TRANSFORMING SECURITY IN THE MOBILE CLOUD ERA

How to Protect Your Data, Improve Agility, and Stay in Compliance

vmware®

IT is Facing a New Set of Security Challenges

In the age of digital transformation, maintaining secure interactions among users, applications, and data is more complex than ever. Amid the rapid growth of hectic and complex digital environments, the tools IT has used in the past simply aren't sufficient to keep everything safe.

Security threats are also on the rise, and are becoming more sophisticated. Perimeter firewalls, the security standard for traditional infrastructure, can no longer keep them at bay. Disguised as legitimate traffic, malware can slip past perimeter firewalls undetected and spread faster than IT teams can stop it. The result: Organizations are investing time and money in a losing battle.

When the only constant is change, it's time to re-evaluate how IT approaches security, and how it can adapt to keep important data and applications safe.

Nothing is the Same in the Mobile Cloud Era

As businesses have increasingly moved to digital models, key components like applications and infrastructure have grown and shifted in major ways. And malicious attacks have adapted and become more sophisticated, too.

- **The nature of applications has changed**
  Once static and confined to physical servers, applications now range from mobile to multi-tiered distributed to container-based, and everything in between. Risks and exposures vary greatly across environments, and traditional, perimeter-centric security doesn't provide the visibility and control IT needs to keep individual workloads running securely.

- **The nature of infrastructure has changed**
  Data center infrastructure is no longer confined to a hardware-centric on-premises approach. Servers, switches, and routers have given way to private clouds. Virtualization has ushered in new models that leverage the power of software to speed development and improve application performance. User infrastructure has also changed, from corporate-managed desktops to mobile devices, laptops, and IoT.

- **The nature of security attacks has changed**
  Now that applications and infrastructure are on the move, so are security threats. As cyberspace has become weaponized, new types of threats have emerged, from hackers to hostile nation states and more. With a proliferation of tools to help attackers breach perimeter firewalls, disguised threats can easily enter the data center and spread through unprotected east-west traffic.

Staying in Compliance is Key

Not only have applications, infrastructure, and security attacks changed—but the burden of compliance is also growing. As attacks become more frequent, regulatory bodies are enforcing existing rules, and creating new ones. Organizations are doing their best to protect sensitive data and stay in compliance, but it's becoming increasingly difficult to keep up.

Business are facing:

Strict industry-specific requirements, such as PCI, FISMA, ECPA, NIS, and HIPAA

Differences in regulations from on-premises to the cloud

Advanced, persistent threats from new and unknown sources

The difficulty of keeping up

In a study by Forrester, two-thirds of survey respondents reported they are efficient at meeting data compliance standards, yet when asked about their progress in adhering to various data compliance regulations, they said full compliance was achieved in less than 50% of all efforts.[1]

[1] Leverage Micro-Segmentation To Build Zero Trust Network, Forrester, July 2015

Security Breaches Exact a Steep Toll

From combatting emerging threats to staying in compliance, it's no wonder that organizations today are spending more than ever to keep their data centers safe. But it appears to be a losing battle, as security losses are outpacing security spend. A recent study reveals that cybercrime represents the fastest-growing cause of data center outages, rising from 2% in 2010 to 22% in 2016.[1] In the digital era, that price tag isn't sustainable. It takes resources that could be better spent elsewhere, and drains away profit. And budgets are only one part of the problem. Organizations are facing stiff competition, and a loss of reputation or user trust that often comes with a breach could set them back permanently. Even if confidence can be salvaged, the loss of time and money spent dealing with the threat can put growth and innovation efforts on the back burner. Simply spending more money on security isn't enough to solve the problem. There needs to be a total transformation in the way organizations approach and deliver security.[2]

[2] Cost of Data Center Outages, Ponemon Institute, January 2016

$500 Billion

the approximate annual cost of global cyber espionage[1]

It’s Time for Total Transformation

With so many factors to consider, one thing is clear: When it comes to security, IT is facing a monumental challenge. Teams need to evolve security to adapt successfully. But where should they begin?

Let’s take a look at some top priorities to consider:

- **Focus and align controls to the applications and data that need to be protected.** The right controls can help ensure that applications and data stay safe, no matter where or when they travel through the data center.
- **Provide context to reduce complexity and noise.** With more visibility, IT leaders can make informed decisions based on the whole picture—not just a fragment.
- **Automate remediation and incident response.** Automation can provide fast, accurate resolutions to issues that would otherwise take days or weeks to identify and solve.

A Transformative Approach at Every Level

To move forward, organizations need a platform that aligns security to the applications and data they are trying to protect. That can be accomplished through a ubiquitous software layer independent of the underlying physical infrastructure or location.

With the right platform, organizations can:

Secure application infrastructure

Secure identity and endpoints

Streamline compliance

Let's take a closer look at each one.

Secure Application Infrastructure

Today, application infrastructure is divided between on-premises data centers, clouds, and distributed applications that leverage microservices. To keep everything safe, organizations need a unified solution that offers visibility and control—and perimeter-centric network security can't provide that.

With a virtualized network, IT can:

- Abstract infrastructure from the applications running on top of it, for full visibility and context into the environment
- Enable micro-segmentation to protect individual workloads, no matter where they are in the data center
- Encrypt data at rest for an additional layer of security, offering protection even if it falls into the wrong hands

Secure Identity and Endpoints

Enterprises today aren't just dealing with a mix of operating systems—they are also juggling mobility, Bring Your Own Device (BYOD) policies, and a surge of connected (IoT) appliances. With so many endpoints, it can be difficult to monitor and identify potential or active security breaches. Sensitive data can be put at risk in countless ways.

With a unified software layer that covers all users and endpoints, IT can:

- Secure all endpoints with a single solution
- Deploy any app through one catalog that features built-in compliance
- Leverage micro-segmentation to extend security beyond VDI and mobile endpoints
- Automate remediation against security threats

Streamline Compliance

Regulatory compliance issues are complex, and keeping up with them can be a tremendous challenge. This is especially true for organizations that are rapidly transitioning from on-premises data centers to cloud-based approaches, which come with a whole new set of demands and regulations. The regulatory environment is likely to continue to grow, and companies must develop better ways to demonstrate compliance. A holistic approach to security can provide the visibility IT needs to stay in compliance with ease.

A virtualized network with a unified software layer can help businesses:

- Streamline compliance processes
- Leverage the benefits of third-party tools without risking security
- Enable visibility on and off premises

A Better Approach to Security

Securing interactions among users, applications, and data is a challenge—but with the right tools, it's not impossible. By virtualizing the network and enabling automation and micro-segmentation, enterprises can transform security to protect their customers, their data, and themselves.

The market leader in virtualization technology, VMware transforms security with a ubiquitous software layer across application infrastructure and endpoints. This holistic approach maximizes visibility, context, and control to secure the interactions among users, applications, and data.

Modern IT professionals use VMware solutions to gain deep visibility into the interactions between users and applications, and the context to understand what it means. With VMware, IT teams can stop spending the majority of their time on compliance efforts and focus on what drives real value instead.

MAKE THE SMART CHOICE

Start your security transformation >

Join Us Online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Item No: vmware-transforming-security-in-the-mobile-cloud-era-TS-0218 2/17