NUTANIX™

YOUR ENTERPRISE CLOUD

Application-Centric SECURITY

Content

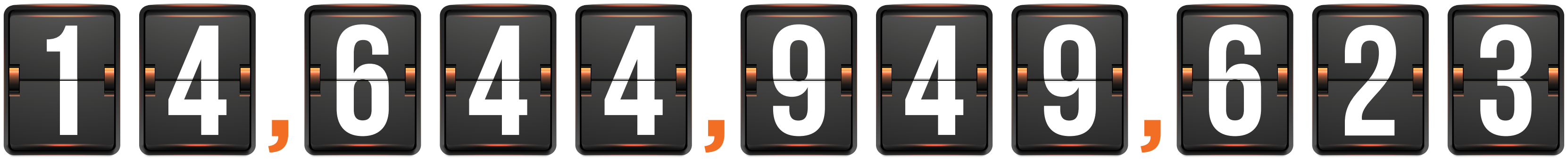


Figure 1
Source https://www.breachlevelindex.com/. Every month the number of security breaches increases. Cyber criminals are targeting high value data with sophisticated attacks designed to bypass perimeter-based controls. Once inside the corporate network, attackers can be free to move from one system to another, in search of sensitive or personally identifiable information. These breaches can go unnoticed for weeks or even months.

The State of Data Center Security

The state of security today can be summed up in one word: **more**. More security breaches. More sophisticated threats. More cyber risk. More business-critical technologies. More regulatory requirements. More growth. More complexity. And none of it looks to be waning any time soon.

Meanwhile, the data center continues to evolve at an increasingly rapid rate as IT organizations struggle to fulfill their mission and be responsive to business needs that are evolving just as fast. The adoption of Software-as-a-Service, cloud-based infrastructure, and virtualization increases the complexity of the data center while flattening the IT architecture and making it easier for attackers to move laterally across these pools of resources and harder for IT teams to know where to place security controls.

Amidst all this rapid change, the approaches to security are struggling to keep up. Organizations continue to practice more traditional methods of protecting the IT environment with a focus on infrastructure – for example, implementing network segmentation via perimeter firewalls. Perimeter-based security traditionally only protects the environment from external threats, and it can be difficult to leverage them to restrict internal traffic or prevent laterally spreading attacks.

It's time for a new approach that considers the organization's need to protect traffic behind the perimeter firewall in a manner that delivers more: more agility. More flexibility. More security. More protection. That's exactly what IT organizations achieve when they adopt an application-centric approach to security with microsegmentation.

> “Data is a pervasive asset that crosses traditional boundaries on-premises and into cloud services. Every business needs a data-centric security strategy to prioritize datasets for mitigation of growing business risks caused by data protection and privacy laws, hacking, fraud, and ransomware.”
>
> – Gartner – Hype Cycle for Data Security, 2018

Application-centric Security Policy

Application architecture has changed dramatically over the last five-to-ten years. Applications have evolved from running on a single server to an abstract collection of virtual machines (VMs) and services (such as SaaS, microservices, and containers) that deliver the application. To further complicate matters, those services and VMs may not all run from the same location. Traditional approaches mostly require policy to be written in terms of the network (e.g., an IP address), and in today’s dynamic datacenter, this requirement makes policy management a frequent and painful process.

The good news is that virtualization’s dominance in the datacenter and cloud provides some potential relief. By its nature, a virtualization platform understands all of the VMs and how they are connected to the network regardless of any deployment or configurations changes. When you leverage that network knowledge, security policy becomes something that can be automated, and switching to defining security in terms of the application instead of the network endpoints just makes sense. That’s where microsegmentation and app-centric policy come into play.

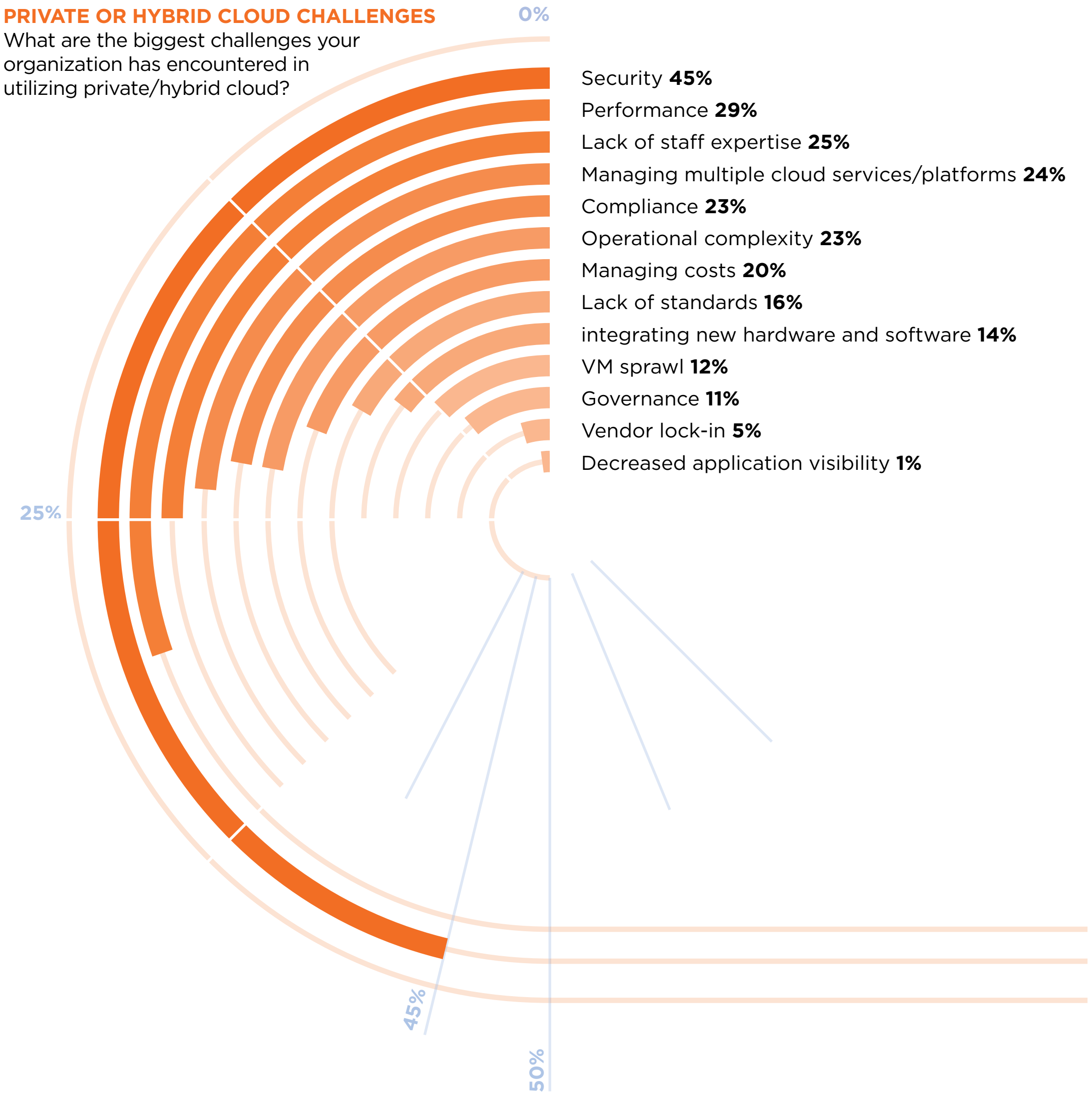
Being app-centric means shifting the focus away from individual VMs and their network identity to the applications themselves. Doing this application-based segmentation decouples policy from the network, simplifying policy administration and management. Security policies are mapped to logical groups or categories of VMs – used to define applications, application tiers (web servers, data bases, middle tiers), or isolation groups (test and development v. production). Once the application is assigned to a group or category, the associated policy follows the VM wherever it goes. The virtualization layer detects network changes and updates the rules accordingly. In addition, policies are automatically applied when VMs are provisioned, change network configuration, power state or migrate. This removes the burdens of change management.

App-centric security offers IT organizations a new approach to security policy management and, by doing so, helps address a lot of the challenges facing IT organizations today. The remainder of this eBook takes a look at those challenges and how app-centric security can address them to enable a more secure application environment.

CHALLENGE:

Organizations Face Growing Cyber Security Risk

PRIVATE OR HYBRID CLOUD CHALLENGES
What are the biggest challenges your organization has encountered in utilizing private/hybrid cloud?



Criminals know that large enterprise data centers contain valuable information. This has given rise to more frequent and highly targeted attacks on that valuable data. When perimeter or even smaller zone-based security is used, an attacker only needs to defeat a few "walls of security" before they are freely able to move and search for additional targets. Simply put, the perimeter-based approach to security is outdated and can't prevent lateral movement of a cyber-attack. Not only does perimeter security fail to stop advanced threats that spread from one system to another, but it can't easily adapt to protect today's dynamic IT environments. Organizations need a way to protect applications and prevent the propagation of network threats while ensuring the ability to deploy, migrate, and manage applications at the speed businesses demand.

SOLUTION:

Microsegmentation Reduces Risk

> "The increasingly dynamic nature of data center workloads makes traditional segmentation strategies complex, if not impossible, to apply. Further, the shift to microservices architectures for applications has also increased the amount of east-west traffic and further complicated the ability of traditional fixed firewalls to provide this segmentation."
>
> – Gartner – Hype Cycle for Threat-Facing Technologies, 2018

Microsegmentation, sometimes called east-west firewalling, is the concept of creating granular network policies between applications and services. Implementation of microsegmentation is a key part of a defense-in-depth strategy against modern data center threats by providing the next layer of defense beyond traditional perimeter firewalls. Microsegmentation essentially reduces the security perimeter to a fence around each service or virtual machine. The fence can permit only necessary communication between application tiers or other logical boundaries, thus making it very difficult for cyber threats to spread laterally from one system to another. Therefore, compromising one tiny perimeter doesn't automatically expose any other targets.

Making microsegmentation application-centric further streamlines security operations by enabling the ability to define high-level policies without needing details about the underlying infrastructure or network identifiers. Policy focuses on application tiers or groups and what types of communication are allowed. This is an important distinction as it separates the policy and groups from more dynamic network identifiers like IP addresses. This significantly reduces the complexity typically involved in policy management. The responsibility for understanding the infrastructure or network connectivity is removed from the human policy writers and left to the virtualization platform, which always knows the information needed to automatically update the policy accordingly.

Ideally, policy writers should incorporate application-level security policy without any changes to the existing network configuration, keeping things simple and allowing admins and architects to focus on the business or application requirements, not the network infrastructure. Eliminating the reliance or impact on the existing physical network also eliminates the need to change or rearchitect the physical design. As a result, the time required to implement security policy dramatically shortens.

CHALLENGE:

Lack of Application Understanding and Domain Knowledge

> "Visibility is the key to defending any valuable asset. You can't protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the telltale signs of a breach in progress and to stop it. Today, many firms fail to detect an in-progress breach for weeks, even months, unable to limit the damage."
>
> – Forrester, The Eight Business And Security Benefits Of Zero Trust

Data center virtualization, networking architectures, and the applications they support are complex. It's no longer possible to easily understand how applications are deployed or communicate simply by walking into the data center and tracing cables. The modern application can comprise multiple physical servers and virtual machines. In some cases, applications may not even be running on-premises. As a result, organizations have little idea how systems and hardware connect physically or over a network. The issues that arise from a lack of visibility come to light when one considers the traditional approaches to policy creation: blacklisting and whitelisting. When using the blacklisting approach, the policy writer allows most communication (default allow) and attempts to block malicious or unwanted traffic. This approach is simply impractical given the volume of new attacks that bombard data center networks on a daily basis.

A better approach to policy management comes from whitelisting. The policy writer blocks all traffic (default deny) and then creates policies to allow required application and user communications. In the modern data center, however, whitelisting is a formidable task. For it to be effective, application owners must have a complete understanding of the communications of their application. With the advent of service architectures and microservices, this knowledge can be spread across multiple teams, making it that much more difficult to implement.

SOLUTION:

Bring Visibility and Context to Policy Creation

> “Visibility is important to creating a strong security posture. Investing in visibility and discovery solutions is an opportunity to reduce cybersecurity risks. However, more than half of all respondents (55 percent) say their organizations are not purchasing such solutions. Further, the lack of visibility into sensitive data, applications and platforms is why many companies are concerned about the security of both public and private clouds.”
>
> – Ponemon, Separating the Truths from the Myths in Cybersecurity, 2018

Take the mystery out of network policy creation. Allow policy owners to visualize the discreet interactions between different entities inside the application, enabling them to understand exactly how each part of an application communicates with the others. Anyone should be able to look at the visualization and understand what VMs and services are involved in delivering an application and what physical infrastructure is used to run those servers. With this understanding, policy writers can be sure they’re implementing the best policies for those applications and services.

Comprehensive visibility eliminates the guesswork out of policy writing. Creating policies for the allowed traffic becomes a simple, repeatable process. It ensures that the appropriate policies are applied and reduces errors that could impact application availability or security. The automatic discovery of communications between VMs and visualization of application traffic and relationships reduce the need for application domain knowledge. Policy writers can create policies automatically based on real-time visualization of communications between applications and VMs without extensive application domain knowledge. Finally, visibility facilitates troubleshooting and incident response as IT organizations can see the root cause of performance and availability issues.

CHALLENGE:

Meeting Standards and Regulatory Compliance Requirements

TOP 5 INDUSTRIES EXPERIENCING DATA BREACHES

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

- Financial Services
- Industrial Manufacturing
- Service
- Technology
- Retail

IT organizations must contend with an ever-growing list of regulatory compliance and standards, including the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the European Union's General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI-DSS). Failure to comply with the necessary standards and regulatory compliance requirements can result in steep fines, legal actions, or business interruptions from government audits. To further complicate matters, the expense of mandated security practices from regulatory compliance efforts can seem to be in opposition to business goals or the desire to reduce spending and increase efficiency and profits.

Policy writers are challenged to implement controls where compliance requirements dictate in the least complex and most efficient manner. Combined with the complexity of many modern applications, this can become a tough problem to solve. For example, if a standard dictates implementing controls for production systems that contain customer data but do not need to be applied to test/development servers, then policy writers should have the ability to do just that—and no more. A common practice to address the need for this type of segmentation is to create dedicated islands of infrastructure for specific areas of compliance. This segmentation can reduce the scope of security controls, but it does not help contain costs or reduce management overhead. Modern on-premises infrastructure can be architected to achieve similar economies of scale to public cloud offerings; the introduction of physical segmentation removes those benefits.

SOLUTION:

Simplify Compliance

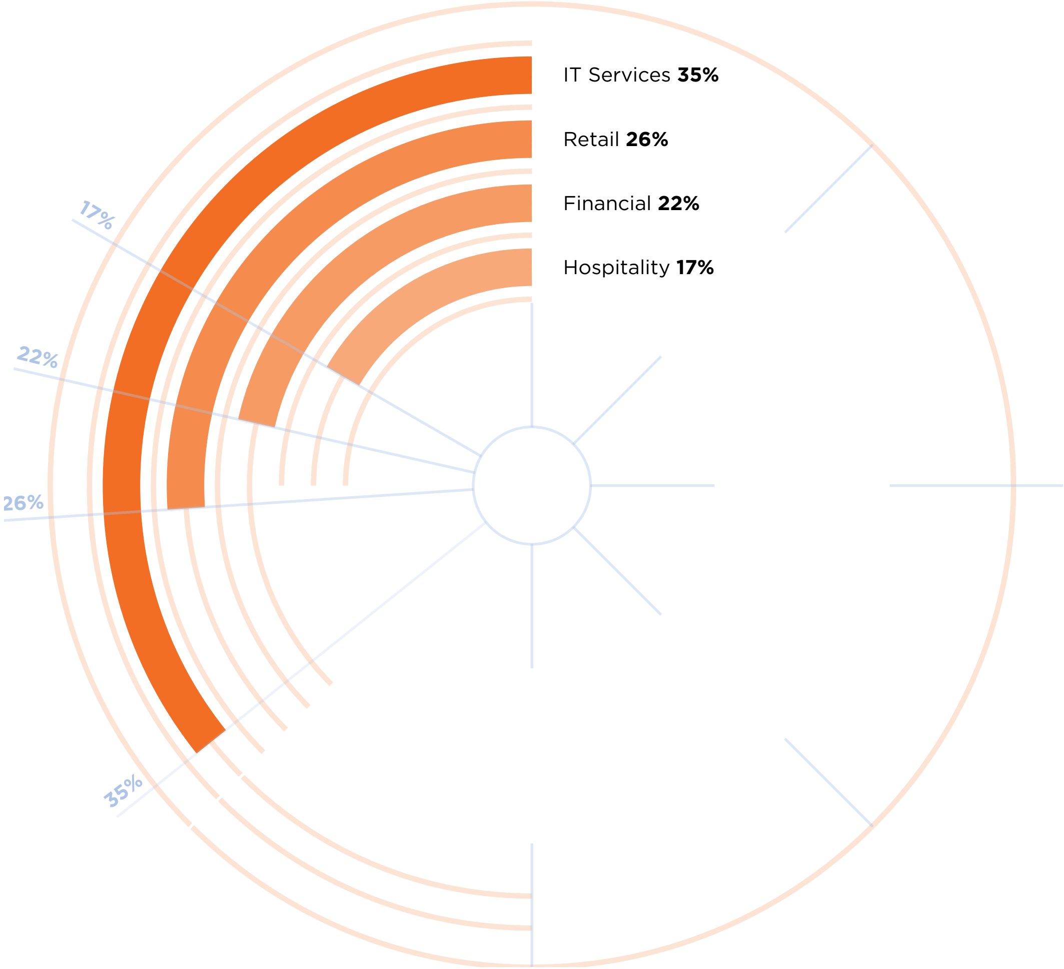


Figure 2
Verizon, 2018 Payment Security Report,, https://www.verizonenterprise.com/verizon-insights-lab/payment-security/2018/

The key here is to move from physical or infrastructure-based controls to using application or VM level polices based on software controls.

The granularity of software-defined, app-centric security allows policy writers to easily apply security controls surgically —only where they're needed to meet regulatory requirements. The granularity can be virtual machine or encompass application-level segmentation. Being software-defined, these boundaries are easily expanded and contracted, allowing regulated and non-regulated workloads to more easily mix using a shared infrastructure. There's no need to create costly dedicated infrastructure just for compliance purposes.

A wholistic approach also simplifies compliance management and audits. There is the ability to abstract policy from deployment of infrastructure details, allowing easier management, audit, and repeatability. Rather than looking at servers and services individually, the policy can be more comprehensive at the application level; all member services or VMs in an application are then subject to the same compliance policy. As new services or components are identified as members of the application group, they can easily be added to the overarching policy.

CHALLENGE:

Achieving Agility Across the IT Organization

“Organizations can’t handle increased complexity with manual processes. The nature of technology, particularly software-enabled technology, means that increased scalability and flexibility naturally lead to greater complexity. It becomes exceedingly easy to spin up system instances in the cloud, for example, when you can do so through a few API calls versus racking and stacking physical hardware. While technology scales, though, the ability to manage it through manual processes doesn’t.”

– Forrester, Reduce Risk And Improve Security Through Infrastructure Automation

IT has moved from the back office to being key to many companies’ competitive strategies. Businesses need to move fast to be competitive. That means IT must move faster. The dynamic nature of today’s applications further complicates matters. Modern applications need to scale up or down based on business needs and potentially burst out into public cloud infrastructures should demand exceed local capacity. Cloud computing and virtualization have helped to some extent by enabling the automation of many common tasks.

Application owners can provision new VMs and services at the click of a button. But while automation streamlines operations both on-premises and in the cloud, it must extend across all disciplines of data center operations: infrastructure, applications, networking, and security. In many cases networking and security have been left out of the automation effort and must fall back to slow, manual tasks. Manual intervention to make changes to security policy or configuration of physical devices brings an otherwise automated application deployment (provision VMs, attach storage, deploy application software, connect networking, etc.) to a crawl.

The manual process of configuring network switch ports or applying static security policies creates a bottleneck every time there’s a change in the environment and has a higher potential for error. IT can’t afford to have networking and security be a bottleneck. They too must be automated and become a checkbox as opposed to a roadblock.

SOLUTION:

Automate Networking and Security Operations

Validated processes for changes to policy or application configuration should be codified and automated. Most traditional security technologies can have automated configuration changes, but because these security controls are applied at a macro level v. application/VM, it can be difficult to understand the impact of a change done for one entity on another in a shared environment. When infrastructure, operating systems, or other changes are made in absence of the impact on applications that rely on those elements, problems can occur. Effective automation also requires a new focus on the application and security technologies that have the ability to apply controls at the same level. Once again, deep application knowledge or comprehensive visibility are not only key to the creation of the application-level policy, but also to the ability to automate the application and management of those policies.

INCREASING COMPLEXITY NECESSITIES THE USE OF AUTOMATION

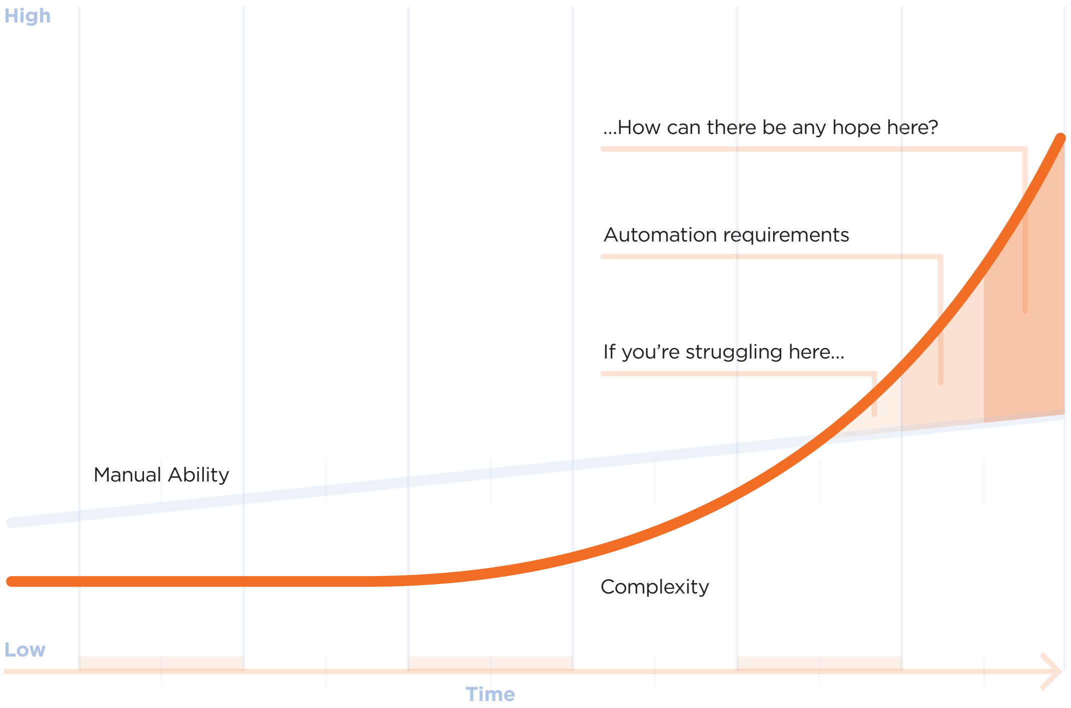


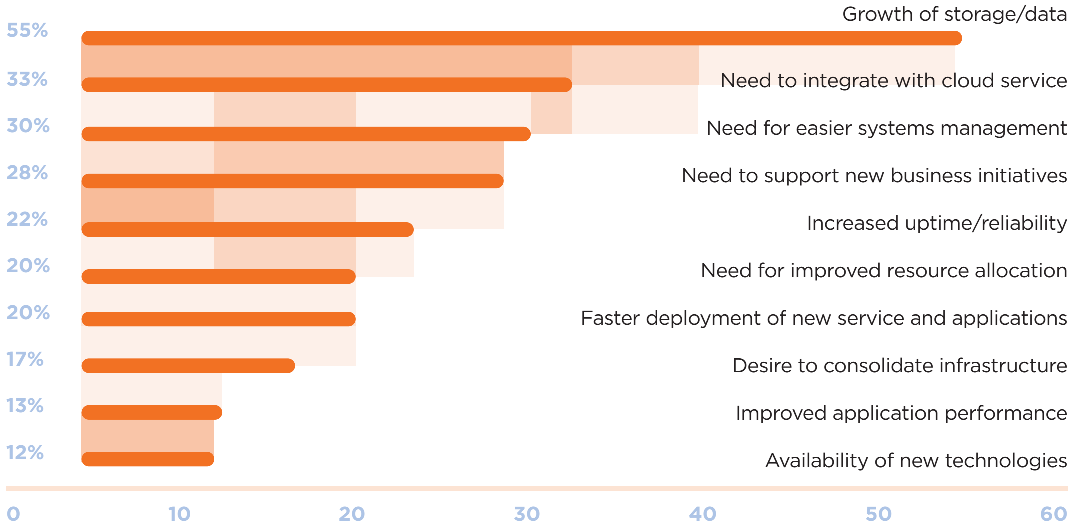
Figure 3
Forrester, Reduce Risk And Improve Security Through Infrastructure Automation, June 22, 2018

CHALLENGE:

Datacenter Complexity Leads to Policy Complexity

WHAT'S DRIVING IT INFRASTRUCTURE CHANGE

What three factors are driving the most change in your organization's IT infrastructure environment?



Note: Maximum of three responses allowed.
Data: Interop ITX Survey of 200 cloud computing users who use or plan to use IaaS, December 2017

The simple data center and application design that could be documented with a few diagrams and a spreadsheet dissolved long ago. Data centers are now becoming more complex as the number of contributing factors increases. Complexity is driven both by business trends, such as mobile computing and big data analytics, as well as IT trends that further increase the complexity, including virtualization, containers, cloud computing, etc. All this complexity impacts efficiency, costs, service availability and reliability, and of course, security.

The scope of IT was traditionally defined by assets sitting in a data center. Those physical walls along with some basic functional or departmental segmentation made up an easily defined set of perimeters that could be protected by physical network devices. This method of implementing physical security devices to create protective fences around large groups of IT assets is no longer effective or practical in this environment. It would dictate the use of many more devices with complex configurations. Although it may be possible to achieve, it would be financially untenable.

Managing traditional network policies is an extremely complex task because the large number of rules significantly increases the possibility of misconfiguration. Additionally, due to rules being written at the network address layer, the policies can quickly become incomprehensible.

As the momentum toward hybrid and multi-cloud operations continues, this problem of complexity compounds. Admins are burdened with wrangling policies across the public cloud, hosted private cloud, on-premises data center, etc., all highly prone to mistakes that lead to network vulnerabilities.

SOLUTION:

Leverage Virtualization and Categorization to Reduce Policy Complexity

COMPLEXITY OF BUSINESS AND IT OPERATIONS IS A SIGNIFICANT SECURITY RISK

83%
claim too much complexity

78%
site rapid growth of data assets

76%
integration of 3rd parties into internal networks and applications

Ponemon Institute, The Need for a New IT Security Architecture: Global Study, 2017

Policy needs to be simple. Policy is made complex by the need to enumerate the network identifiers of application components. Ideally, being able to abstract those components will greatly simplify the policy language. This abstraction turns the policy from network centric to application centric to focus not on the dynamic network, but on the more static definition of what an application needs to function. Consider all the IP addresses and infrastructure details that would no longer clutter policy definition. Policies become legible with less need for updates due to network or location changes. Virtualization allows much of this network information to be populated dynamically, streamlining network policy to only require details for permitted or allowed communication between application components or external entities.

This app-centric method provides a simple and intuitive policy model ideal for virtualization teams and application owners. Networking complexities are removed from the policy language, reducing the need for application domain knowledge. Instead, policies are mapped via application type, isolation zone, or other categories that become the building blocks of security policies. Once policies are defined, application and enforcement can be managed by tagging VMs or services to be included. The simple process of adding or removing the tags to include or exclude a VM from policy greatly simplifies application and daily IT administrative tasks.

Conclusion

In many ways, the modern data center has outgrown the traditional perimeter firewall, thus increasing the risk of a security breach. Security controls must evolve to work within today's IT environment—an environment that's characterized by rapid growth, change, and complexity. Organizations need security controls that provide granular protection behind traditional perimeter security to prevent the spread of threats and protect IT assets wherever they go.

With the huge increase in high value data stored in enterprise data centers, security attacks have become more sophisticated. Recent breaches covered in the media show how small vulnerabilities have been used as a point of entry, and then the sophisticated malware spreads throughout the datacenter. Part of this situation can be blamed on a legacy perimeter-based design. In the legacy design, segmentation is done at a macro scale that typically ends at the datacenter, which means that once those defenses are defeated, the malware is free to spread.

The solution has been known for some time now: **microsegmentation**. Microsegmentation moves security from the perimeter to VM or application granular controls that limit DC communication to what is minimally required for applications to operate. In a microsegmented environment, malware spread is greatly reduced if not completely blocked.

What has prevented widespread use of micro segmentation has been the complexity and cost of implementation. Modern applications are complex; they span multiple servers, leveraging microservices and even cloud-based shared services. The overhead of understanding, enumerating, and maintaining policy for 1000s of end points proved too complex for most to entertain. With modern virtualization and the level of context and visibility available now makes successful implementation of a microsegmentation strategy possible.

App-centric security from Nutanix Flow is the answer.

- Increase Application Security via Microsegmentation
- Isolate Environments without physical network complexity
- Ensure Regulatory Compliance
- Easily integrate additional network functions from 3rd parties

Nutanix Flow simplifies network and policy management with a focus towards applications, enabling applications and environments to be governed independent of the physical infrastructure. Fully integrated into the Nutanix platform, Flow delivers powerful networking and microsegmentation functionality with an intuitive policy creation and management interface that allows IT teams to easily visualize and secure the most complex enterprise applications. To learn more about Nutanix Flow or view a live, personalized demo with a solution consultant, visit https://www.nutanix.com/products/flow/.

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