
NUTANIX
YOUR ENTERPRISE CLOUD
MODERNIZING YOUR INFRASTRUCTURE?
Here's Why
You Should Take a
SECURITY-FIRST
Approach

Content

INTRODUCTION:

SECURITY IS EVERYONE'S PROBLEM

"The number of cyberattacks doubled in 2017, making it the worst year ever for data breaches and cyber incidents around the world. With the majority of incidents not being reported, the Online Trust Alliance estimates that the actual number could exceed 350,000."

Source: "Cyber Incidents and Breach Trends Report," Online Trust Alliance, January 25, 2018.

It should be news to no one that the number of cyber attacks and data breaches continues to rise. More than three-quarters of organizations have been victims of one or more successful cyber attacks.

What about your business? How well are you protecting it against the onslaught of threats?

Don't stop reading just because your job title doesn't have the word security in it. Worrying about cyber threats is not only the job of the chief information security officer and the security team. The fact is that cybersecurity is everyone's responsibility, including recommenders and decision makers for IT infrastructure.

Why is that? Read on to discover how and why the infrastructure you choose impacts your ability to protect your business from cyber threats. You'll learn how a security-first infrastructure can improve your security posture to better protect your business from attack by today's cybercriminals.

[1] "2018 Cyberthreat Defense Report," CyberEdge Group, 2018.

IS YOUR ORGANIZATION NEXT?

77%

OF ORGANIZATIONS HAVE BEEN VICTIMS OF ONE OR MORE SUCCESSFUL CYBER ATTACKS

Source: "2018 Cyberthreat Defense Report," CyberEdge Group, 2018.

45%

INCREASE IN DATA BREACHES REPORTED IN 2017 COMPARED TO 2016

Source: "2017 Annual Data Breach Year-End Review," Identity Theft Resource Center, 2018

14,712

COMMON VULNERABILITIES AND EXPOSURES (CVES) PUBLISHED BY MITRE IN 2017

Source: Common Vulnerabilities and Exposures List, The MITRE Corporation

$3.86

MILLION IS THE AVERAGE TOTAL COST OF A DATA BREACH

Source: "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute LLC, Sponsored by IBM Security, July 2018.

COMPLEX INFRASTRUCTURE COMPOUNDS SECURITY CHALLENGES

AS APPLICATIONS AND INFRASTRUCTURE HAVE EVOLVED — FROM LEGACY TO VIRTUALIZED TO CLOUD-NATIVE — THEY'VE CREATED ADDITIONAL LAYERS OF COMPLEXITY AND RISK. HERE'S WHY:

MULTIPLE VENDORS

For many companies, the data center infrastructure includes one or more technology stacks of different computing, virtualization, storage, and networking solutions. Often, stacks include products from multiple vendors.

MULTIPLE APPROACHES

Each one of those vendors has a narrow, fragmented view of the infrastructure stack, with an even narrower view of security. A storage vendor may be focused on security within the context of the vendor's solution, but not within the context of the entire infrastructure. A virtualization vendor looks only at its virtualization solution and related security implications. And so on …

MULTIPLE SECURITY GAPS

The infrastructure silos that result from this complex environment mean that it's the responsibility of your business to resolve the security gaps and incompatibilities that arise across all of your various component vendors. The burden to maintain adequate security at the infrastructure level becomes more than most companies can handle — there simply aren't enough cybersecurity experts available to constantly upgrade software, patch vulnerabilities, confirm security configurations, and perform other related tasks across the complex IT infrastructure.

Current cybersecurity efforts aren't good enough

89% of respondents in a global survey say their cybersecurity function does not fully meet their organization's needs.

Source: "Cybersecurity regained: preparing to face cyber attacks," EY, 2017.

WHAT PERIMETER? WHY SECURITY MODELS MUST EVOLVE

When the data center was well-defined, static, and primarily made up of physical hardware, securing the perimeter was a reasonable approach to protecting the business against cyberattacks. However, virtualization, cloud computing, mobile devices, and the Internet of Things have all contributed to the dissolution of the perimeter.

Today, much of the traffic moves laterally inside the data center compared with traffic that travels in and out of the external network. Traditional security solutions such as firewalls are often blind to the internal communication between virtual machines and applications. Once cybercriminals infiltrate the network, they can take up residence and move laterally without being detected.

COMPLEX INFRASTRUCTURE + TRADITIONAL SECURITY APPROACHES = INCREASED RISK

- **Security holes:** Add-on infrastructure products and manual efforts to implement and maintain them increase complexity without resolving all the security gaps.
- **Software upgrade delays:** Validating and maintaining a security baseline through software upgrades is time-consuming and often involves error-prone manual processes.
- **Lack of viable alternatives:** Although multi-product strategies can mitigate many threats, most alone have proven to be too complex and resource-intensive to be practical in a traditional, multivendor infrastructure stack.

Security errors are a top risk

Miscellaneous errors were the second most cited reason for a data breach, after web applications.

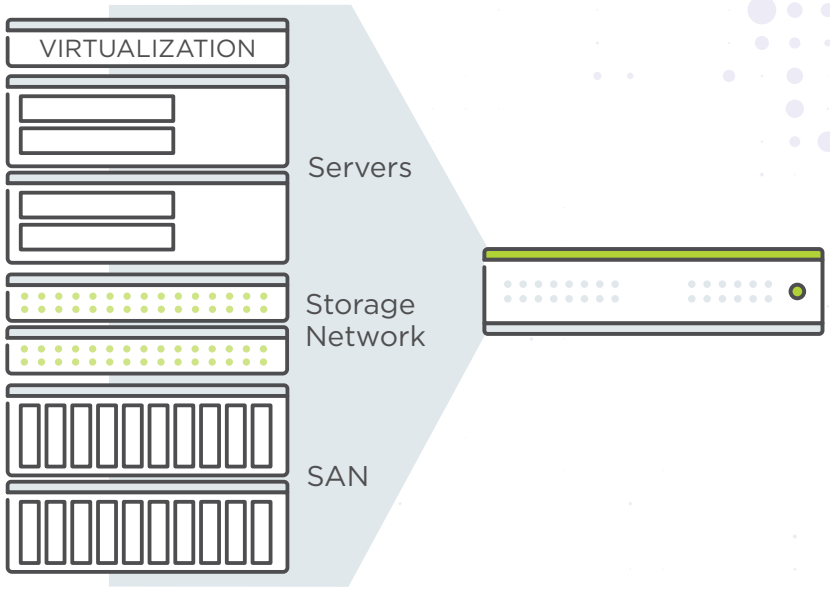
Source: "2018 Data Breach Investigations Report," Verizon.

For all the reasons discussed — heterogeneous environment, complexity, security gaps, dissolving perimeters, manual software upgrades, and more — the most effective security approach for today's data center begins with a platform developed with the philosophy of "security first."

What does a security-first infrastructure platform look like? It's a single, fully tested platform with security at its core — and simplicity as its cornerstone. By combining storage, computing and networking into a single platform, a security-first infrastructure platform can improve security and control through:

- Security best practices and standards that are "baked" into the software-defined infrastructure throughout the development lifecycle
- Built-in functionality for security and compliance, including role-based access control, multifactor authentication, encryption, and other capabilities
- Automation and self-healing to maintain security baseline configurations without manual intervention
- An application-centric approach for improved threat protection Integration and support of third-party security solutions for defense in depth and a holistic approach to security

ORGANIZATIONS NEED A BETTER APPROACH TO CYBERSECURITY



An infrastructure that simplifies operations and security
A hyperconverged infrastructure (HCI) is software-defined with no dependency on proprietary hardware and combines storage, computing, and networking into a single system to:

- Greatly simplify operations and security
- Lower total cost of ownership (TCO)
- Accelerate agility and time to value
- Deliver greater scalability and performance

REQUIREMENT #1:

A BATTLE-HARDENED SOFTWARE DEVELOPMENT LIFECYCLE

A single platform built using a security mindset can close the gaps created by the complexity of infrastructure silos. To do so, security considerations must be a core component of every step of the infrastructure lifecycle — from product development and deployment, through routine monitoring and remediation — and cover the entire infrastructure stack, including storage, virtualization, and management.

When a vendor uses a robust security development lifecycle, security is incorporated into product development from the start, avoiding difficult tradeoffs later in the lifecycle between security and performance or features. For example, research and development teams work together to fully understand all the code in the platform, whether it is built in-house or inherited from dependencies.

Tests for Common Vulnerabilities and Exposures (CVE) should be included in the product's quality assurance process. The vendor should schedule regular updates to address known CVEs for minor release cycles to minimize zero-day risks without slowing down product evolution.

REQUIREMENT #2:

BUILT-IN SECURITY BEST PRACTICES AND CAPABILITIES

Infrastructure-level security with a hardened platform helps you protect against various types of cyberattacks, including data breaches, unauthorized access, and other threats.

1. **Protection for data-at-rest:**
   Safeguard sensitive user and application data from theft or loss with self-encrypting drives or software encryption that meets regulatory compliance requirements for your industry, including HIPAA, PCI DSS, and others.

2. **Role-based access control:**
   Restrict access to the infrastructure and sensitive data using role-based access control to reduce the risk of unauthorized access and comply with regulatory requirements.

3. **Identity and authentication mechanisms:**
   Prevent account takeovers and mitigate the risk of compromised credentials by using SAML 2.0 authentication mechanisms for single sign-on and multifactor authentication for system administrators. According to Neil MacDonald, Gartner vice president, "At a minimum, CISOs should institute mandatory multifactor authentication (MFA) for all administrators."[1]

Attackers at the gates
73% of cyberattacks are perpetrated by outsiders, with members of organized criminal groups behind half of all breaches.

Source: "2018 Data Breach Investigations Report," Verizon

[1] "Gartner Top 10 Security Projects for 2018," Gartner, June 6, 2018.

REQUIREMENT #3:

AUTOMATION AND SELF-HEALING

Given the dynamic and complex nature of today's technology landscape, it's become nearly impossible to maintain adequate security measures using human efforts alone. That's why automation has become a must-have capability for successful cybersecurity efforts.

At the infrastructure level, automation accelerates software validation and upgrades while significantly limiting the risk of reducing the security posture because of human error. With self-healing capabilities and automation built into a single, hardened platform, the upgrade process for all system software becomes non-disruptive and effortless so that IT teams don't postpone regular updates.

For example, a single, hardened infrastructure solution should include:

- **Automatic validation of security baselines:** When deploying infrastructure and continually protecting it from inadvertent or malicious changes, security baselines (developed from industry and U.S. Department of Defense standards) help vendors harden the infrastructure from the "factory." Making the baseline compatible with automated assessment tools accelerates accreditation time.
- **Automatic configuration management:** Automate periodic monitoring for unknown or unauthorized changes to configurations and self-heal the infrastructure from the baseline deviation to remain in compliance.
- **Network automation:** Streamline and automate common network configuration changes, like VLAN configuration or load balancer policy modifications, based on application lifecycle events for virtual machines.

Failing the cybersecurity readiness test
A global survey conducted by Forrester Consulting evaluated participating companies on cybersecurity readiness (quality of strategy and execution) and found that 73% rank as cyber novices, with a long way to go before they reach the cybersecurity expert levels.

Source: "2018 Hiscox Cyber Readiness Report," Hiscox.

[2] "Gartner Top 10 Security Projects for 2018," Gartner, June 6, 2018.

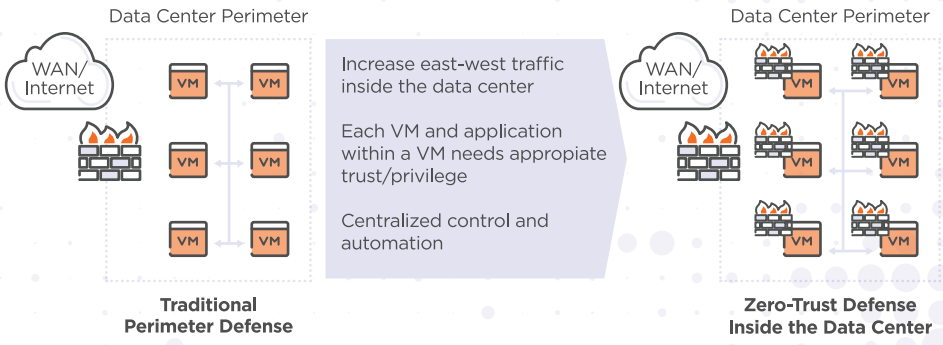
REQUIREMENT #4:

APPLICATION-CENTRIC SECURITY

Historically, deploying microsegmentation has been a daunting effort, requiring manual analysis of lateral data center traffic, contextual understanding of each application, and time-consuming mapping of application workflows to identify logical groupings for segmentation. Despite the clear benefits of this security best practice, the challenges of implementing microsegmentation has limited its impact and reach.

Application-centric security in a single, hardened platform significantly reduces the complexity of using microsegmentation to protect against internal and external threats not detected by perimeter-oriented security products. Here's how:

- **Visualization:** By showing application traffic, performance, and availability, you get complete visibility into and understanding of workload behavior, allowing you to quickly identify logical connections and inform the appropriate application-centric policies.
- **Grouping:** Categorizing virtual machines and applications based on use case, compliance need, or data sensitivity — instead of dynamic network identifiers such as IP addresses — simplifies the process of protecting and isolating sensitive workloads and data.
- **Granular policy:** Granular policy controls let you define multitiered applications and then restrict or allow traffic to and from, as well as within, the application tiers.



The Zero Trust model and microsegmentation

Zero Trust is a security concept created by John Kindervag, former principal analyst at Forrester Research. The idea is centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify everything trying to connect to its systems before granting access.

One of the enabling capabilities of Zero Trust is microsegmentation, a way to create secure zones to isolate applications and workloads and protect them individually. By applying segmentation rules to the workload or application, IT can reduce the risk of an attacker moving from one compromised workload or application to another.

REQUIREMENT #5:

DEFENSE IN DEPTH THROUGH ECOSYSTEM PARTNERS

Obviously, security measures shouldn't stop at the infrastructure level. To avoid security gaps, single platforms need to integrate with third-party security solutions to create a holistic, defense-in-depth approach.

This requires the vendor to support a robust ecosystem of validated solutions from third parties, such as data and endpoint security solutions. One way for the infrastructure platform to integrate with third-party services is via service chaining of network functions.

What is service chaining? It's a capability that lets you leverage virtualized network functions from third-party software.

How does it work? Services are inserted in line with virtual machine traffic and can be easily enabled for all traffic, or deployed only for specific network traffic.

What are some examples? Common network functions that can be inserted include: virtual firewall, network threat detection (i.e., IPS/IDS), application performance monitoring (APM), or general application network diagnostics.

TOP 5 INDUSTRIES EXPERIENCING DATA BREACHES

2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute LLC, Sponsored by IBM Security, July 2018

START WITH A SECURITY CHECKLIST FOR INFRASTRUCTURE DECISIONS

It's clear that IT infrastructure plays a critical role in cybersecurity. That's why every infrastructure decision should include security as a non-negotiable core tenet. It should not be an afterthought, nor should it be limited to whether a vendor meets a particular standard or not. The stakes are high, and companies need every advantage to prevent cybercriminals from wreaking damage.

Insist on the following when choosing a robust, security-hardened infrastructure platform:

- ✓ Full-stack security development lifecycle
- ✓ Out-of-the-box hardened platform with security best practices built-in
- ✓ Automated validation and self-healing of baselines
- ✓ Detailed security documentation for auditors and infrastructure architects
- ✓ Application-centric security capabilities
- ✓ Robust and growing security ecosystem
- ✓ Built to address common security certifications and standards
  - Common Criteria Certified
  - FIPS 140-2 Validated Data Encryption Modules
  - NIST-SP800-131A Compliant
  - NSA Suite B Support
  - Section 508 VPAT Compliant
  - TAA Compliant

"Business leaders and senior stakeholders at last appreciate security as much more than just tactical, technical stuff done by overly serious, unsmiling types in the company basement. Security organizations must capitalize on this trend by working closer with business leadership and clearly linking security issues with business initiatives that could be affected."

Peter Firstbrook, research vice president at Gartner, "Gartner Identifies the Top Six Security and Risk Management Trends," July 3, 2018.

LEARN MORE

MAKE CYBERSECURITY A CRITICAL PART OF YOUR NEXT INFRASTRUCTURE DECISION. LEARN MORE ABOUT HOW NUTANIX CAN HELP YOU IMPROVE YOUR COMPANY'S SECURITY POSTURE.

ADDITIONAL RESOURCES:

- Nutanix Flow – www.nutanix.com/products/flow
- Acropolis Platform Security – www.nutanix.com/products/acropolis/security
- Cloud Security and Compliance – www.nutanix.com/products/beam/cloud-security-compliance

About Nutanix

Nutanix is a global leader in cloud software and hyperconverged infrastructure solutions, making infrastructure invisible so that IT can focus on the applications and services that power their business. Companies around the world use Nutanix Enterprise Cloud OS software to bring one-click application management and mobility across public, private and distributed edge clouds so they can run any application at any scale with a dramatically lower total cost of ownership. The result is organizations that can rapidly deliver a high-performance IT environment on demand, giving application owners a true cloud-like experience.

Learn more at **www.nutanix.com** or follow us on Twitter **@nutanix**.

NUTANIX™

YOUR ENTERPRISE CLOUD