FORTINET

Understanding the Underlying Causes of Complexity in Security

Implications of Digital Transformation for the CIO

Table of Contents

FORTINET

Executive Overview

Network diversification is an unavoidable consequence of digital transformation (DX). CIOs preside over networks that serve growing numbers of users, and applications inside and outside the organization. A plethora of devices are now connected to the network. Many of these are mobile, some are user-owned, and others, such as Internet-of-Things (IoT) nodes, have no user at all. Networks also deliver a variety of applications and services, increasingly through complex hybrid IT architectures that extend to multiple public clouds.

Securing networks has become the greatest obstacle to DX for IT executives.[1] One difficulty lies in the high degree of complexity and cost associated with managing multiple point products that don't communicate with each other and share threat intelligence. Another challenge is how to deliver consistent security policy across all distributed locations with common network access control practices. The overreaching goal is to reduce risks, protect critical applications, and achieve compliance while maximizing business value from security investments. Security complexity must first be resolved if DX is to be successful and sustainable.

85%

of IT executives surveyed said network security is a large barrier to DX efforts.[2]

By 2025, the total installed base of IoT-connected devices is projected to exceed 75 billion worldwide.[3]

The Security Impact of Network Diversification

As organizations embrace DX to improve business outcomes, networks must support increasingly diverse users, devices, and applications. These pose a variety of security risks:

DX organizations are providing network access to diverse users

IT staff must support connectivity not only for employees but also for customers, contractors, and suppliers. Many of these users connect to the network with personal devices, such as phones, tablets, and laptops. Contractors and suppliers may also attach service-related equipment.

Because the company does not own these endpoints, it can be difficult for the IT team to protect the network from threats that may originate from them. IT staff have no control over the security software that the endpoints may, or may not, be running. For the same reason, protecting the safety and privacy of the devices' users is also challenging.

The applications and data that network users need are in multiple clouds

Because traffic between enterprises and clouds and between the clouds themselves is inherently internet traffic, it is usually encrypted.[4] But the same secure sockets layer (SSL) and transport layer security (TLS) encryption protocols that provide protected access for users also create a hiding place for malware. Recently, it was discovered that hackers have stashed malware in hidden directories in SSL-protected WordPress sites.[5] The implications are serious, as WordPress powers more than a third of all the websites on the internet.[6]

Another problem with working in the cloud is that users may intentionally or inadvertently leak intellectual property or other privileged data to the cloud. Finally, the cloud services themselves may not be adequately secured by their providers. This is especially true in the case of Software-as-a-Service (SaaS) solutions such as the widely used Office 365.

CIOs face significant technical hurdles as they attempt to enable all authorized network traffic to travel swiftly and seamlessly wherever it needs to go while effectively barring all unauthorized traffic.

Adopting DevOps principles to improve development efficiency increases security risks

DX organizations are adopting DevOps principles so that they can drive new software products or business applications into production quickly and update code frequently and efficiently. DevOps teams rely heavily on cloud services for these capabilities.

However, liberal cloud provisioning rights for developers and a lack of security awareness in the development process lead to a variety of security gaps and mishaps. One of the prevalent causes of security vulnerabilities is the incorrect configuration of virtual servers in public clouds. This is a highly detailed process that can be a hazard for developers who are inexperienced with security protocols.

An even greater risk may be posed by IoT-connected devices

IoT devices are proliferating by the billions globally.[7] These sensors, cameras, printers, and other headless devices may be company-owned, but they typically lack robust built-in security. Additionally, as DX drives interconnectivity, the traditional "air gap" between operational technology (OT) networks (where many IoT devices reside) and the corporate network is disappearing. These two trends give bad actors an opportunity to use IT-based threats to attack the less-defended OT systems.

Business continuity and even national security may be at risk when cyber threats originating in an employee email or a web application find their way onto OT networks. The widely publicized attack on the Ukrainian electricity grid that left 230,000 without power is just one example of such a risk.[8] As a result of IT and OT convergence, nearly 90% of organizations have now experienced a security breach within their supervisory control and data acquisition (SCADA) and industrial control system (ICS) architectures.[9]

Security challenges are no longer confined to the network edge

Because neither users nor applications in a DX company can be enclosed within the traditional network perimeter, a security strategy based solely on perimeter defenses is now untenable. Protecting the network and users in a DX organization requires a defense-in-depth strategy, but as CIOs go deeper into the network, they are discovering even greater complexities.

As a result of IT/OT convergence, nearly 90% of organizations have now experienced a security breach within their SCADA/ICS architectures.[10]

The Complexities of Separating and Grouping Assets

As part of their defense-in-depth strategies, corporate CIOs see the need to add layers of protection inside the network so that an attack on one area cannot move laterally (east-west) to impact network assets in other areas.

They are not alone in this. Governments and industry groups have recognized how network diversification poses various consumer privacy and national security risks. Their concerns have resulted in regulations and standards that require the isolation of sensitive digital assets. Among the most prevalent of these is the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

A common method used to effect asset separation is network segmentation. The goal is usually to allocate specific IP addresses, router ports, or virtual LANs to specific users, applications, devices, or data. Only the users, hardware, and software specifically assigned to a specific network segment are then able to access resources on that segment. It is difficult, however, to define network segments such that each contains all the assets requiring isolation and nothing but those assets. Protected data and applications, and the users authorized to access them, are often dispersed across departments. Additionally, the same devices may be used to access both protected and unprotected applications.

A segmentation scheme that leaves some sensitive assets unprotected is obviously unacceptable. However, erring on the side of caution is hardly a better alternative for the CIO. Unnecessarily locking down assets that do not require protection can disrupt operations, which can be particularly detrimental in OT environments.

Moreover, even if it were possible to segment the network to meet all compliance requirements, these requirements will inevitably change over time. So will the organization itself, especially if it engages in heavy restructuring or merger and acquisition (M&A) activity. Here, it is impractical in a DX organization to redesign the network architecture every time the business is impacted by a new regulatory change or business reorganization.

Leaving sensitive assets unprotected is unacceptable. But locking down assets that do not require protection can disrupt operations.

The Burdens of Managing Access Control in Diverse Networks

In addition to the difficulties of defining network segments for effective asset separation or grouping, CIOs need to consider how to enforce and manage access to the different segments. This includes verifying the identity of all entities requesting access as well as inspecting the content of all traffic traversing each segment. To preserve network performance, access permission decisions must be made in real time.

CIOs often make three critical errors in designing a segmentation plan for a DX-enabled network:

Trust is all or nothing

In principle, only trusted entities with the appropriate credentials for a particular segment should be given access. However, many access control solutions assume that certified devices and applications, as well as authorized users, are trusted. Unfortunately, more than one-third of breaches involve internal users, and 29% involve stolen credentials.[11] Moreover, trusted devices and applications can be compromised.

A network supporting DX must protect sensitive assets, but without causing unnecessary burdens for those who legitimately require access to the assets. Such a balance can be very difficult to achieve.

Threat protection is insufficient or disconnected

Inspecting the content of all traffic traversing a particular segment requires advanced threat protection capabilities, including SSL/TLS inspection, an intrusion prevention system (IPS), and web application firewall capabilities. A lack of pervasive advanced threat protection (ATP) results in an inability to detect the full range of threats, such as hackers spoofing the credentials of authorized users or malware hiding in encrypted web traffic. Unfortunately, many network segmentation solutions either are missing crucial ATP capabilities or experience significant performance degradation when these capabilities are turned on.

Security operations are inefficient and ineffective

Some organizations do deploy pervasive threat protection, but these capabilities exist in the form of disparate security appliances and software solutions that are managed through separate dashboards, typically by different staff members. This raises the total cost of ownership (TCO) of network security by increasing the costs of software adoption, support, operation, and training.

Even if they had the budget to expand the security team, CIOs would be hard-pressed to do so, as the cybersecurity skills gap widens. There are now millions more open jobs in the space than qualified candidates to fill them.[12]

Further, the lean teams working in most organizations must contend with a growing number of security alerts associated with myriad access control policies on siloed security solutions. Responding to all of these individually can overwhelm the staff. Moreover, the siloes themselves add risk, because they prevent the security team from seeing the entire network security apparatus in a single pane of glass. Managing access control policies across multiple networks, users, devices, and applications reduces the ability of security staff to respond to threats quickly and in a coordinated fashion.

CIOs need end-to-end security visibility, too. Without it, they have no way to accurately and continually assess the security posture to report to the CEO and board.

In an IDC survey, 37% of respondents reported receiving 10,000 security alerts each month; 52% of those alerts were false positives.[13]

Conclusion

CIOs are overwhelmingly committed to support DX with superior network performance, while protecting their organizations' users and IT assets. But network diversification and compliance requirements conspire to complicate network security. And traditional network-based segmentation strategies fall short. Many of the solutions in place today either give CIOs a false sense of security or lock down assets in a way that impedes productivity and undercuts business advantage. CIOs must find a better way to reduce security complexity so that it supports, rather than hampers, DX.

[1] "2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

[2] Ibid.

[3] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," Statista, accessed June 17, 2019.

[4] "Q3 2018 Threat Landscape Report," Fortinet, November 2018.

[5] Ionut Arghire, "Attackers Store Malware in Hidden Directories of Compromised HTTPS Sites," April 1, 2019.

[6] "Usage statistics and market share of WordPress," W3Techs, accessed July 31, 2019.

[7] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," Statista, accessed June 17, 2019.

[8] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," WIRED.com, March 3, 2016.

[9] John Maddison, "Is Converging Your IT and OT Networks Putting Your Organization at Risk?," Fortinet, May 9, 2018.

[10] Ibid.

[11] "2019 Data Breach Investigations Report," Verizon, June 2019.

[12] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

[13] "2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

FORTINET

www.fortinet.com

345418-0-A-EN

August 13, 2019 12:05 AM

eb-FA-understanding-the-underlying-causes-of-complexity-in-security