers like Microsoft will continue to add native email security capabilities. It will be up to the email security vendors to continue to add innovative features that will convince security teams that they need to continue to invest in a third-party solution for email security. |
| Trajectory (known or prospective) | Significant success | This technology harnesses various aspects of messaging security and has multiple applications for organizations. The business value is high since it can work with technologies such as DLP and protect the sensitive data via identity-based encryption controls. |

**FIGURE 15** TechRadar™: Equilibrium Phase, Network Vulnerability Scanner, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | A network vulnerability scanner uses the network to actively probe other devices and discover security holes. The scanner typically resides on one host, from which it launches probes, collects results, and compares the results with a database of vulnerability fingerprints. |
| Usage scenarios | | In this sense, a vulnerability scanner is similar in function to a virus scanner. A host-based vulnerability scanner's capabilities, however, are more sophisticated and the tool is more introspective, determining whether the host on which it resides complies with established security policy. |
| Vendors | | BeyondTrust, Digital Defense, IBM, Qualys, Rapid7, Tenable Network Security, Tripwire |
| Estimated cost to implement | | Costs are highly variable, as they are typically based on the size and design of the network being scanned. |
| Ecosystem phase | Equilibrium | This market is reaching saturation, as many of the larger companies have already deployed this technology. Also, the PCI DSS has caused a shift toward software-as-a-service (SaaS) scanning models. |
| Business value-add, adjusted for uncertainty | Medium | As PCI continues to drive this market, this space becomes more commoditized. Vulnerability scanners are often seen as a checkbox for compliance purposes, with more intensive penetration testing outsourced to specialized expert consultants. Vulnerability assessment is transitioning to vulnerability management, which helps organizations understand their risk and how to remediate. To add value, solutions must focus on improving operations through integrations with technologies like GRC solutions or ticketing systems. Web application scanning capabilities will also continue to mature, adding additional value to the solution. |
| Time to reach next phase | 3 to 5 years | The maturity of the space signifies that it will continue to grow slowly over the next few years. New threats or disruptive technologies such as Internet Protocol version 6 (IPv6) could change this market should these types of tools meet needs from unanticipated threat vectors. |
| Trajectory (known or prospective) | Moderate success | Most large organizations have deployed some type of network vulnerability scanner. Smaller companies can get by with standalone open source tools. This will limit the success of this space, since smaller organizations will not need to purchase a commercial product to meet their needs. |

**FIGURE 16** TechRadar™: Equilibrium Phase, Next-Generation Firewall (NGFW), Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | NGFW will replace network firewall (FW) and IPS in most instances. There will still be a small market for standalone FWs and IPS. NGFW forms the technology foundation for Zero Trust network architecture design. NGFWs are already serving as segmentation gateways in Zero Trust networks. |
| Usage scenarios | | NGFWs are multipurpose security appliances that replace standalone appliances for FWs and IPS. |
| Vendors | | Barracuda Networks, Check Point, Cisco Systems, Forcepoint, Fortinet, Palo Alto Networks, SonicWALL |
| Estimated cost to implement | | Varies: One can buy appliances based on per-Gbps line speeds or based on the interfaces/devices supported. |
| Ecosystem phase | Equilibrium | The intersection of unified threat management (UTM) and network firewalls with traditional IPS is creating a more integrated multifunction gateway in which firewall and intrusion prevention are just two of the many features served by these gateways. The ready availability of dense multicore CPU appliance architectures and the rise of low-cost merchant silicon to meet specialized processing demands (such as SSL offloading and inspection) means that hardware now has the horsepower to put best-of-breed firewall and IPS functionality on the same box. |
| Business value-add, adjusted for uncertainty | High | NGFWs combine core security technologies such as firewalls and IPS, together with other security functionality, into a single appliance. This greatly simplifies network architecture and management and reduces costs because you have fewer security appliances to manage. |
| Time to reach next phase | 3 to 5 years | The standalone IPS market is a relatively mature space, but the next-generation firewall and UTM markets are expanding. We believe the time to reach the next phase is three to five years. |
| Trajectory (known or prospective) | Significant success | At Forrester, we have been anticipating this merger of technologies, and we see a bright future for integrated multifunction gateways. In fact, we anticipate that the speed and power of these devices will enable future security professionals to use these types of devices in the very core of their network to create a future state architecture we call the Zero Trust network architecture. |

**FIGURE 17** TechRadar™: Equilibrium Phase, Web Application Firewall, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Web application firewall (WAF) is a software, service, or hardware device that filters input to and output from a web server. The purpose is to block malicious input and unintentional data leaks to protect the web server and internal data. |
| Usage scenarios | | WAFs are often deployed as an explicit proxy or a bridge in front of the web server or as an offline device that sniffs web traffic. WAFs allow for virtual patching that creates special rules to block known vulnerabilities until development can patch the problem. |
| Vendors | | Akamai, Barracuda Networks, Cisco Systems, Citrix, Distil, F5 Networks, Imperva (Incapsula), Instart Logic, Qualys, Signal Sciences, tCell, Trustwave |
| Estimated cost to implement | | Medium to high. |
| Ecosystem phase | Equilibrium | Growth in the web application firewall space was stagnant until it was put into the PCI DSS. PCI has driven adoption of this technology since 2008. Although application code reviews and other software delivery life cycle (SDLC) security methods can be effective in preventing some vulnerabilities from ever being delivered to customers, WAFs provide a cost-effective and scalable solution to web-based attacks that continue to evolve over time. Cloud-based WAFs have become a popular deployment model. |
| Business value-add, adjusted for uncertainty | Medium | The business value of WAFs is medium; this is further counteracted by the fact that operational complexity is significant. WAFs require constant maintenance and monitoring. Some WAFs are able to do application profiling and contribute business intelligence, but overall, it is still a security-oriented product. WAF's security orientation does address a security imperative, however, as web app attacks accounted for about 40% of confirmed breaches in 2015.* WAFs provide granular control for web-based transactions that help in meeting PCI DSS requirements — this satisfaction of compliance requirements is the primary business impact of WAF today.<br>*Source: "2016 Data Breach Investigations Report," Verizon, 2016 |
| Time to reach next phase | 5 to 10 years | PCI continues to be the biggest driver in this space, and many late adopters to the web application firewall world will implement this technology in the next year or two, making the WAF of today ubiquitous in any organization dealing with credit cards. However, WAF technology is evolving to meet trends such as cloud-based applications and machine learning to reduce the cost and maintenance. |
| Trajectory (known or prospective) | Moderate success | As WAFs become more automated, scalable, and easy to use, these advancements may become the largest inhibitor for the trajectory of a space. Because even large web farms can be protected by a single WAF cluster, the size of the market may be self-limiting by the quality of the technology itself. Additionally, web application firewalls may increasingly become a feature of other security and network devices. |

**FIGURE 18** TechRadar™: Equilibrium Phase, Web Security Gateway, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | A web security gateway provides management of URL filtering, antimalware, internet application control, DLP, and bandwidth. |
| Usage scenarios | | Organizations typically use web security gateways to enforce acceptable use policies, defend against content-borne threats, manage HTTP bandwidth, and prevent data leaks. |
| Vendors | | Barracuda Networks, Cisco Systems, Forcepoint, Intel Security (McAfee), Microsoft, Symantec (Blue Coat Systems), Trend Micro, Trustwave, Zscaler |
| Estimated cost to implement | | Varies: It can be a proxy add-on to servers or built into the solution from the above vendors. There can be additional cost when adding this onto the solutions purchased from above vendors. Another variation can be based on the IP addresses that you want to control against. |
| Ecosystem phase | Equilibrium | The web security space is in transition, with new competition from cloud-based services such as Zscaler, which do not require on-premises proxies. Traditional web security vendors have invested in SaaS services as well: Cisco Systems acquired ScanSafe, Barracuda Networks acquired Purewire, Symantec acquired MessageLabs, and Blue Coat Systems launched a new web filtering service. As adoption of cloud-based web content filtering continues to increase, the traditional gateway market will shrink significantly. In addition, vendors are embedding the functionality in next-generation firewalls. |
| Business value-add, adjusted for uncertainty | Medium | Web content filtering can provide protection from threats embedded in websites visited by corporate employees. This can reduce outbreaks in many instances. Additionally, web content filtering is used to enforce acceptable use policies in many organizations and offers value to other departments such as legal and human resources. |
| Time to reach next phase | 1 to 3 years | This market is beginning its next phase with cloud-based services. Early adopters are already looking to move their web content filtering off-premises. The success or failure of the deployments done by these early adopters will determine the future of web content filtering. Many organizations are opting for a hybrid transition model leveraging existing investments and SaaS at the same time. Also, some of this functionality may be done by firewalls and unified threat management (UTM) appliances, thereby eliminating the need for a dedicated on-premises proxy appliance. |
| Trajectory (known or prospective) | Moderate success | Web content filtering has traditionally been designed to block URLs outside of corporate policy and thus have been important in the realms of human resources and legal affairs. As these tools continue to respond to the extended enterprise, companies increasingly rely on antimalware capabilities, rich application control for web 2.0 applications, and DLP policy enforcement. |

**FIGURE 19** TechRadar™: Equilibrium Phase, Wireless IDS/IPS, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Wireless intrusion detection/prevention systems (WIDS/WIPS) proactively prevent wireless attacks and discover rogue access points. A WIDS solution will scan the air for malicious traffic and rogue devices automatically, substantially mitigating the risk of wireless attacks. Currently, WIDS and WIPS are synonymous acronyms in terms of functionality, with some manufacturers using one term over another for marketing purposes. |
| Usage scenarios | | Without WIDS technology, security personnel are blind to the traffic moving through the air. WIDS provides visibility and alerting capability vital to enhancing wireless security. This system can often proactively protect against wireless attacks. Additionally, new solutions offer automated rogue destruction. |
| Vendors | | Cisco Systems, Extricom, Fluke Networks, Fortinet, HPE (Aruba Networks, ProCurve), Juniper Networks, Mojo Networks, Motorola |
| Estimated cost to implement | | Varies: WIDS/WIPS are priced by the wireless sensor. Because a WIDS sensor can "see" farther than a transmit/receive AP, fewer WIDS sensors are needed per installation than APs. A general rule of thumb is one dedicated WIDS sensor for every six to 10 APs. However, some vendors offer a base functionality of WIDS sensing as the primary use of one radio in a multiradio AP. |
| Ecosystem phase | Equilibrium | Wireless networks remain an attractive target for attackers: Hackers can steal credentials or attack wireless infrastructure and gain access to protected internal networks. WIDS/WIPS provide dedicated sensors or radios that continuously monitor the air for these types of attacks. Additionally, even internal users will occasionally deploy unauthorized access points (known as rogue APs). These tools monitor for rogue devices and may even have the ability to contain or shut down rogue APs. The PCI DSS mandates wireless scanning. |
| Business value-add, adjusted for uncertainty | Medium | As attack vectors evolve, more cybercriminals target wireless networks that are not properly protected. WIDS provides business value two ways: by reducing the cost of the PCI compliance and by reducing the risk for wireless. |
| Time to reach next phase | 5 to 10 years | Compliance remains the primary driver of adoption, and most companies whose compliance efforts require this technology have already rolled it out. In addition, wireless IDS/IPS has become embedded into most wireless infrastructure systems. Expect this technology to stall until wireless hackers devise some new ways of exploiting 802.11 wireless networks. |
| Trajectory (known or prospective) | Moderate success | WIDS/WIPS technology has a potential to be extremely useful in a wireless environment where traditional wired IPS technology lacks complete visibility into the radio frequency (RF) environment. |

## Decline: NAC And IPS Are On Their Way Out

There are some controls whose features and benefits were either merged into other technologies or were never fully embraced by the enterprise. These technologies are on the decline in the security space, although many will find a new life providing intelligence to infrastructure and operations professionals. We placed two technologies in the Decline phase:

- **Network access control (NAC) (see Figure 20).** NAC is on the decline, and we have seen minimal success for this technology.[16] NAC enjoyed moderate success with enterprises looking to secure guest access but has since struggled to advance. NAC may merge with similar or complementary technologies, such as internal network prevention systems or network segmentation appliances. Mobility and consumerization drive the need for user access security. There are several NAC architectures, including appliances (physical and virtual); NAC-enabled switches, routers, and servers; and software. All approaches are complex to deploy and require integration with network infrastructure. While access control functionality is important in the digital business, this need is more easily solved at the gateway than the endpoint, especially in a Zero Trust network.[17] Bradford Networks, Cisco Systems, ForeScout Technologies, HPE (Aruba), and Juniper Networks are significant vendors in this space.
- **Network intrusion prevention (see Figure 21).** Network intrusion prevention systems (IPS) are on the decline as NGFW systems overtake it. Our research shows that all significant vendors in this space have added firewall capability or are planning to do so.[18] IPS also helps fulfill PCI DSS requirements mandating that security pros place intrusion detection and prevention devices in the line of traffic and perform proper inspection to mitigate threats. This means that large PCI initiatives often fund IPS deployments.[19] While growth in the IPS space has slowed somewhat, it will continue to be a core proactive protection strategy. Expect a new growth surge as late adopters realize that their fears of blocking good traffic are unfounded and that best practices companies begin to universally deploy network IPS internally. Top standalone vendors in this space include Cisco Systems, IBM, and Trend Micro.

**FIGURE 20** TechRadar™: Decline Phase, Network Access Control (NAC), Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | Today's NAC solutions provide five primary features: 1) pre- and post-admission control to assess the current state of a connecting device to IT policy; 2) automated remediation to update the device if it's out of compliance; 3) multiple enforcement options (IPsec, MAC-based, and web authentication); 4) dedicated guest access management for third parties and customers; and 5) rogue device detection to identify unsanctioned devices such as wireless access points, switches, routers, and mobile devices on the network. |
| Usage scenarios | | Top scenarios include controlling internal employee access, guest access, contractor/supplier access, and regulatory compliance (GLBA, HIPAA, SOX, and PCI). |
| Vendors | | Bradford Networks, Cisco Systems, Extreme Networks, ForeScout, HPE (Aruba), Pulse Secure |
| Estimated cost to implement | | Varies: Due to the mix of out-of-band, infrastructure, and software-based solutions, there are many pricing models. |
| Ecosystem phase | Decline | Forrester believes the market for standalone NAC offerings is currently in the Decline stage and will phase out in the next five years. There are several reasons. First, solutions are complex to deploy, scale, and manage. There are several NAC architectures, including appliances (physical and virtual), infrastructure (NAC-enabled switches, routers, and servers), and software. Even the hardware-based approaches require the deployment of agents on endpoints and hosts. All approaches require integration with network infrastructure components. |
| Business value-add, adjusted for uncertainty | Negative | NAC functionality is important, but security pros need access control that is much more role- and data-centric than device-centric. Generally, vendors can identify and inventory mobile operating systems (Apple, Android, Windows mobile, etc.) as well as take actions to either grant them internet access or block them. However, they can't actively fingerprint and enforce policies and have phones checked for health and anomalous behavior after connection. Also, NAC won't stop a malicious insider who wants to commit a security breach. Just because someone has a clean machine doesn't mean you can stop their malicious activity. |
| Time to reach next phase | 3 to 5 years | Forrester believes that the market for standalone NAC offerings is currently in the Decline stage and will likely phase out in the next five years. |
| Trajectory (known or prospective) | Minimal success | NAC functionality is useful, but as a standalone product, the market will have minimal success. As this market evolves, vendors will embed NAC functionality into security software suites or into switching infrastructure. The number of vendors offering standalone NAC solutions is shrinking, and those that are left, such as Bradford Networks and ForeScout Technologies, are working to ensure that their appliances are part of an extended solution that offers more than just NAC. |

**FIGURE 21** TechRadar™: Decline Phase, Network Intrusion Prevention, Q4 '16

| Element | Categorization (if applicable) | Explanation |
|---|---|---|
| Definition | | A network intrusion prevention system (IPS) device monitors network and/or system activities for malicious or unwanted behavior and can react in real time to block or prevent those activities. |
| Usage scenarios | | IPS solutions provide proactive security controls to protect sensitive and critical data from attack. Because these devices are inline and can enforce policy and block attacks, they provide an efficient protection platform that is easy to manage. These devices reduce the need for incident response, forensics examination, and device rebuilding and recovery that are common in environments with passive intrusion controls. |
| Vendors | | Check Point, Cisco Systems, Dell, Fortinet, IBM, Intel Security (McAfee), Juniper Networks, Palo Alto Networks, Radware, SonicWALL, Trend Micro |
| Estimated cost to implement | | Varies: One can buy appliances based on per-Gbps line speeds or based on the interfaces/devices supported. |
| Ecosystem phase | Decline | The intersection of unified threat management (UTM) and network firewalls with traditional IPS solutions is creating a more integrated multifunction gateway in which firewall and intrusion prevention are just two of the many features served by these gateways. The standalone IPS market is a relatively mature space, but the next-generation firewall and UTM markets are expanding. |
| Business value-add, adjusted for uncertainty | Medium | An intrusion prevention system complements traditional firewalls by inspecting the entire network packet, looking for malicious traffic that is often invisible to Layer 3 firewalls. While firewalls are the cornerstone of any network security design, IPS appliances are the bulwark. Within the time-honored security approach known as defense-in-depth (DiD), IPS devices are the second line of network defense. |
| Time to reach next phase | 5 to 10 years | Forrester believes that the market for standalone IPS offerings is currently in the Decline stage and will likely phase out in the next five to 10 years. |
| Trajectory (known or prospective) | Significant success | IPS has been successfully deployed by most of the world's largest companies. Forrester sees continued success in this space as IPS becomes as ubiquitous for all networks as firewalls are today. Although NGFWs will ultimately replace IPS, expect a new growth surge as late adopters realize their fears of blocking good traffic are unfounded and best practices companies begin to universally deploy network IPS internally. |

**Recommendations**

## Segment Your Network, Invest In Analytics, And Automate Response

It's important to understand that the threat landscape is always changing and stasis is not an option. Look for areas of weakness within your network, and then strengthen them with some of the new threat mitigation technologies that are already demonstrating significant success. More specifically, as a security leader you should:

- **Design security using Zero Trust principles.** Too often, security is an afterthought of network design, and yesterday's hierarchical networks are ineffective against today's advanced cyberthreats. We must strip away yesterday's hierarchical network so that security is no longer merely an overlay but is built into the DNA of the network itself. We're overburdened with individual security controls deployed in a seemingly haphazard manner. We must look for products that consolidate individual security controls into fewer devices like NGFWs or data access and security capabilities integrated directly into cloud security gateways.
- **Invest in detection.** When preventive controls fail, security teams must rely on network and application visibility to quickly identify and respond to security incidents. NAV and security analytics solutions provide a type of network omniscience that is imperative in today's threat environment. The sooner the security team is able to detect, contain, and remediate a breach, the sooner the firm can deal with the consequences. Today, many security teams don't even realize they've suffered a breach; it's often a third party that informs them.
- **Prioritize technologies that automate response.** Enterprises should be more fearful of the consequences of cyberattacks — which are real, probable risks for any connected organization — than they are of the remote possibility that these proactive controls will block legitimate traffic. Proactive controls are the best defense against the majority of cyberattacks. The emergence of better detection and decision-making technologies like security analytics is now making it possible to automate breach response to limit the impact of cyberattacks. Take proactive steps to protect data and use automation and orchestration tools to speed remediation efforts.
- **Choose the right delivery model.** Today's security teams are strapped staff and skill. Many of the technologies outlined in this report are available as managed services or security-as-a-service (SaaS). Sourcing your technology from a service provider can dramatically cut the time to deployment, in some cases improve protection, and provide 24x7 coverage and customer service. Email security and web filtering delivered via a SaaS model is already widely accepted, and malware analysis SaaS is following in its footsteps.

## Supplemental Material

### Online Resource

The underlying spreadsheet that exposes all of Forrester's analysis of each of the 20 technologies in the TechRadar (Figure 1) is available for download.

### Data Sources Used In This TechRadar

Forrester used a combination of two data sources to analyze each technology's current ecosystem phase, business value adjusted for uncertainty, time to reach next phase, and trajectory:

› **Vendor surveys, briefings, inquiries, and advisories.** Forrester surveyed a diverse set of vendors with products and partnerships in one or more of the technology categories.

› **Current and prospective customer and user inquiries and advisories.** Forrester relied on user inquiries and advisories to determine current and prospective uses for the technologies and their impact on the customers' businesses and the users' work.

## The Forrester TechRadar Methodology

Forrester uses the TechRadar methodology to make projections for more than a decade into the future of the use of technologies in a given category. We make these predictions based on the best information available at a given point in time. Forrester intends to update its TechRadar assessments on a regular schedule to assess the impact of future technical innovation, changing customer and end user demand, and the emergence of new complementary organizations and business models. Here's the detailed explanation of how the TechRadar works.

› **X-axis: Divide technology ecosystem maturity into five sequential phases.** Technologies move naturally through five distinct stages: 1) creation in labs and early pilot projects; 2) survival in the market; 3) growth as adoption starts to take off; 4) equilibrium from the installed base; and 5) decline into obsolescence as other technologies take their place. Forrester placed each of the 20 threat mitigation technologies in the appropriate phase based on the level of development of its technology ecosystem, which includes customers, end users, vendors, complementary services organizations, and evangelists.[20]

› **Y-axis: Measure customer success with business value-add, adjusted for uncertainty.** Seven factors define a technology's business value-add: 1) evidence and feedback from implementations; 2) the investment required; 3) the potential to deliver business transformation; 4) criticality to business operations; 5) change management or integration problems; 6) network effects; and 7) market reputation. Forrester then discounts potential customer business value-add for uncertainty. If the technology and its ecosystem are at an early stage of development, we have to assume that its potential for damage and disruption is higher than that of a better-known technology.[21]

› **Z-axis: Predict the time the technology's ecosystem will take to reach the next phase.** Security and risk professionals need to know when a technology and its supporting constellation of investors, developers, vendors, and services firms will be ready to move to the next phase; this allows them to plan not just for the next year but for the next decade. Of course, hardware moves more slowly than software because of its physical production requirements, but all technologies will fall into one of five windows for the time to reach the next technology ecosystem phase: 1) less than one year; 2) between one and three years; 3) between three and five years; 4) between five and 10 years; and 5) more than 10 years.[22]

› **Curves: Plot technologies along one of three possible trajectories.** All technologies will broadly follow one of three paths as they progress from creation in the labs through to decline: 1) significant success and a long lifespan; 2) moderate success and a medium to long lifespan; and 3) minimal success and a medium to long lifespan. We plot each of the [number] most important technologies for threat mitigation on one of the three trajectories to help security and risk professionals allocate

their budgets and technology research time more efficiently.[23] The highest point of all three of the curves occurs in the middle of the Equilibrium phase; this is the peak of business value-add for each of the trajectories — and at this point, the adjustment for uncertainty is relatively minimal because the technology is mature and well-understood.

› **Positions on curves: Where possible, use this to fine-tune the z-axis.** We represent the time a technology and its ecosystem will take to reach the next phase of ecosystem development with the five windows above. Thus, technologies with more than 10 years until they reach the next phase will appear close to the beginning of their ecosystem phase; those with less than one year will appear close to the end. However, let's say we have two technologies that will both follow the moderate success trajectory, are both in the Survival phase, and will both take between one and three years to reach the next phase. If technology A is likely to only take 1.5 years and technology B is likely to take 2.5 years, technology A will appear further along on the curve in the Survival phase. In contrast, if technologies A and B are truly at equal positions along the x-, y-, and z-axes, we'll represent them side by side.

## Companies Interviewed For This Report

Akamai
AlgoSec
Attivo
BAE Systems
BeyondTrust
Blue Coat Systems
BluVector
Certes Networks
Check Point
Cisco Systems
Citrix
Cryptzone
Dome9
Fidelis Cybersecurity
FireEye
Forcepoint
ForeScout
Hexis
HPE
IBM
Imperva
Intel Security
IXIA
Juniper Networks
LogRhythm
Niksun
Palo Alto Networks
Phantom
RSA
SafeBreach
Skyhigh Networks
Solar Winds

SonicWALL
Sophos
Splunk
Stratum Security
Tenable
TopSpin Security
Trend Micro
Tripwire
Unisys
vArmour
Vaultive
Vectra Networks
VeloCloud
Verisign
Watchguard
Zscaler

## Endnotes

[1] Breaches are often part of larger, more complex criminal initiatives. Many attribute the breaches at Anthem and the US Office of Personnel Management (OPM) to state-sponsored agents seeking to gather sensitive intelligence on high-level individuals. By reflecting on these breaches, we can glean long-term lessons to help security pros improve their firm's overall security posture. For more, see the "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[2] Source: Stephanie Balaouras, "Cybersecurity Takes Center Stage In US Presidential Election," Stephanie Balaouras' Blog, July 25, 2016 (http://blogs.forrester.com//stephanie_balaouras/16-07-25-cybersecurity_takes_center_stage_in_us_presidential_election).

[3] Data is the lifeblood of today's digital businesses, but sophisticated cybercriminals have given rise to a complex market for data security and privacy. Forrester's Data Security And Control Framework, integrated with our Zero Trust Model, guides you through substantive changes to your processes for defining, dissecting, and defending data. For a complete overview, see the "Protect Your Intellectual Property And Customer Data From Theft And Abuse" Forrester report.

[4] Zero Trust eliminates the idea of an internal trusted network and an untrusted external network. Instead, security becomes ubiquitous throughout the digital business ecosystem. S&R leaders invest in threat intelligence and vulnerability management, and develop robust detection, incident response, and forensic capabilities. For a step-by-step guide to Zero Trust implementation, see the "Five Steps To A Zero Trust Network" Forrester report.

[5] Forrester defines security analytics as a platform which provides real-time monitoring and facilitates rapid incident detection, analysis, and response. For more information, see the "Counteract Cyberattacks With Security Analytics" Forrester report.

[6] The security gap between new attack methods and traditional controls continues to grow in favor of the attackers. Hackers today are highly organized, well-funded crime syndicates or state-sponsored agents, and continued cyberattacks demonstrate ever more devious ways of bypassing security controls. For a full picture of the potential damage this represents to your business, see the "Understand The Business Impact And Cost Of A Breach" Forrester report.

[7] Breaking news of a massive customer breach dominates headlines for days. However, months and even years later, affected customers still struggle with the aftermath, and firms are still absorbing the costs. By reflecting on these breaches, we can glean long-term lessons that help security and risk (S&R) pros improve their firm's overall security posture, its breach response, and its appreciation of privacy law and customer trust. For more information, see the "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[8] For further details on TechRadar methodology, read Supplemental Material section of this document and our report introducing this new type of research. See the "Introducing Forrester's TechRadar™ Research" Forrester report.

[9] Software defined networking (SDN) and network functions virtualization (NFV) are completely different, but I&O pros must invest in them together because one without the other offers little value. For a full picture of the innovations on the horizon of infrastructure and operations, see the "Top Eight Technology Trends That I&O Pros Should Watch: 2016" Forrester report.

[10] With HIPAA audits and fines on the rise, a rapidly changing threat landscape, and increasing public sensitivity regarding patient privacy, Forrester sees an increased focus on security and risk maturity. For more information on healthcare security, see the "Industry Spotlight: US Healthcare Security Budgets And Priorities, Q4 2015 To Q3 2016" Forrester report.

[11] In order to protect your sensitive data in the cloud from security breaches, privacy abuses, and other incidents, you need an overarching strategy and a detailed road map that includes cloud discovery and workload management, data protection, activity and threat monitoring, data loss prevention, and identity and access management. For more information on cloud security, see the "Create Your Cloud Security Technology Strategy And Road Map" Forrester report.

[12] As data volumes explode, it is becoming a herculean task to protect sensitive data from cybercriminals and malicious actors while preventing privacy infringements and abuses — intentional and unintentional. To see how cloud encryption gateways compare to other technologies, see the "TechRadar™: Data Security, Q1 2016" Forrester report.

[13] Many SDN solutions seem similar but provide very different benefits and architecture from both emerging and traditional networking vendors. For market overview of SDN, see the "Vendor Landscape: Software-Defined Networking Overlay Solutions" Forrester report.

[14] Trust is the fundamental problem in information security today. By changing our trust model we can change our networks and make them easier to build and maintain. For more information on Zero Trust network architecture, see the "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" Forrester report.

[15] In Forrester's 47-criteria evaluation of email content security vendors, we identified the nine most significant vendors in the category and researched, analyzed, and scored them. To see how the vendors stack up, see the "The Forrester Wave™: Email Content Security, Q4 2012" Forrester report.

[16] In 2011, Forrester conducted a comprehensive evaluation of NAC offerings when the technology was in its survival stage. To see who led the pack and who was left behind, see the "The Forrester Wave™: Network Access Control, Q2 2011" Forrester report.

[17] Forrester's Zero Trust Model of information security banishes the old security motto of "trust but verify" and replaces it with a new motto: "Verify but never trust." For more information on using Zero Trust design methodologies, see the "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem" Forrester report.

[18] Because of the increasing demand for Zero Trust networks, Forrester envisioned the development of a new product category called a network segmentation gateway, a product category that is much more than a "next-generation firewall." For more information, see the "Market Overview: Network Segmentation Gateways, Q4 2013" Forrester report.

[19] To effectively deal with the broad and complex requirements of Payment Card Industry (PCI) data security, you need to break the elements apart to provide enhanced clarity. We've designed the PCI X-Ray series to provide actionable information to help Forrester Research clients become PCI-compliant. This document deals with the IDS and IPS aspects of the PCI Data Security Standard (DSS) and provides practical technical guidance to help ensure PCI compliance before your auditor shows up to develop the report on compliance (ROC). See the "PCI X-Ray: IDS And IPS" Forrester report.

[20] Note that the five phases are not of any prescribed length of time. For the typical technology ecosystem profiles for each of the five phases, see Figure 3 in the introductory report. See the "Introducing Forrester's TechRadar™ Research" Forrester report.

[21] We outline the detailed questions we ask to determine business value adjusted for uncertainty in Figure 4 of the introductory report. See the "Introducing Forrester's TechRadar™ Research" Forrester report.

[22] Forrester will include relatively few technologies that we predict will take more than 10 years to reach the next ecosystem phase. Expect to see these 10-year-plus technologies only in the Creation phase for fundamental hardware innovations and in the Equilibrium and Decline phases for hardware and software on the "significant success" trajectory. We provide details on how we predict the amount of time that a given technology will take to reach the next phase of technology ecosystem evolution in the introductory report. See the "Introducing Forrester's TechRadar™ Research" Forrester report.

[23] We provide detailed information and examples of how we predict the amount of time that a technology will take to reach the next phase of ecosystem development in the introductory report. See the "Introducing Forrester's TechRadar™ Research" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

## We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

## Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

**Marketing & Strategy Professionals**

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

**Technology Management Professionals**

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

**Technology Industry Professionals**

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.