THREE KEY STEPS TO TRANSFORMING IT SECURITY

Security Is Top of Mind for Every Business

As people, devices, and objects become more connected, protecting all these connections and environments has become more critical than ever. In a recent survey of IT priorities, 69 percent of respondents told Tech Pro Research that improving security represented their top IT initiative for 2017.[1]

In the same survey, respondents also said security would be their biggest IT challenge in the year ahead. That's because IT organizations need to secure each and every interaction between users, applications, and data—however and wherever they are connecting. And they need to do it in an environment that is constantly changing, and increasingly dynamic.

Security risks are high for businesses in every industry, and they are continuing to escalate. According to a recent study, the average total cost of a data breach increased from $3.52 million to $3.79 million in just one year.[2] For organizations that are embracing cloud and virtualized environments, maximum visibility and control are key to mitigating this risk.

Evolving Risks in a Dynamic Threat Landscape

Every business has become a digital business—a transformation that's given rise to significant changes on the IT landscape, and consequently new challenges for IT security.

Start with the evolution of application infrastructures, which have transitioned from on-premises data centers that run physical infrastructure to highly dynamic environments that reside on public and private clouds. And consider how applications themselves are changing. Organizations are moving away from monolithic application stacks to distributed, multi-tiered apps that are based on microservices. As the workforce becomes more mobile and distributed, end-user environments are evolving as well. They are no longer limited to corporately managed desktops, but are centered around mobile devices, bring your own device (BYOD) initiatives, and the Internet of Things (IoT).

As a result, traditional network perimeter security models are no longer sufficient to protect the sprawl of applications and users, or to meet escalating compliance requirements. Environments and users aren't contained neatly behind perimeter firewalls, but instead require more flexible, agile protection against attackers that have become more sophisticated. Cyberspace has become increasingly weaponized. Even an inexperienced hacker—using toolkits such as Zeus and BlackPoS—can target a business with advanced attacks that can do real damage to its productivity, resources, and reputation.

As we adjust to account for these developing challenges at the doorstep, compliance standards are becoming increasingly complex—forcing the average IT team to spend 20 percent of its time on compliance efforts.

THE STAKES ARE HIGH FOR SECURITY

- Cybercrime represents the fastest-growing cause of data center outages, rising from 2 percent in 2010 to 22 percent in 2016.[3]
- Average cost of a data center outage is rising to $740,357 in 2016.[4]

[1] "IT Budget Research: Where CXOs are placing their bets for 2017," Tech Pro Research, July 2016.

[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.

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

[4] Ibid.

vmware®

Three Areas of Focus for Effective IT Security

Protecting an organization with a robust, compliant security solution isn't easy when the infrastructure and its users are rapidly changing. The old ground rules of network security simply don't apply anymore, and IT teams need to keep pace with:

- Changing infrastructures—The infrastructure used to run applications like web and database servers 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—The regulatory compliance environment has become increasingly complex as organizations face new requirements.

Deliver Visibility and Context to Transform Security

In order to stay a step of ahead of your changing security needs, you need deep visibility into every interaction between users and applications. You also need a solution that provides context to understand what those interactions mean. Combined, greater visibility and context can help you align your security controls and policies to the applications you are expected to protect.

The foundation for such a solution? A ubiquitous software layer across your application infrastructure and endpoints that's independent of the underlying physical infrastructure or location.

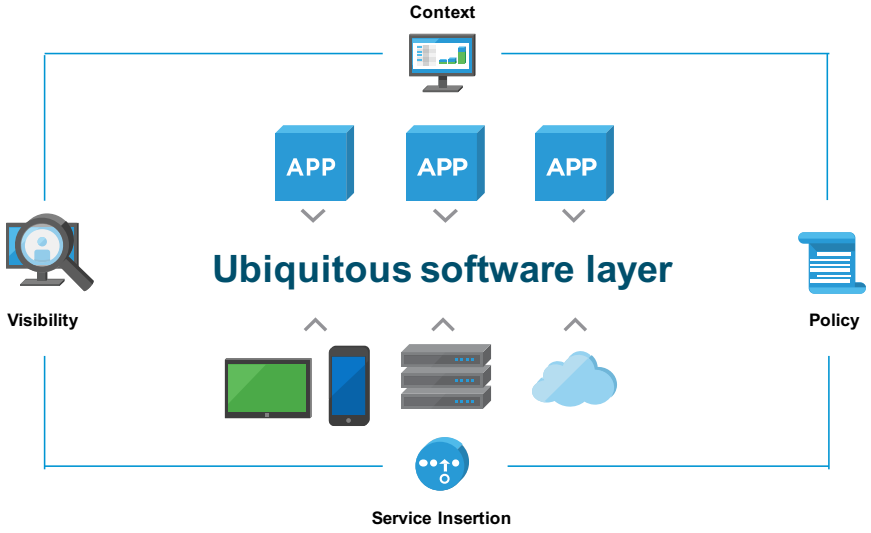


FIGURE 1. A Ubiquitous Software Layer Means Security Is Everywhere

In fact, effective security requires multiple layers of protection. And the right software solution within the infrastructure provides you with the best possible control point to increase visibility, enforce policy, and enable insertion of third-party services for additional intelligent protection.

Let's take a closer look at these three key steps to transforming your IT security:

- Secure application infrastructure—Abstract infrastructure from applications, improving visibility and better aligning security to apps.
- Secure identity and endpoints—Employ a ubiquitous software layer across all users and endpoints for better visibility and control, without impacting the user experience.
- Streamlined compliance—Apply software across the app infrastructure, identity, and endpoints to simplify compliance.

"As more companies compete for talent in a limited marketplace, the skills gap will become an even greater problem. Companies may be forced to rethink strategies and look for (security) solutions that are more proactive and require less management to allow them to make the best use of resources."[5]

JAMES MAUDE
SECURITY ENGINEER
AVECTO

1. Secure Application Infrastructure

As application infrastructure models evolve, the traditional perimeter-centric network security approach cannot provide enough visibility and control inside the data center. At the same time, stored data at rest has become a much more valuable target for attackers. To address these problems, you need to transform the way you secure your application infrastructure.

The solution starts with virtualization, and the ability to abstract the underlying infrastructure from the applications running on top of it—whether that infrastructure is on-premises or in the public cloud. This layer of abstraction provides full visibility into the data path, and an ideal enforcement point to compartmentalize applications through micro-segmentation of the network. Employing micro-segmentation in software lets organizations simplify security policy, and align it more closely to the application needs. It also lets the policy follow the application as it moves across private and public clouds. An abstraction layer also provides a platform for additional third-party services to be inserted for more advanced security protection.

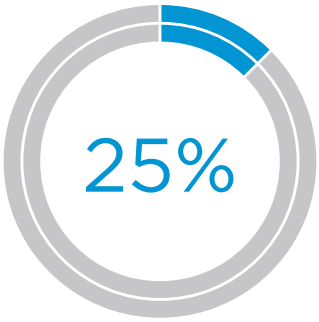
Micro-segmentation also helps IT prevent security threats from breaching defenses by enabling the principle of application-centric least privilege, which reduces the infrastructure's attack surface.

An abstraction layer between applications and the underlying infrastructure not only helps IT avoid attacks; it provides an ideal point to encrypt stored data. By encrypting data at rest, at the workload level, organizations can ensure that application infrastructure data is safe, even if it falls into the wrong hands.

2. Secure Identity and Endpoints

As your business goes digital, mobile devices are proliferating fast. Organizations like yours are employing everything from Android, iOS, Windows, macOS, and other devices to empower workforces and re-imagine traditional business processes. Supporting all these devices and platforms is challenging, especially as companies embrace enterprise mobility, BYOD, and IoT initiatives.

[5] http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.



By 2020, more than 25 percent of all identified attacks in the enterprise will involve Internet of Things (IoT).[6]

By applying a ubiquitous software layer across all users and endpoints to verify user identity and device posture, you'll be equipped to address this challenge. This approach provides end-to-end visibility and control of the user and endpoint, extending all the way into the data center or cloud, where the application infrastructure resides. With a software layer, IT can add an adaptive, conditional layer of security at each transactional level, from users to the resources they're accessing. It helps secure corporate data and reduce the cyber-attack surface, without impacting the user experience.

Look for a single solution that can protect all your endpoints, including smartphones, tablets, laptops, wearables, and IoT devices. As a result, IT can seamlessly deploy any app—including native, web, remote, virtual apps, and Windows desktops—through a single app catalog with built-in single sign-on, data security, and endpoint compliance. For today's dynamic workspaces, you want a solution that extends security beyond the virtual desktop interface (VDI) and mobile endpoints into the data center with micro-segmentation.

Because every business has specific security needs, your solution should also help you customize your environment to align with your priorities. You'll have a foundation for working with security partners, who can leverage the visibility and control points provided to complement the solution with their own service offerings.

"Customers are walking away from businesses that suffer breaches, and the regulatory environment is such that businesses will need substantial protection, whether they build it into their organizations or outsource the responsibility."[7]

FADI ALBATAL
SENIOR VICE PRESIDENT
ABOVE SECURITY

3. Streamline Compliance

Managing risk and maintaining continuous compliance are always major concerns. It's especially important for industries like financial services, government, and healthcare organizations, which face strict requirements such as PCI, HIPAA, ECPA, the Directive on Data Protection for Europe, and more. Regulations and requirements are growing, while the digital landscape and advanced persistent threats continue to evolve, making it more challenging than ever to ensure and demonstrate compliance.

To complicate matters, organizations are rapidly transitioning from on-premises data centers and adopting the cloud, making it even more challenging to meet business, regulatory, and policy demands.

With a ubiquitous software layer across application infrastructure and endpoints, you're taking a holistic approach to compliance. This unique approach provides an ideal location to implement compliance controls, and gain the visibility necessary to demonstrate compliance. The right solution provides a technology platform in which validated tools and services from ecosystem partners can be dynamically inserted to further streamline the compliance process.

Using a compliance reference architecture framework, you can link between integrated software and hardware capabilities and specific regulatory controls with independent audit validation. And you can leverage an independently validated program to securely run highly regulated workloads. Whether you are employing a private or public cloud environment, you want assurances that your organization can remain continuously compliant. That requires a solution with the speed, efficiency, and agility you demand, while streamlining your compliance process.

[6] "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016," Gartner Inc., April 2016.

[7] http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/.

Security for a Changing Landscape and Needs

Robust security has always been essential for business networks, and as the pace of change accelerates, it's more necessary than ever. As traditional infrastructure, applications, and workforce models evolve, your IT team is under increasing pressure to protect the business from emerging new threats.

A ubiquitous software layer across application infrastructure and endpoints can help you transform your security. It lets you maximize visibility and context of the interaction between your users and applications, so you can align security controls and policies to the applications you are protecting. And it makes it easy to complement your solution with third-party security services for additional intelligent protection.

GET STARTED TODAY

Transform Your IT Security for Today's Landscape

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