TechTarget Custom Media

Cyber Security for the Digital Age: How to Scale, Modernize and Automate IT Security

As digital strategies transform businesses worldwide, IT infrastructures are undergoing profound change. Moving far beyond the servers and desktops of an earlier generation, enterprises now rely on both public and private clouds, linked by high-bandwidth networks. At the same time, the use of smartphones, tablets, application infrastructure, virtualized workloads, cloud services and Internet of Things (IoT) devices, is multiplying exponentially. The result: Networks are no longer bound by physical limits, but instead extend far beyond the walls of office buildings, warehouses and factories.

These broad infrastructure changes create new challenges for cyber security in a world in which attacks are steadily increasing in number, variety and sophistication. Also raising the bar for data protection are demanding regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) in financial services and Health Insurance Portability and Accountability Act (HIPAA) in health care. In addition, the European Union's General Data Protection Regulation (GDPR) goes into effect with stiff penalties in May 2018. Defending data in this new environment requires a comprehensive and integrated approach to cyber security.

Security challenges

The need to keep data secure is more urgent than ever due to steady drumbeat of costly cyber attacks. According to the Ponemon Institute, the cost for each

Sponsored by vmware

Table of Contents:

stolen record containing sensitive and confidential information was $141 in 2017, while the size of the average data breach increased by 1.8% from 2016 to 2017.[1] The expansion of the network perimeter means that threats can come from both inside and outside the data center. Some of the most dangerous and prevalent attacks are:

- **Man-in-the-middle.** A malicious actor inserts him or herself between two parties involved in a digital interaction. Each of the two parties believes data they receive from the other is secure. But the malicious actor impersonates each party while siphoning off the data for ulterior purposes, leaving the two parties unaware of any theft.
- **Ransomware.** A malicious actor encrypts data and demands a payment from the victim in order to unencrypt the data. Usually spread by phishing emails, ransomware may be spread by other means as well. For example, the WannaCry ransomware attack was spread by a virus.
- **IoT-based DDoS attacks.** IoT devices are many and varied, including everything from factory floor sensors to video security cameras, which were recruited into the Mirai botnet that paralyzed parts of the Internet in the fall of 2016.
- **Infections from endpoints.** Whether smartphones, tablets, or laptops, employees' personal devices travel with them, becoming exposed to data theft and malware as they access the Internet through insecure Wi-Fi networks and utilize potentially infected USB devices. When the BYOD device rejoins the corporate network, an infection can spread throughout an organization.
- **Cyber attacks and malicious hackers.** The damage caused by cyber criminals as well as malicious actors can be significant. Disgruntled employees and contractors may misuse privileged access for personal gain, downloading information worth millions of dollars to sell it on the outside.

With such an imposing array of threats from both inside and outside, IT leaders might be led to deploy a patchwork of different security solutions to address each threat. For example, identity and access management, encryption, intrusion detection and analytics all might be purchased and deployed separately. However, this approach can lead to problems of its own by creating the unnecessary cost and complexity of managing multiple products and vendors, as well as the uncertainty that the different point products are working together to provide complete protection.

The security solution

A comprehensive security solution is the best way to keep data safe. It should consist of a framework of technologies that are integrated with each other to address the following requirements:

Identity and access management

With cyber criminals and malicious actors seeking to gain access to protected data, the ability to authenticate users and verify their identity is critical. Biometric and two-factor authentication are major improvements over conventional passwords. Used with single sign-on, they can secure and streamline user access to applications, whether native, web, remote, virtual, on-premises, or in the cloud.

Once users have been identified, least-privileged access should be implemented so users are allowed access only to the minimum amount of applications and data they need to do their work. For example, employees in the facilities department should not have access to corporate payroll or human resources data.

And because threats may originate from inside as well as from outside an organization, it is important that end users be treated as untrusted. Formerly, employees working within a corporate office building were considered trusted, but as the array of attacks described above indicate, it is no longer reasonable to apply trust to employees or devices under any circumstances.

Endpoint and IoT security

A “don’t-trust” approach must be applied to all endpoint devices, including desktops, laptops, tablets, and smart phones. Although mobility is an important productivity enabler, mobile devices, BYOD in particular, are susceptible to malware that users might unwittingly acquire and spread throughout an organization. And IoT devices are also ripe targets for malware because many lack basic security features and cannot acquire them through upgrades.

A highly recommended approach is to implement unified endpoint management, which can help ensure access to all resources from a broad variety of end-user and IoT devices across global networks. Unified endpoint management technology can also detect and remediate threats. And it incorporates personalized and dynamically configured policies together with simplified end-user profile management across any virtual, physical, or cloud-based environment.

In addition, encryption of data both in motion and at rest is also mandatory, and is particularly important for wireless networks, which are capable of sending sensitive data beyond the walls of a company.

Data center security

Because it offers many benefits, including efficient resource utilization and streamlined management, virtualization is widely deployed on servers and storage devices in the data center. Virtualized servers and storage are key parts of converged infrastructure, as well as hyper-converged infrastructure, which adds networking technology to the mix. Also for reasons of efficiency and improved management, virtual desktop infrastructure (VDI) has taken hold in many organizations.

Virtualized storage such as vSAN technology affords important security benefits. In recent years, self-encrypting drives became popular as a way to automatically encrypt data at rest. But the addition of self-encryption to virtualized storage means self-encrypted physical drives are no longer necessary.

In VDI, security is improved because applications and data reside on the server, not on endpoint devices, eliminating a major point of potential compromise. When data going to and from the VDI devices is encrypted, security is enhanced further.

Whether at the server or desktop, a virtualized infrastructure can provide benefits for regulatory compliance as well. The centralized control of IT resources enabled by virtualization makes it easier for IT managers to demonstrate, in case of a compliance audit, where data is located and where it is traveling.

Networking security

Network virtualization delivers many security benefits. As with server, storage, and desktop virtualization, a virtualized network de-couples the network functions from physical network devices by implementing them in software. This enables security functions to be embedded into the virtualization hypervisor, which enables applications to be compartmentalized through micro-segmentation of the network. Micro-segmentation helps isolate any malicious penetration to the segment in which it occurs, even on converged and hyper-converged infrastructure, preventing it from moving to other segments.

Network virtualization also enables security policies and services to be tied to individual applications and workloads, traveling with them should they be moved from one data center to another, or be deployed in a hybrid cloud environment.

As with server and storage virtualization, network virtualization helps enable regulatory compliance. Micro-segmentation and granular security of workloads isolate sensitive systems and help to demonstrably ensure that operations are compliant with a host of different regulations.

Cloud security

In just a few years, public cloud services have emerged as a key piece of IT infrastructure. Although IT leaders initially had doubts about sending data from their own data centers to an off-premises facility within the public cloud, many experts agree that cloud services are typically more secure than most private data centers. Cloud-based servers that encrypt customer data are highly secure, and when data traveling to and from the cloud is encrypted, security is enhanced further.

With regard to regulatory compliance, the ability to demonstrate for audit purposes that data is encrypted is important. Also important for compliance is data sovereignty, which mandates that data stored in one country be subject to the laws of that country. Regulations governing personally identifiable information (PII), such as the GDPR, may require that data pertaining to an individual be stored in the same country in which the person resides. A comprehensive security solution should give IT managers visibility into the encryption status of data as well as its physical location in the cloud.

Information lifecycle management, compliance and data loss prevention

Information lifecycle management (ILM) encompasses data access, usage, storage, transfer, deletion, and destruction and therefore touches on all parts of data management and security. An important part of ILM is data loss prevention (DLP), which governs the data that end users can access and send outside the corporate network. DLP is an important technology to prevent the malicious or inadvertent exposure of critical data such as trade secrets or confidential customer information.

Like ILM, compliance with regulatory guidelines should be integrated into all aspects of data management and security. A comprehensive security and compliance solution enables the consistent implementation of regulatory controls with the visibility necessary to demonstrate compliance. An important tool is a compliance reference architecture that links integrated software and hardware capabilities and specific regulatory controls with independent audit validation.

Conclusion

The era of digital business is bringing fundamental change to IT infrastructure. Mobile and cloud services have become essential to many organizations. New endpoints such as IoT devices are creating new opportunities to increase operational efficiency. But altogether, these changes have made the task of securing data and assuring regulatory compliance exponentially more difficult at a time when security threats have never been more numerous, varied, or threatening.

Because attacks can come from both inside and outside an organization, security must be pervasive, and both users and their devices must be untrusted. A comprehensive cyber security solution is the best way for organizations of all kinds to address these new realities. Such a solution should encompass identity and access management, endpoints, virtualization, networking, the cloud, ILM, and compliance. Only by deploying a full array of security technologies designed to work together in an integrated framework, can an organization embark on the journey of digital business with confidence.

For more information, please visit http://vmware.com/go/cybersecurity