5 Mistakes To Avoid When Evaluating Your Next Security Investment

Table of Contents

Executive Overview

Keeping pace with today's digital innovations takes scrutiny, time, and effort, especially when integrating any new technologies into your organization. Adding new tools and investments increases the complexity and vulnerability of enterprise security environments. New software and services can cause unwieldy heterogeneity, exposing gaps in communication and collaboration, creating siloed systems, and slowing response times. Securing the enterprise against next-generation cyber threats calls for a unified, integrated security architecture, automated for operational efficiency—a security architecture that is 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

Today's always-on, connected organizations combined with rapid cycles of digital innovations create a great influx of connected devices as well as application and content consumption models. The explosion of connected devices has splintered the security perimeter, causing gaps in visibility, manual IT management burdens, and more attack vectors targeting new edges. The introduction of Internet-of-Things (IoT) devices and the addition of cloud-based data storage and applications, mobile devices, new branch locations, and their commensurate hybrid users introduce unique security vulnerabilities, complexities, and risks. Security device and vendor sprawl introduce even more gaps, allowing attack sequences to go undetected. And when they are detected, enforcement and responses lag behind.

At the same time that the networks and their corresponding digital attack surfaces expand, cyberattacks become more automated, sophisticated, and granular, leveraging cloud scale and automation as they target known and newly created gaps in security postures. Evolving attack techniques, some with polymorphing attack components capable of targeting multiple edges simultaneously, aim for these vulnerable targets.

Addressing these new risks and securing these attack vectors require a more unified security solution. Forward-looking security postures should:

- Cover the full attack surface and easily expand to include new edges
- Manage the full attack cycle detection to enforcement
- Aim to have singular context-aware security policy across
- Support multiple provider and hybrid cloud environments with cloud-native security
- Assess risks and automatically make adjustments to the security posture for timely prevention
- Monitor and manage all solutions, enabling lean IT teams to scale to meet the organization's security needs

Context-aware high-performing security embedded into the connectivity and compute layers is critical for the success and ease of the digital innovation journey. Creating a unified, self-healing environment across the full connection—device and users to applications—minimizes security gaps and provides timely and coordinated preventions and responses across the attack life cycle.

Mistake #1: Trusting too much

With “trusted” devices now deployed on the outside of an organization’s network perimeter and “untrusted” ones often roaming freely inside it, a legacy, perimeter-based security model isn’t effective in today’s security climate. Hybrid users working on- and off-premises, in public and private clouds, need free access to the network and applications. Meaning even more stringent access permissions.

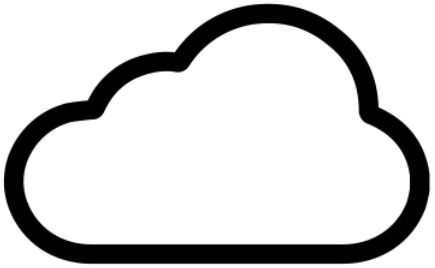
Best practices dictate a zero-trust security model, meaning no user or device is trusted by default. Instead, access to resources is granted or denied based upon the user’s identity, and permissions are assigned based on that user’s duties and responsibilities. Zero-trust principles mitigate the risk of malicious or vulnerable devices and users, especially now that the perimeter has expanded and splintered in the work-from-home world, and endpoints have massively multiplied. Implemented correctly, zero trust mandates access to real-time threat intelligence to detect and respond to accelerating and sophisticated cyberattacks, with even more capabilities for prevention of lateral movement and abuse of permission.

With multiple ways to access and consume data in multi-cloud environments, implementing and enforcing a zero-trust security model requires strong network segmentation and access control. The organization’s security architecture should be able to automatically identify devices connecting to the network, securely authenticate the user, and provide or deny access based on the permissions associated with that user’s account.

A strongly enforced zero-trust security policy also requires internal network segmentation, which limits lateral movement of attackers and malware and decreases the probability and impact of a data breach. It doesn't matter if applications are on the network or in the cloud—users and applications can be geographically independent and still create secure and reliable connections.

Building a zero trust network access (ZTNA) solution takes this approach and applies it to application access. This requires leveraging a variety of components, such as a client, a proxy, authentication, and security. This is even harder than it sounds, because in most organizations, these components are provided by different vendors, so they run on different operating systems and use different consoles for management and configuration. This makes establishing a successful zero-trust network access model across all of those vendors almost impossible.

More than 94% of organizations have adopted cloud computing, and 84% of them have multi-cloud deployments.[1]



Organizations leverage almost 5 different cloud platforms on average.[2]

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

Organizations struggle to ensure consistent security policy and enforcement across multi-cloud environments. Managing multi-cloud security with custom solutions is complex and makes it difficult to maintain consistent security controls, manage and optimize application access, and maintain overall performance across the corporate wide-area network (WAN). This is even more true when multiple solutions from multiple vendors are used across the various instances.

The most significant risks in multi-cloud deployments are caused by sprawl and security bolt-ons and misconfigurations. Hybrid cloud deployments located outside the network perimeter and accessible from the public internet can cause unauthorized access issues.

In order to fully capitalize on the promises of the cloud, security capabilities need to support effective usage of cloud resources with features like auto scaling, and be environment-aware to provide the granularity needed to integrate and be truly cloud native across multi-cloud deployments.

An integrated security configuration management solution is therefore essential for cloud security. Multi-cloud environments need coordinated detection and enforcement across the digital attack surface to enable quick responses to threats that take advantage of security misconfigurations. Hybrid cloud applications that reside in disparate cloud environments require cloud-native, consistent, context-aware security solutions that assess and automatically adjust to the risks following the data.

Mistake #3: Focusing on detection instead of time to prevention

Cyber criminals are increasingly using automated and targeted attacks. These well-orchestrated campaign sequences give cyber defenders a limited window in which they can disrupt the attack sequence, meaning detection and response. When these attackers leverage automation, cloud scale, and artificial intelligence (AI) to sequence even more sophisticated and polymorphing attack components across splintered perimeters, manual detection and response just can't keep pace.

In order to effectively protect an organization against the latest, fast-moving attack tactics, you need to be able to "reprogram" your security posture in time to break the attack sequence before it is successful. This means evaluating your security ability to move from detection to launching new defense across your environments. This will include evaluating the detection capabilities for accuracy and speed. And it should not stop there. Look into unified datasets that allow for holistic detection vs. symptom-based detection. Evaluate the quality of the AI, and look into global and community threat-intelligence sharing, so you are never a "second" Patient Zero. And most important, evaluate the ability of the solution to generate new prevention across the attack cycle, and automatically distribute them across the different technologies and devices. This is the moment that your defense starts.

Second, your security team must have real-time access to the most recent threat intelligence. A well-trained machine-learning (ML) classifier can differentiate true threats from false positives, so security teams can focus their investigations and remediation efforts on real attacks. These classifiers can be integrated into a wide range of security solutions. Solutions deployed in-line can also automatically detect threats based on behavioral anomalies and respond using predefined playbooks. ML can also be used to 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 and quick-moving attacks.

A robust network and security posture 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 detection, prevention, and response across the digital attack surface and life cycle with converged networking and security across edges, clouds, endpoints, and users.

Mistake #4: Expanding connectivity without native security

To manage the growing array of devices on their networks and the cyber threats associated with them, many organizations deploy a range of unintegrated ("point") security products that are difficult to monitor or manage, some will even have different vendors across hardware, software, and X-as-a-Service for the same use case. This increases the complexity of securing network environments.

Cloud-based applications are essential for businesses to run and enable digital innovation. This is expanding the network and creating new network edges. Companies have to be agile and adaptive so that application availability and the user experience are consistent, regardless of where they are working. And although today's networks are designed to be highly agile, most traditional security solutions are not. That means that an adaptive cloud network environment may leave critical resources and data unprotected while security solutions are focused on keeping up with the momentum. The remedy is to look for a solution that converges security and networking functions into a single, integrated system that can expand to any edge.

Look for consistency across deployment models that in turn will allow you to mix and match hardware, software, and X-as-a-Service offerings into a singular security posture. High availability (HA) through leveraging 5G and Long-Term Evolution (LTE) technologies, as well as shifts to software-defined WAN (SD-WAN) for better utilization of resources and total cost of ownership (TCO), should be included in your consideration. This will ensure the adaption of new offerings through the journey of digital innovation is smooth for you and your teams.

32%

of IT leaders say that a reliance on “too many manual processes” is a leading security challenge.[3]

Mistake #5: Not including your full ecosystem

One of the major challenges with rapidly expanding the network edge is that many of the technologies needed to make things work don't work together. Most cybersecurity solutions aren't even aware of one another, and this lack of integration and the resulting complexity slows security teams and provides attackers with open opportunities to exploit. Making matters worse, much of the digital innovation progress to date has been piecemeal, without a unifying security strategy or framework. As a result, most organizations have accumulated a wide variety of isolated security tools designed to protect a function or one segment of the network in isolation. This lowers visibility and restricts control, leading to missed threats and ineffective responses.

One way to help is to coordinate and collaborate with threat-intelligence partners, research organizations, and vendors. Organizations such as FortiGuard Labs collaborate with the global intelligence community to share industry best practices and impede the spread of attacks. This community works hard to see and protect businesses against millions of events, whether from global fabric deployments or from partners preventing a "second" Patient Zero for community known threats. Working together helps provide unification of visibility, detection, and coordinated responses.

The remedy is a solution that can easily integrate with the rest of your deployment to form a unified front for detection and response natively, and through a rich ecosystem designed to span the extended digital attack surface. A new-generation protection solution should also be capable of integrating with a wide range of third-party vendor solutions via application programming interfaces (APIs), connectors, and DevOps automation tools and scripts.

An open API architecture enables communication and synchronization among different devices. Custom-built connectors provide a higher level of integration and interoperability, allowing real-time communications and automatic updates across the ecosystem. A library of DevOps tools and scripts enables rapid, customizable deployment and management, scaling the capabilities of lean security teams. This type of integrated security architecture can provide consistent protection and connections across every network edge, no matter where they reside.

35% of IT leaders rely upon nonintegrated security architectures.[4]

Conclusion

With change being the only constant and rapid consumption of new innovations that are added to an existing environment, simplicity and adaptivity are key. As networks continue to grow more complex and heterogeneous, organizations require a broad, integrated, and automated security platform to simplify and optimize incident detection, prevention, and response. This enables unified visibility across the entire digital attack surface, closing security gaps, and reducing complexity while speeding operations and incident responses.

A successful digital experience provides trusted, high-performing connections between users, devices, and applications, across diverse and global environments and cloud configurations. Consolidating silos is simply not enough for this to work—network and security coordination, unification, and convergence together with partner collaboration are the answer. Avoiding these five mistakes when evaluating your next security investment will help close security gaps, unify siloed systems, and speed response times.

[1] "RightScale 2019 State of the Cloud Report from Flexera," Flexera and RightScale, February 27, 2019.

[2] Nick Galov, "Cloud Adoption Statistics for 2021," Hosting Tribunal, January 19, 2021.

[3] "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[4] Ibid.

www.fortinet.com

March 8, 2021 3:01 PM

5-Mistakes-to-Avoid-eBook

914666-0-0-EN