GUIDE TO RETHINKING YOUR IT SECURITY

Responding to the Security Challenge of a Changing IT Landscape

vmware®

Defining an Age of Digital Transformation

Watching the rise of businesses that were born digital—think Uber and Airbnb—we see how technology serves as a competitive differentiator for these enterprises. Uber, for example, became the world's largest taxi service without owning any cars; and Airbnb has emerged as the world's largest hospitality business without owning any real estate.

Reshaping traditional businesses

At the same time, we can also see how technology is transforming more mature, traditional businesses. Manufacturing companies, for instance, are finding it imperative to embrace software as a means to make operations more efficient and productive. Jeff Immelt, chairman and CEO of General Electric, puts it succinctly: "It's our recognition that if you go to bed as an industrial company, you're going to wake up as a software company." What GE and others are learning is that competing in today's business environment means being a digital business.

Sizing up the Security Challenge

Accompanying this rising tide of digital transformation is the colossal and continuing growth in the number of end users with digital devices, as well as in the volume of applications and data that must be managed. It's a phenomenon that's generated a perfect storm of security threats for IT organizations. Data centers that were once safely on-premises have evolved into a highly dynamic public and private multi-cloud environment. And users that once worked from corporate desktops are constantly on the move outside the workplace, expecting to access corporate networks from their own devices and even through the Internet of Things (IoT).

A rising tide of risk

With these factors at work, the exposure to risk keeps expanding. And sophisticated attackers are aiming to exploit these data center vulnerabilities. In one recent survey that assessed global enterprise IT security, 75 percent of respondents conceded that they would likely be fighting off a cyberattack in 2016.[1] IT organizations also face mounting demands for regulatory compliance. In fact, compliance responsibilities account for up to 20 percent of an IT employee's time.[2]

In this changing IT landscape, the resulting security challenges are clear, even though they're not simple to solve: How do we protect interactions between users, applications, and data?

ADDING UP THE IMPACT

- Average cost of a data center outage increased to $740,357 in 2016.[3]
- Including costs associated with stolen intellectual property, global cyber espionage costs businesses up to $1 trillion annually.[4]
- In 2016, the average cost of a data breach increased to $4 million, or $158 per lost or stolen record.[5]

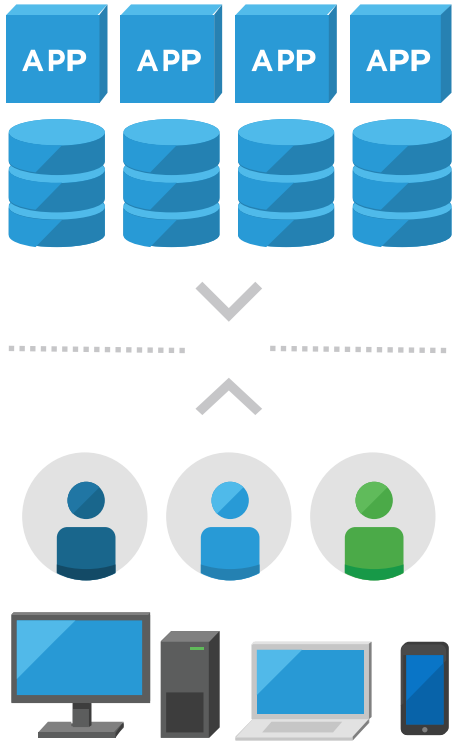


Figure 1. "Digital transformation impacts IT and security"

[1] State of Cybersecurity: Implications for 2016, ISACA, 2016.
[2] Cost of Data Center Outages, Ponemon Institute, January 2016.http://datacenterfrontier.com/white-paper/cost-data-center-outages/.
[3] Cost of Data Center Outages, Ponemon Institute, January 2016.
[4] Https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.
[5] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, June 2016.

Five Areas for Rethinking IT Security

As we've already seen—even with IT security spending topping $80 billion in 2016 alone[6] —the old approach to IT security isn't sufficient to stem the rising threat levels. With that in mind, here are five considerations to help you rethink your approach to IT security:

1. Changing the model for security
   Using bolt-on point solutions, standalone boxes, or software products, traditional IT security systems are complex and poorly coordinated. What's needed is a holistic, architected model that delivers security simply and effectively.
2. Implementing a ubiquitous software layer
   With a ubiquitous software layer across application infrastructure and endpoints, it's possible to abstract infrastructure from the applications running on top of it. As a result, you can apply security effectively and easily throughout the data center.
3. Providing maximum visibility and context
   By abstracting the infrastructure from your applications, you get visibility into application data flows and full end-to-end context for interactions between users, applications, and data.
4. Aligning security controls and policies to your applications
   With the benefits of maximum visibility and context, you can begin to align your security controls and policies to the applications you're trying to protect.
5. Inserting additional third-party security services
   By aligning security controls and policies to your applications, you can then start to insert additional third-party security services for additional layers of intelligent protection.

NEW RULES FOR NETWORK SECURITY

The old ground rules of network security simply don't apply anymore, and IT teams need to keep pace with:

- **Changing infrastructure:** Infrastructure is evolving from on-premises environments to support cloud and distributed apps.
- **Increasing mobility:** IT needs to expand its security policies to support a flood of new devices and models.
- **Escalating compliance:** Organizations face new requirements for regulatory compliance.

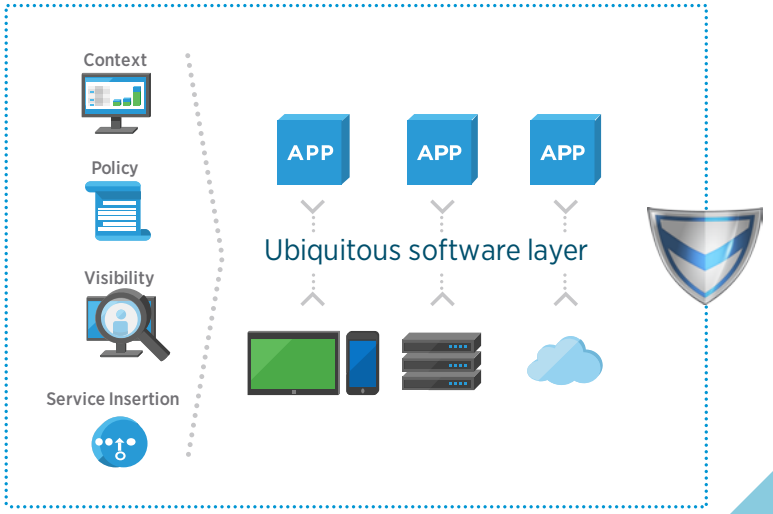


Figure 2. A Ubiquitous Software Layer Means Security is Everywhere

[6] "Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016," Gartner Inc., August 2016.

Taking a Three-Prong Approach to IT Security

Transforming your security environment in order to meet today's critical security challenge calls for a three-prong strategy.

Protect the Data Center: Rethink Management and Security for Your Data Center

You need the means to better "compartmentalize" your sensitive assets, to better align security controls around these assets, and to gain more visibility and control to help you detect and respond to threats.

Protect the Endpoint: Rethink Management and Security for User Infrastructure

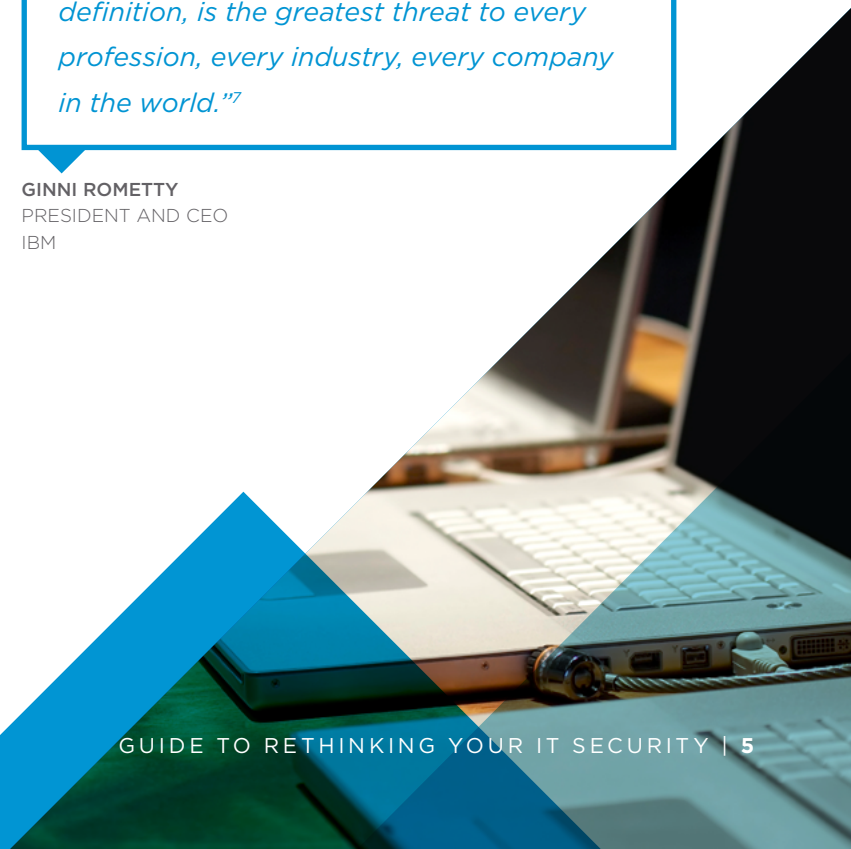
With the proliferation of mobile devices and operating systems, there is no uniform fabric for user infrastructure. It's a great big, heterogeneous world out there. You need better visibility and control—not just from an infrastructure perspective, but from an app-centric perspective—without damaging the experience that users expect.

Protect the User: Rethink User/Access Controls

User access is critical to empower your workforce. You need an approach that can help you reduce the attack surface, create greater visibility into user interactions, and enable an efficient response to inevitable security threats.

> *"We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true—even inevitable—then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."*[7]

GINNI ROMETTY
PRESIDENT AND CEO
IBM



[7] "IBM's CEO on Hackers: 'Cyber Crime is the Greatest Threat to Every Company in the World." Forbes. November 24, 2015.

Conclusion

Digital transformation represents a massive opportunity for your business. But with this opportunity comes risk, and a steep challenge—to protect the rising number of interactions between your users, your applications, and your data.

By rethinking your approach to IT security, you can answer this modern security challenge. Transforming your security starts by establishing a ubiquitous software layer across your application infrastructure and endpoints. With this software layer in place, you'll gain deep visibility into these interactions you want to protect, and the context to understand what they mean.

GET STARTED TODAY

Get help with rethinking your approach to IT security

LEARN MORE >

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