For: Security & Risk Professionals

Three Technical Innovations Will Ignite Zero Trust

by John Kindervag and Andre Kindness, May 5, 2015

KEY TAKEAWAYS

Your Network Is Broken

The networks we all use today were designed in the 1980s and 1990s -- last century. These networks were created before there were worms, viruses, cybercrime, and data breaches. As businesses moved into the 21st century, most technology matured and evolved to meet the needs of this new digital age. But the one thing that hasn't changed is your network.

Zero Trust Is The Answer

Forrester has found that a flawed trust model where external networks were untrusted but internal networks were trusted by default was the fundamental problem of the modern network. Attackers have repeatedly, and with great success, exploited this implicit trust assumption. The only solution is to adopt a Zero Trust approach.

Three New Innovations Will Fuel Zero Trust Adoption

Most modern security controls fit nicely into a Zero Trust network when one considers them systemically as part of a holistic solution instead of as standalone products. However, there are three innovations that are fueling Zero Trust networking: next-generation firewalls, virtual network infrastructure, and network orchestration solutions

Three Technical Innovations Will Ignite Zero Trust

by John Kindervag and Andre Kindness
with Stephanie Balaouras, Rick Holland, Kelley Mak, and Josh Blackborow

WHY READ THIS REPORT

Forrester's Zero Trust Model of information security is gaining worldwide traction. Security and risk (S&R) pros at large enterprises are adopting and implementing Zero Trust networks and discovering huge benefits from this move. Building a Zero Trust network is becoming easier as a result of several new technological innovations that have happened in the past few years. The network and security landscapes are quickly and dramatically changing. These changes will help usher in the era of widespread acceptance and adoption of Zero Trust networking. In this report, we examine the implications of these changes and highlight the three technical innovations that will help S&R pros move from Zero Trust as concept to Zero Trust as reality.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Five Steps To A Zero Trust Network

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

TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015

YOUR NETWORK IS BROKEN

The networks we all use today were designed in the 1980s and 1990s — last century. These network paradigms were created before there were worms, viruses, cybercrime, data breaches, and nation-state attacks. As businesses moved into the 21st century, most technology matured and evolved to meet the needs of this new digital age. Applications moved from client/server models to web-based deployments. Moore's Law has proven itself prescient as hardware speeds have continued to increase just as the cost to manufacture silicon chips has been reduced over time.[1] But the one thing that hasn't changed since last century is your network. It remains in the ancient past of Internet time and must be revolutionized. Your legacy network:

- **Lacks robust, embedded security.** Networking remains primarily a hierarchical design featuring large switching cores that distribute traffic to users in a multihop and convoluted way. These networks were designed to be efficient and cost-effective, not secure. When security concerns arose, networkers invariably tried to build castle walls around the network to protect it. The network security industry is so tied to the ideas of medieval castle building that words such as "moat" and "bastion" are commonplace. However, just as the medieval castle could not survive the technological disruptions of modern warfare, so to the hierarchical network cannot survive the technological disruptions of the modern cyberattacker.

- **Fails to address the technical needs of today's digital business.** It's apparent to everyone that the old medieval perimeters are no longer enforceable in the world of network security. Often termed deperimeterization, modern networkers and security professionals must deal with the implications of cloud use, virtualization technologies, software-defined networking (SDN), BYOD, and mobile device proliferation. All of these innovations have changed the way business works. Our networks are now highly bifurcated and distributed. A perimeter is not only unenforceable, it does not even exist. The castle walls have come tumbling down. A new way of defending the crown jewels must be developed, adopted, and implemented.

ZERO TRUST IS THE ANSWER

In 2008, Forrester Research embarked on a project to look at networking from a security perspective and to determine how networks must evolve to meet the security challenges of the 21st century. This led to the development of the Zero Trust Model of information security and the design paradigms contained in our Zero Trust reference network architecture. Forrester concluded that a flawed trust model where external networks were untrusted but internal networks were trusted by default was the fundamental problem of the modern network. Attackers have repeatedly, and with great success, exploited this implicit trust assumption. In fact, for most attackers it was relatively easy, because once they bypassed the perimeter of legacy hierarchical networks and compromised the credentials of internal employees and systems, they essentially had free rein to root around inside a company's systems with impunity looking for valuable data that they could steal for their own use or to sell on underground black markets.

In a Zero Trust network, one never assumes trust and one never assumes that a business process is self-contained within the infrastructure confines of the company. The implications of Zero Trust networks were immediate and intuitive for many technology management organizations struggling with either the threat or impact of a data breach. Zero Trust was the first architectural model for the modern age. It acknowledged an increasingly mobile workforce where neither employees nor business processes operated behind imaginary castle walls. Zero Trust:

- **Demands that S&R pros continuously monitor all traffic for suspicious activity.** Zero Trust strips away the anthropomorphic tendency to humanize networks and computers. We say, "Alice and Bob are on the network." In reality, neither Alice nor Bob have ever been on a network. Packets generated by devices asserted to come from the identities known as Alice or Bob are what traverses networks. Packets are not people. They are electrons and photons that represent binary data that can be useful to various computational devices. Therefore, it makes no sense to apply human concepts such as trust to those packets. Attackers can compromise identities and devices. If you take a Zero Trust approach to security, you never assume trust, and this forces you to continuously monitor all network traffic for suspicious activity and to check and enforce the assertions made by this binary information.

- **Protects access to sensitive data regardless of device type, location, or user population.** Zero Trust does not care about the physical location of the device generating packets; it securely connects the device regardless of its location. Also, it does not allow unfettered access to data just because a device is located on a trusted network. This approach automatically demands that S&R pros control access to data more granularly. In medieval times, guards at the gate enforced the comings and goings of people in and out of the castle. But with no walls surrounding the castle any longer, guards must be placed closer and closer to the valuables that need protection. The crown jewels must be in sight of the guards at all times, with the guards allowing only a very limited group of people intimate interaction with those jewels.

- **Requires that S&R pros have an in-depth understanding of their firms' sensitive data.** Unfortunately, many security teams and their counterparts in tech management have no visibility into their crown jewels — their toxic or proprietary data — in order to even begin creating the strategy to protect it. Therefore, it's important to remember that Zero Trust is data-centric. In a Zero Trust network, S&R pros create microperimeters of control and visibility around the firm's most sensitive data assets and the ways in which the enterprise uses its data to achieve its business objectives. Know your data: Know where it is, know how toxic it is, and know which users or devices are supposed to have access to it. This is the first step in your Zero Trust journey.

THREE NEW INNOVATIONS WILL FUEL ZERO TRUST ADOPTION

In just a few short years, Zero Trust has grown from conceptual theory to implemented reality as vendors have developed technologies that make adopting a Zero Trust architecture more and more feasible and available to almost all organizations. Early adopters of Zero Trust were governments, defense contractors, or very large enterprises that had the manpower necessary to implement and manage this new type of network. Today, technological advancements have made deploying and maintaining Zero Trust networks easier and more intuitive (see Figure 1).[2]

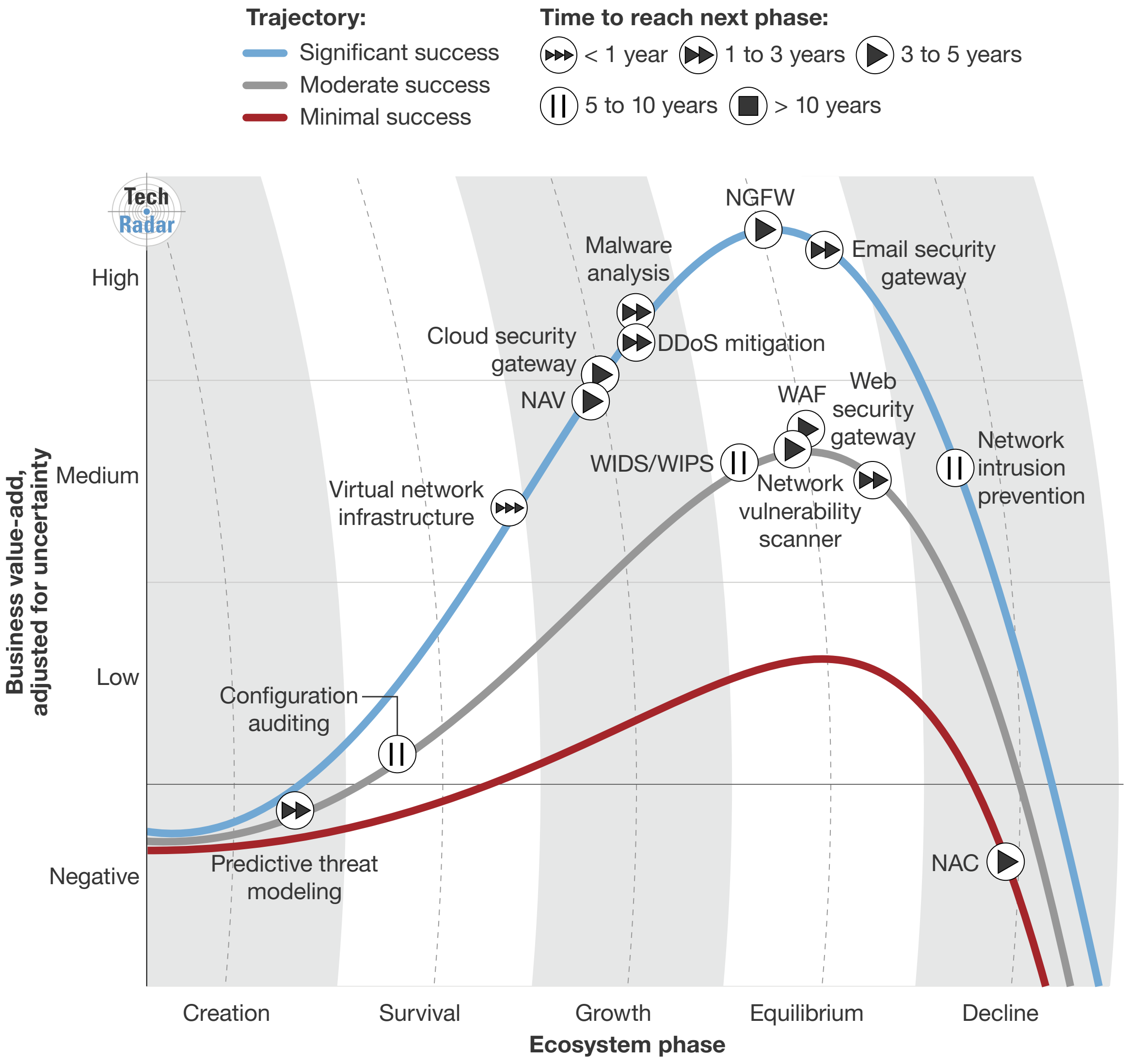
Vendors have even banded together to create partnerships which essentially offer off-the-shelf Zero Trust solutions. For example, Brocade has partnered with Palo Alto Networks to build an integrated Zero Trust solution for big iron data centers.[3] Meanwhile, VMware is building a Zero Trust ecosystem around its NSX network virtualization offering.[4] In fact, most modern security controls fit nicely into a Zero Trust network when one considers them systemically as part of a holistic solution instead of as standalone products (see Figure 2).[5] There are three innovations fueling Zero Trust networking:

- **Next-generation firewalls (NGFWs).** Zero Trust network architecture is possible because of advancements in firewalls. The creation of NGFWs pulled powerful network security controls into a single high-speed gateway that security professionals can place in the center of a network instead of at the edges where they are far away from the data they need to protect. At Forrester, we call next-generation firewalls "segmentation gateways" because using the antiquated term firewall connotes an edge device. But Zero Trust requires that security be placed as close as possible to the data it's designed to defend. By using the term segmentation gateways, we underscore the notion that technology professionals must build security into the very fabric of the modern network and not push it to the side as IT did when securing last century's hierarchical networks.

- **Virtual network infrastructure (VNI).** The development and adoption of VNI has accelerated the adoption of Zero Trust networking tremendously. VNI architecture uses physical and virtual network components to: 1) leverage and balance workloads between virtualized and physical infrastructure; 2) act as a vertically integrated Layer 2 to Layer 7 module within the infrastructure; 3) create a fabric of horizontally interconnected components; 4) automate and orchestrate the infrastructure to deliver the right services for each user; and 5) allow management by business units.[6] Before VNI, segmenting your networking into a series of microperimeters protecting and monitoring sensitive data assets was a manual process.

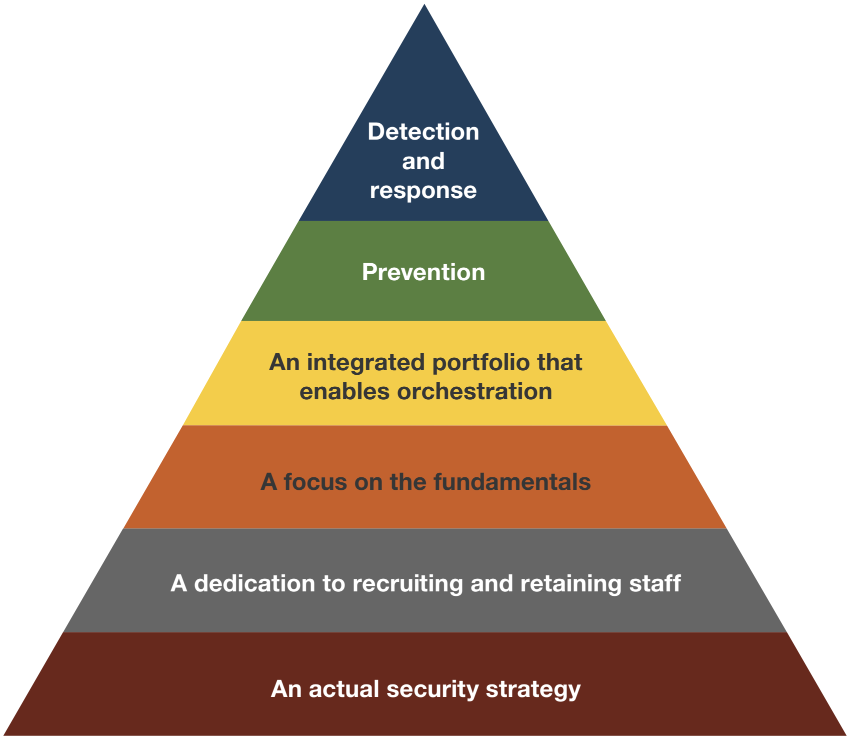
- **Network orchestration solutions.** The desire for agile network programmability powered by centralized management is key to 21st-century networking. It's also key to security. In Forrester's "Targeted-Attack Hierarchy Of Needs" we state that need No. 4 is "an integrated portfolio that enables orchestration." In many large enterprise environments, it's not unusual to find dozens and dozens of point security products with their own management interface and little integration across. If you want to detect and respond to threats in real time (as opposed to 205 days later), you need security analytic solutions that integrate with your segmentation gateways and your virtual and physical network infrastructure.

Figure 1 TechRadar™: Network Threat Mitigation, Q1 '15



119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 2 The Targeted-Attack Hierarchy Of Needs


Detection and response
Prevention
An integrated portfolio that enables orchestration
A focus on the fundamentals
A dedication to recruiting and retaining staff
An actual security strategy

119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Innovation No. 1: Next-Generation Firewalls Serve As The Foundation For Zero Trust

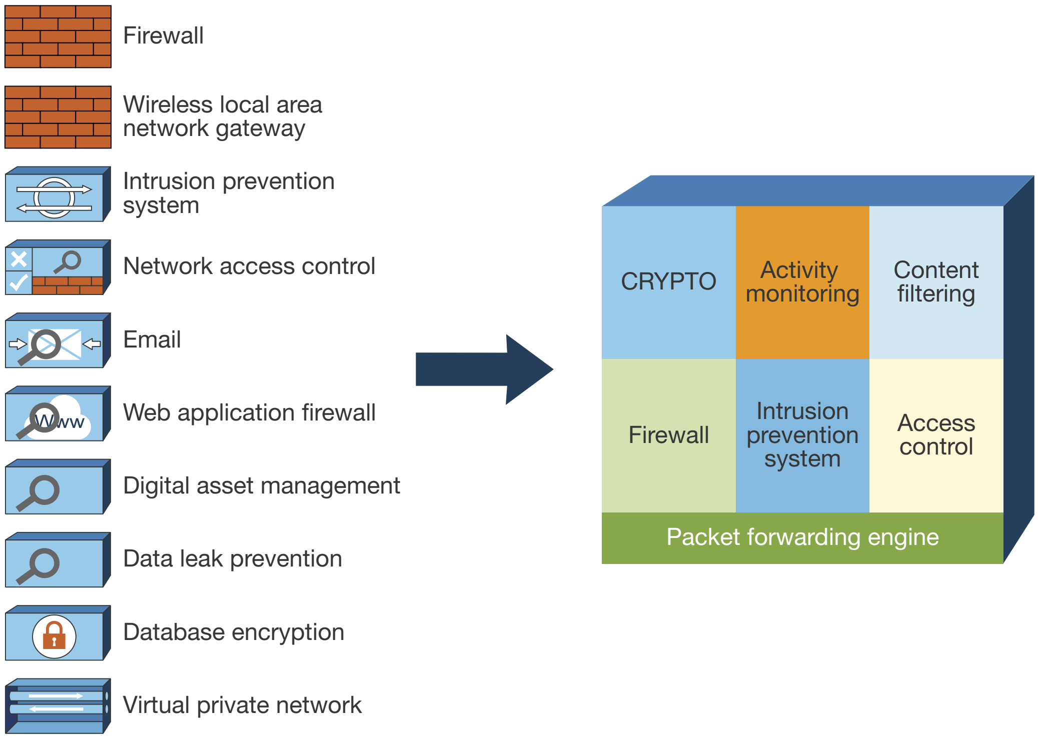
NGFWs serve as the foundation for Zero Trust. Since they can serve as segmentation gateways, S&R pros can place NGFWs inside the network to protect sensitive systems and data without appreciably degrading performance. The real reason our industry did not place security controls inside the perimeter was because of performance fears. However, Moore's Law holds true. Technology, especially security hardware, has become faster and faster as the computing components that run these devices have become more powerful and less expensive. NGFW vendors suitable to serve as segmentation gateways include CheckPoint Software Technologies, Cisco Systems, Dell SonicWall, Fortinet, Intel Security, and Palo Alto Networks. The segmentation gateway serves as the heart of a Zero Trust network. It enforces the three main tenets of Zero Trust at a tactical and technological level because it:

- **Provides location-independent secure connectivity.** In a world increasingly driven by mobile and cloud adoption, security professionals must free themselves from the tyranny of location. Few, if any, modern enterprises even attempt to contain all sensitive traffic within a single perimeter. The days of hauling all worldwide Internet traffic back to a central data center are long gone. Mobile devices may well connect from anyplace in the world via multiple transport mechanisms, including Wi-Fi and LTE. Segmentation gateways have the ability to help provide secure connectivity as most of them will support clientless SSL VPN (using TLS) to provide encrypted tunneling. Since the segmentation gateway can decrypt VPN traffic, it can also inspect it for threats using intrusion prevention features and apply Layer 7 firewall rules to help make certain that remote access traffic is clean.

- **Enables granular access control to the data.** Firewalls are designed to control access. In fact, firewalls evolved from simple access control lists (ACLs) into dedicated appliances that not only did access control but also maintained stateful knowledge of the packet. Known as stateful packet inspection firewalls, they made decisions based on information in Layer 2 and Layer 3 of the packet. Next-generation firewalls, however, have Layer 7 visibility, so the access control can be more precise than in a stateful firewall. Access control rules can be based on higher-level information such as the application in use or the identity of the user in the flow. This type of information is very valuable as it helps security professionals understand the location and potential sensitivity of data being accessed through a connection.

- **Inspects and logs all network traffic.** Most breaches are simple, but they are successful because attackers understand how to avoid detection. They know that most S&R pros fail to monitor their internal networks for direct traffic. The latest Mandiant M-Trends report reveals that it takes breached organizations a shocking 205 days to detect breaches. Worse still, a third party alerted 69% of those organizations to their breach.[7] Attackers know that once they gain access to the internal network, they will have their privileges elevated to the level of a trusted user, and this allows them unfettered access to the internal network by default. A segmentation gateway helps solve this problem because almost all traffic will run through it and it can then forward that traffic to a security analytics system for evaluation and threat detection. This efficient solution makes it much more difficult for attackers to remain invisible (see Figure 3).[8]

Figure 3 Rebuilding The Secure Network



119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Innovation No. 2: Virtual Network Infrastructure Simplifies Zero Trust Interconnectivity

Before VNI, in order to create a Zero Trust network, networking professionals built out one-dimensional network maps and used the command line interfaces (CLIs) of each switch to direct certain types of traffic to a segmentation gateway through a particular virtual local area network (VLAN). Once the tagging was complete, the segmentation gateway could read the tag and apply policy to the VLAN so that that traffic flowed to the correct microperimeter.

Since this process was often manual, many networking professionals loathed to even begin building Zero Trust networks. Many teams were overwhelmed and weren't sure where to start. Network infrastructure had over time become a spaghetti of connections with various Layer 4 through Layer 7 appliances dangling off the network like warts. Any slight change could cause networks to crash. However, with VNI, S&R pros can:

- **Easily segment their network into microperimeters.** Unlike traditional network architecture and solutions, VNI architects a network infrastructure that automatically interweaves connections and services to create microperimeters. This greatly simplifies planning, deploying, and managing Zero Trust networks and is driving the second generation of Zero Trust networks. By leveraging virtual networking, S&R pros and their networking counterparts can more easily create the microperimeters around their sensitive data and build powerful Zero Trust networks.

- **Place controls close to the firm's most sensitive data assets.** VNI technology allows S&R pros to insert virtual controls, such as virtual versions of next-generation firewalls, directly and automatically into the virtual network itself. These software-based next-generation firewalls serve as virtual segmentation gateways and make deploying distributed Zero Trust networks easier, more cost-effective, and manageable.

VNI offerings are available from vendors in both hardware platforms, such as Alcatel Lucent's Application Fluent Networks, Avaya's Virtual Enterprise Network Architecture, and Cisco Application Centric Infrastructure; and software platforms, such as Nuage Virtualized Services Platform and VMware NSX. Other companies are looking to expand the definition of VNI by creating new ways of virtualizing network infrastructure. Startups with interesting technology in the VNI space include Illumio and vArmour.

Innovation No. 3: Network Orchestration Tools Ease Deployment And Management

In a perfect world, we would achieve that much-hyped single-pane-of-glass that has been promised for so many years. This interface would be as easy to use as an iPad and as visually stunning as the screens seen in science fiction movies such as "*Minority Report*." While that fictional future may take a long time to get here, we can proactively move toward easier and effective orchestration in our networks if S&R pros:

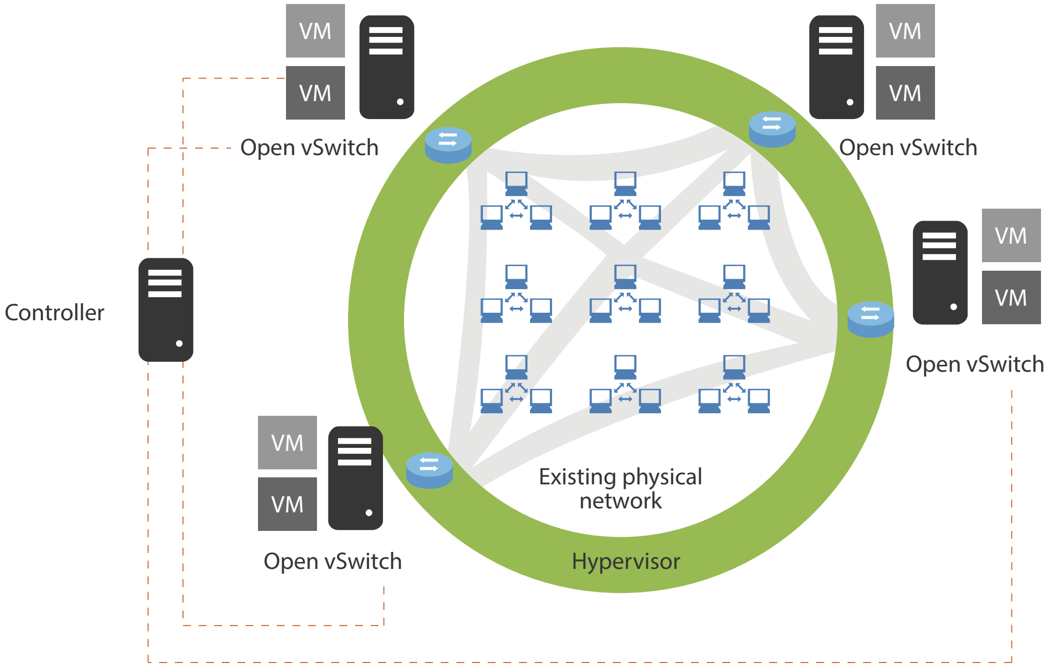
- **Select NGFW/segmentation gateways with intuitive management interface.** To meet the demands of a very agile business, technology pros need software that manages the network at the speed of business. In a Zero Trust network, management becomes the new backplane. The goal is to reduce the number of management interfaces as much as possible. The segmentation gateway management console becomes, in effect, the actual segmentation gateway for the entire enterprise no matter how many appliances or virtual segmentation gateways are actually deployed. Therefore, segmentation gateways should be chosen based on a vendor's ability to provide both hardware and software versions as well as the intuitive and efficient nature of the management console. It's best to standardize on a single segmentation vendor, as any theoretical security value in using multiple vendors will be trumped by more efficacious management.

- **Select network solutions that can manage virtual and physical components.** Additionally, there will usually be separate interfaces for both the virtual network and the physical network for your environment. Software-defined networking holds great promise in merging the management of virtual and hardware networks across multiple vendors, which is the fifth objective of Forrester's VNI architecture (see Figure 4).[9] The maturity of SDN may signal a significant shift in the ability of organizations to more gracefully manage their networks ubiquitously (see Figure 5).[10] SG management centers or VNI interfaces may also expand their capability to manage other parts of the network as the battle for orchestration dominance begins. The VNI vendors are now putting greater focus on their management capabilities in order to solidify their positions, while companies such as CloudPassage and Proofpoint Net Citadel are looking at taking unique, and perhaps revolutionary, approaches to agile orchestration.

- **Send log and metadata information to your security analytics solution . . .** You should send log and metadata information from both the hardware and software networks to a security analytics tool for correlation (see Figure 6).[11] That the hardware network and the software network don't talk or share context is a weakness that attackers are well able to leverage in order to avoid detection. Security analytics offerings including CSG Invotas, IBM Q1 Labs, Intel Security, LogRhythm, and RSA also have the ability to push into the orchestration wars, as those tools have a vast amount of important data relevant to the effective management of the network.

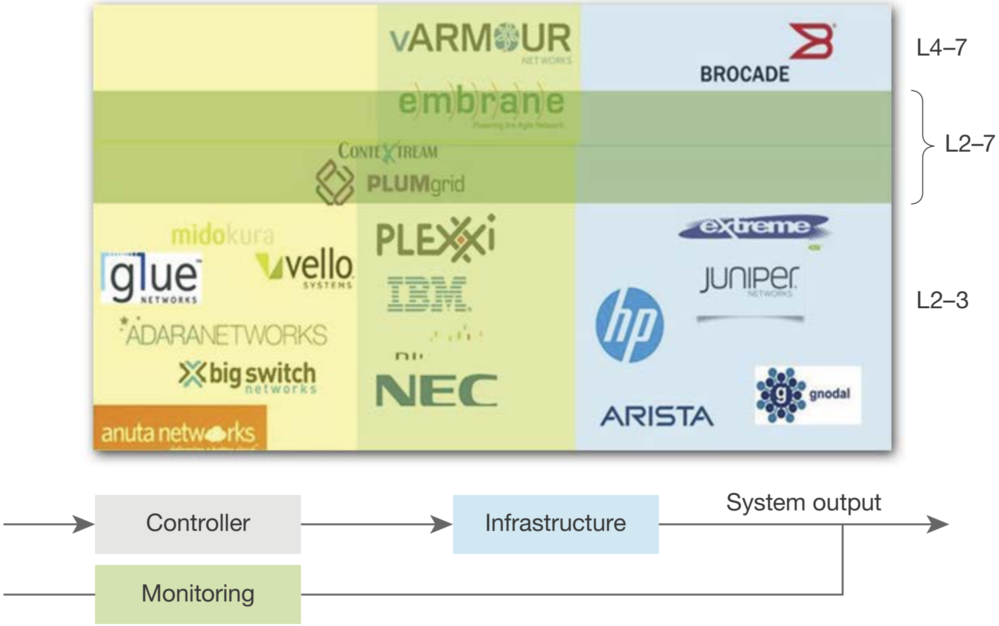
- **. . . and send your configuration data too.** It is also wise to send the configuration data from both hardware and software networks — as well as the segmentation gateway — to a configuration auditing platform that can look for configuration errors or other potential flaws so that each organization might lock down the network more efficiently while maintaining a high degree of usability. Vendors such as AlgoSec, FireMon, RedSeal, Skybox Security, and Tufin have offerings that can provide a significant uplift in this area.

Figure 4 SDN Overlay Solution Rides Over The Complex And Connects Virtual Worlds



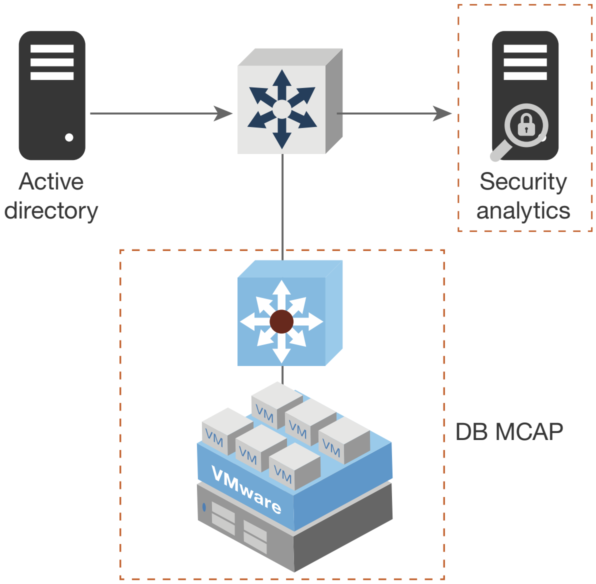
119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 5 Market Taxonomy



119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 6 Example Microcore And Perimeter Integration With Security Analytics



119813 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

RECOMMENDATIONS

USE ZERO TRUST TO DRIVE YOUR 21ST CENTURY NETWORK REDESIGN

Given the changing network and security landscape, many organizations are starting to plan their future network initiatives. For companies looking to leverage NGFWs or VNI, using Zero Trust as a strategic driver is extremely helpful. To get the most out of a Zero Trust project:

- **Talk Zero Trust to the business.** In a post-Target-breach world, executives are concerned about security more than ever before. Zero Trust has been designed to strategically resonate with business leaders while remaining tactically implementable.
- **Engage your application developers and enterprise architects.** Applications drive companies. Breaking down existing silos and planning a 21st century Zero Trust network will help bring all aspects of business technology together in a common goal of building a secure, yet agile, network.
- **Focus on toxic data.** Laws and regulations focus on data, and you should, too. Find your toxic data and build microperimeters around it. Your network and devices are moving outside of your control. Protecting and controlling your data should become your focus. We designed Zero Trust to make your network a very scalable and flexible data control point.

WHAT IT MEANS

A ZERO TRUST NETWORK IS WITHIN YOUR REACH

The transition from hierarchical networks to Zero Trust networks is inevitable. Last century's network is too broken to withstand modern cyberwarfare. Zero Trust networking has been designed to be network- agnostic, thereby positioning it to meet the long-term needs of organizations. Technologies will continue to evolve. New innovations will continue to disrupt. New threats will arise, and new attacks will be launched. In a digital world fueled by data, it's the binary information — the ones and zeros — that will always need to be protected. Because Zero Trust is data-centric, and not network- or device-centric, the key concepts of Zero Trust will always apply. The technological innovations of today — next-generation firewalls, virtual network infrastructure, and orchestration software — make the evolution to Zero Trust easier than ever.

ENDNOTES

[1] Moore's Law is an idea attributed to Intel co-founder Gordon Moore that predicts that the processing power of a computer chip, as measured by the number of transistors on the chip, will double every 24 months while also declining in price. Source: "Moore's Law and Intel Innovation," Intel (http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html).

[2] Not a week goes by without news of network attacks and stolen data. Consumers routinely undergo the stress of fraudulent charges or compromised credit cards. Digital businesses lose millions in stolen intellectual property. Terms such as "botnet" have become part of our vocabulary. To combat the increasing sophistication of cybercriminals, hacktivists, and state-sponsored agents, security and risk (S&R) professionals find themselves on a never-ending quest to maintain the integrity of their extended networks and to protect their firm's most sensitive data. Before investing in yet another point product as part of a failed "expense in depth" strategy, S&R pros must thoroughly understand the technologies, their operational use cases, the required investment, and the potential for long-term market adoption in order to make an informed and educated purchase decision. To learn more, see the "TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015" Forrester report.

[3] Source: "Next-Gen Security Architecture through Brocade Network Devices and Palo Alto Networks Firewall," Brocade Communications Systems (http://community.brocade.com/dtscp75322/attachments/dtscp75322/EthernetSwitchesRouters/208/1/Alliances%20Palo%20Alto%20Networks%20-%20App%20Note%20-%20Next-Gen%20Security%20Architecture%20through%20Brocade%20Network%20Devices%20and%20Palo%20Alto%20Networks%20Firewall.pdf).

[4] Source: "Data Center Micro-Segmentation," VMware (http://blogs.vmware.com/networkvirtualization/files/2014/06/VMware-SDDC-Micro-Segmentation-White-Paper.pdf).

[5] Targeted attacks continue to plague organizations, and these intrusions damage the brand, customer loyalty, and margins. Preparing for and responding to these attacks requires a focused and resolute strategy. We designed Forrester's Targeted-Attack Hierarchy Of Needs to give S&R professionals a framework to accomplish this. To learn more, see the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" Forrester report.

[6] Software-defined networking (SDN) and network functions virtualization (NFV) hold the promise to reposition the network and supporting team from being a business barrier and services liability to an enabler of new business paradigms. However, today's SDN solutions, as outlined in parts 1 and 2 of this series, offer limited value to the majority of infrastructure and operations (I&O) professionals and their enterprises at this point in time. But that doesn't mean that I&O leaders and their teams shouldn't start planning for the inevitable SDN and NFV transition. To learn more, see the "Is Software-Defined Networking Ready For The Enterprise? Part 3 Of 3" Forrester report.

[7] Source: "M-Trends 2015: A View From The Front Lines," Mandiant, 2014 (http://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf).

[8] One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. We call this

"designing from the inside out." If we begin to do all those things together we can have a much more strategic infrastructure. If we look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective. To learn more, see the "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" Forrester report.

[9] Infrastructure and operations (I&O) teams are aligning themselves and infrastructure around key workloads to drive greater simplicity and efficiency. In kind, the networking industry has responded by suggesting that networks can provide greater support for this approach using OpenFlow protocol and software-defined networking (SDN) concepts. SDN provides the means to automate networks to better support different workloads, but I&O professionals also need to understand how SDN can support turning networks into a virtual network infrastructure. To learn more, see the "Workload-Centric Infrastructure Ignites Software-Defined Networking" Forrester report.

[10] Finally, networking has its "cloud." Not since The Beatles touched down at N.Y.'s John F. Kennedy International Airport to perform at The Ed Sullivan Show has there been so much hysteria; yet few understand software-defined networking (SDN) and its components. SDN fanatics theorize that enterprises will embrace this technology/solution because it will open the door for other teams outside networking to harness the network's power, allow the network to automatically flex and efficiently match services to the business' demand, or be an avenue for lowering capital expenditures by moving to white-box switches. Whatever the rationale for SDN, there seems to be one thing everyone agrees on: No one seems happy with their network. To learn more, see the "Is Software-Defined Networking Ready For The Enterprise? Part 1 Of 3" Forrester report.

[11] Zero Trust network abolishes the quaint idea of a "trusted" internal network demarcated by a corporate perimeter. Instead, it recognizes that today's digital businesses must win, serve, and retain customers via new ecosystems of value and systems of engagement unencumbered by physical location. A Zero Trust (ZT) network creates microperimeters of control and visibility around the enterprise's most sensitive data assets and the ways in which the enterprise uses its data to achieve its business objectives. As more security and risk (S&R) professionals embrace and adopt ZT networking principles, there's a need for a defined methodology to help S&R pros build this type of innovative network and realize the benefits of a ZT strategy. To learn more, see the "Five Steps To A Zero Trust Network" Forrester report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

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.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.