Five Common Mistakes When Converging Security and Networking

Table of Contents

Executive Overview

Maintaining today's digital acceleration takes time, effort, and scrutiny. Adding new tools and investments increases the complexity and vulnerability of enterprise security environments, exposing gaps in communication and collaboration, creating siloed systems, and slowing response times. Securing the enterprise against today's increasingly sophisticated threat landscape calls for a cybersecurity platform architecture automated for operational efficiency—a security architecture broad enough to reduce risk across the entire digital attack surface, integrated so security gaps are closed, and automated to increase efficiency and expedite response times.

Introduction

Digital acceleration is driving organizations forward. But for most, it is also stress-testing the underlying networks due to increased complexity resulting from an expanding network and the rapid introduction of new point products and services. And as your network becomes increasingly complex, your organization's ability to manage the network decreases.

But that's not all. Increased complexity not only hinders your ability to manage the network but also impacts its threat detection and response capabilities, increasing its vulnerability to attack. The critical issue is that while your network may be able to support new initiatives, if it's like most networks, it's made up of a collection of individual, siloed networking and security solutions that were never designed to work together. And given today's sophisticated threat environment, the likelihood of a successful attack and data breach is greater than ever.

Requirements for Consolidation

Addressing these new risks and securing these attack vectors requires a consolidated approach. An effective cybersecurity solution designed to provide full protection while reducing complexity should:

- Converge enterprise-grade networking and security solutions into a single device
- Protect the entire attack surface—now and as it expands
- Manage the whole attack cycle, from detection to response
- Support multiple cloud platforms and hybrid-cloud environments with cloud-native security that operates as an extension of the on-premises security posture
- Leverage a single source of threat intelligence across all deployed security technologies
- Monitor and manage all solutions, enabling lean IT teams to scale to meet the organization's security needs

And that's just the start. Reducing complexity goes beyond just having deployed the right technology. It's also about how those technologies work together. And that starts with converging the network with its security infrastructure. And it continues with adopting a platform approach to reduce the number of different vendors needed to complete the solution. The resulting integrated environment minimizes security gaps while providing timely and coordinated preventions and responses across the attack life cycle.

But that's harder than it sounds. Here are five common mistakes organizations make when consolidating their security and networking solutions and strategies.

Mistake #1: Trusting too much

The legacy, perimeter-based security model has been turned on its head, with “trusted” devices deployed outside the network perimeter while “untrusted” ones roam freely inside it. Hybrid users on- and off-premises need free access to the network and its resources from anywhere. Without more stringent policies and consistently enforced controls, the risk of a successful breach increases exponentially—especially as users, applications, and workflows move across and between the various segments of your distributed network.

A zero-trust security model means no user or device is trusted by default. Instead, access to resources is granted or denied based on the user’s identity, and permissions are assigned based on the duties, responsibilities, and functions of users and devices. Zero-trust principles mitigate the risk of malicious or vulnerable devices and users, especially now that the perimeter has expanded and splintered in the work-from-anywhere world while endpoints have multiplied exponentially.

Properly implementing and enforcing a zero-trust security model begins with strong network segmentation and access control. Your security architecture should be able to automatically identify devices connecting to the network, securely authenticate the user, and provide or deny access to network resources based on the permissions associated with that user's account.

Internal network segmentation limits the lateral movement of attackers and malware, decreasing the impact of a data breach. Whether applications are on-premises or in the cloud, users and applications can be geographically independent and still create secure and reliable connections to critical resources without inadvertently compromising the rest of the network.

Application access is another critical component. Zero-trust network access (ZTNA) is built using a variety of tools—client, application gateway, policy engine, authentication, security—but when provided by different vendors using different operating systems and management and configuration consoles, establishing a successful ZTNA solution is almost impossible.

"The shift from implicit trust to zero trust is a response to the rising incidents and costs of cybercrime... A robust implementation of zero-trust solutions can reduce the likelihood of attack."[1]

Mistake #2: Evaluating cloud platforms and security solutions in a silo

Organizations struggle to establish and maintain consistent security policies and enforcement across multi-cloud hybrid environments. Trying to deploy security across such complex environments introduces challenges many IT teams can find overwhelming, such as maintaining consistent security controls, managing and optimizing application access, and maintaining overall performance. This is especially true when multiple solutions from different vendors are being used.

The most significant risks in multi-cloud deployments are caused by sprawl, bolted-on (non-native) security, and misconfigurations. Hybrid-cloud deployments outside your network perimeter but accessible from the public internet can also result in unauthorized access issues.

To fully capitalize on the promises of the cloud, your security solutions must support the effective use of cloud resources, such as auto-scaling, be environment-aware to provide necessary granularity, ensure consistent features and enforcement in any cloud environment, and be truly cloud native across all major cloud platforms.

Multi-cloud environments also require coordinated detection and enforcement across the digital attack surface to enable quick responses to threats. This means that security solutions you have deployed in different platforms not only need to provide cloud-native functionality but also share threat intelligence between clouds to deliver consistent, context-aware security that can assess and automatically adjust to risks. This also enables security policies to follow applications and workflows that span clouds, ensuring that protections are consistently enforced end to end.

Most organizations (72%) are pursuing a hybrid or multi-cloud strategy for integration of multiple services, scalability, or business continuity reasons."[2]

Mistake #3: Focusing on prevention instead of time-to-detect

Cybercriminals increasingly use targeted attacks to exploit network vulnerabilities and misconfigurations. Their well-orchestrated campaigns give cyber-defenders a limited window for disrupting an attack sequence. And manual detection and response just can't keep pace with automation, cloud scale, and artificial intelligence (AI) used to launch sophisticated attack that target distributed perimeters.

To protect your organization against today's high-speed attacks—including quick-changing polymorphic malware—your security posture must be able to "reprogram" itself in real-time to break the attack sequence before it is successful.

To determine if your security system is up to the task, you need to assess five things:

1. Its ability to quickly move from detecting a threat to launching a customized defense across your distributed environment.

2. The accuracy and speed of its detection capabilities.

3. It can generate new preventions across the attack cycle, automatically distribute them across the different technologies and devices, and strengthen existing prevention capabilities.

4. Its participation in global and community threat intelligence sharing so you are never a “second” Patient Zero.

5. The quality of its AI and machine learning (ML) capabilities (if any).

Robust cybersecurity leverages cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application protection across the environment. The strategic use of AI is essential to coordinated prevention, detection, and response across the digital attack surface and life cycle across edges, clouds, endpoints, and users.

ML capabilities are just as crucial. A well-trained ML classifier can differentiate genuine threats from false positives, allowing security teams to focus investigations and remediation efforts on real attacks. Inline solutions leverage ML to automatically detect threats based on behavioral anomalies and respond using predefined playbooks. Machine learning can also aid data collection and analytics, providing threat hunters and security operations center (SOC) analysts with the information they need to rapidly detect and respond to advanced, quick-moving attacks.

Mistake #4: Expanding connectivity without converged security

Organizations are accelerating their digital plans so they can be more agile and adaptive. But while today's networks are designed to be highly agile, most traditional security approaches are not. When networks adapt to changing requirements, entire network segments can be left unprotected. Because of this need for adaptability and scalability, the network and its underlying security infrastructure can no longer be deployed as separate entities layered on top of each other. What you need is a solution that converges security and networking functions into a single, integrated system that can be deployed in any number of form factors.

Unfortunately, to manage their various network environments and the growing array of devices on their networks—and their associated cyberthreats—many organizations have deployed a vast array of standalone security products that are not integrated into the existing infrastructure and do not interoperate. This makes them difficult or impossible to monitor or manage and makes automation impossible. Compounding this problem further, some have even deployed solutions from different vendors to protect their various hardware, software, and cloud use cases.

Cybersecurity product consolidation is transforming security buying. According to Gartner, “75% of organizations actively pursued vendor consolidation in 2022, compared with only 29% in 2020.”[3]

Mistake #5: Not implementing a complete ecosystem

No single vendor will ever have every technology you need when you need it. Likewise, no one can singlehandedly address all the requirements for countering today's threat landscape. The remedy is selecting a solution—usually a platform—that can easily integrate with the rest of your security ecosystem, including solutions from third-party vendors via application programming interfaces (APIs), connectors, and DevOps automation tools and scripts. This allows you to create a unified front for prevention, detection, and response to protect your extended digital attack surface.

An open API architecture enables communication and synchronization between devices from different vendors. Custom-built connectors provide an even higher level of integration and interoperability, allowing real-time communications and automatic updates across the ecosystem. And a library of purpose-built DevOps tools and scripts enables rapid, customizable deployment and management, thereby scaling the capabilities of lean security teams. This integrated security architecture approach uniquely provides consistent protection and connections across every network edge, no matter where they reside or how often they change.

Beyond interoperability is the need to coordinate and collaborate with threat intelligence partners, research organizations, and other cybersecurity and networking vendors. Organizations such as FortiGuard Labs collaborate with the global intelligence community to share industry best practices and impede the spread of attacks, protecting businesses against millions of events. Vendors themselves need to step outside of their self-interest and collaborate with the global intelligence community, sharing best practices and threat research to impede the spread of attacks. Working together expands visibility and threat detection and enables coordinated response, enabling organizations to compete effectively, and securely, in today's digital marketplace.

Conclusion

With change being the only constant, especially given the rapid consumption of innovations being added to existing environments, simplicity and adaptivity are vital. As your network grows more complex and heterogeneous, you need a consolidated cybersecurity platform to simplify and optimize your prevention, detection, and response capabilities. This ensures unified visibility across the entire digital attack surface, closes security gaps, and reduces complexity, all while speeding up operations and incident responses.

Optimized digital experience requires building and maintaining trusted, high-performing connections between users, devices, and applications across diverse and global environments, including hybrid-cloud configurations. Consolidating silos is simply not enough for this to work. Network and security convergence, vendor consolidation, and partner collaboration are the answer. Avoiding these five mistakes when evaluating your next security investment will help close security gaps, unify siloed systems, speed response times, and ensure your security can grow and adapt with your business.

[1] Fortinet, The State of Zero Trust Report, 10 January, 2022.

[2] Cybersecurity Insiders, 2022 Cloud Security Report, January 2023.

[3] Menghan Xiao, Security Week, "Security vendors report economic hit as they struggle to lure newer customers," March 8, 2023.

FORTINET

www.fortinet.com

June 6, 2023 2:20 PM

914666-B-0-EN