Whitepaper

Network Security: An Essential Element of Digital Transformation

Introduction

If IT transformation is about infrastructure modernization, digital transformation is about capitalizing on new technologies. The former is the groundwork, perhaps the less dazzling work; the latter enables innovation that can be more tangible, interacted with by end users. Both require changes to each component of the transformation trifecta — people, process, and technology.

However, digital transformation is something of a double-edged sword. On the one hand, opportunities such as the deployment of cloud-based services, expanded mobile infrastructures, edge computing, and the Internet of Things (IoT) can enable unprecedented agility, cost efficiencies, and connectivity.

On the other hand, these initiatives can also result in greater cybersecurity risk, more complex data governance, regulatory compliance issues, and other challenges for organizations. Organizations that are driving digital transformation will experience more traffic on their networks, more users, more devices, and more complexity. Because of all this, the attack surface is growing for cybercriminals looking to exploit opportunities.

These potential risks are by no means reasons to abandon a transformation strategy, however. Being a digital enterprise has become far too important for success in the modern business world.

But companies need to take the proper approach to building out a transformation strategy that takes into account key areas such as compliance, cloud readiness, and IT modernization. And they need to keep in mind the impact trends such as mobility/Bring Your Own Device (BYOD), the shift to the cloud, and the emergence of the Internet of Things (IoT) will have on each of these areas.

From a technology standpoint, they need to deploy effective network security solutions designed to address the growing attack surface. This whitepaper examines the challenges organizations are facing as they begin or expand their digital transformations, and provides suggestions to help them succeed on the transformation journey.

Key areas to consider:

- Compliance
- Cloud readiness
- IT modernization

Compliance requirements

Organizations today might be facing the most complex and demanding regulatory environment ever — at least as it pertains to the management and protection of data.

Long-standing regulations such as the Health Insurance Portability and Accountability Act (HIPAA) include requirements for organizations in the healthcare sector to protect the privacy and security of patient data. Other regulations apply to data protection in the financial services industry.

Meeting FDIC requirements

A large banking and wealth management services provider had to meet FDIC requirements for network control and visibility. Find out how we helped them design, deploy, and optimize a secure network infrastructure that would make compliance a breeze.

Read the case study

Newer regulations signed into law within the past several years include the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), both of which have broad repercussions with regards to consumer data collection and use. A 2019 Cisco study revealed that, while 97% of respondents said that GDPR applied to their firms, only 59% are meeting all or most GDPR stipulations[1]. The CCPA, widely viewed as a GDPR copycat law, will impact all businesses with consumers residing in the state of California once it goes into effect in 2020.

The expansion of mobile environments and BYOD, the rise of IoT, and the dramatic increase in contracted cloud services have huge implications for regulatory compliance. That's because they all expand the attack surface significantly, by increasing the number of endpoints within an enterprise domain and broadening access to data and applications.

Research firm International Data Corp. (IDC) has estimated that by 2020

1 million

devices will go online every hour

creating even more potential attack points for hackers[2]

Gartner Inc. "forecasts that

14.2 billion

connected things will be in use in 2019, and that the total will reach

25 billion

by 2021, producing immense volume of data.[3]"

As more traffic hits corporate networks, it is easier for organizations to lose visibility of exactly what and who is on the networks. And if they can't even see what's accessing their networks in real time, companies will have an even bigger challenge securing networks across all devices and users for proactive protection against threats.

The growing attack surface combined with limited visibility means attacks become inevitable.

This is a major challenge in terms of compliance, because regulations require that organizations protect sensitive customer data that is stored or used on mobile devices, or moving to and from the cloud. The same goes for data gathered by IoT devices and then delivered to the cloud, to on-premises data centers, or to analytics platforms.

The key question regarding compliance: Is the organization as secure as it can be in this new environment? Companies need to have in place best practices for:

- Governance
- Risk mitigation
- Technology that enables network visibility and access control

Readiness for the cloud

Moving data and workloads to the cloud clearly makes sense for a lot of organizations today — and many are doing just that.

> In a 2018 press release, Gartner estimated that "the worldwide public cloud services market is projected to grow
> **17.3 percent** in 2019 to total **$206.2 billion,**
> up from **$175.8 billion** in 2018[4]"

Cloud infrastructure services are growing at an impressive rate, driven by demand for integrated IaaS and PaaS offerings. According to Gartner, "Software as a service (SaaS) remains the largest segment of the cloud market with revenue expected to grow 17.8 percent to reach $85.1 billion in 2019.[4]"

A key question for organizations looking to deploy these services is how truly prepared are they for the cloud, particularly from data management and cybersecurity standpoints? Do they completely understand their responsibilities versus those of cloud service providers?

Industry research has shown that there is a lot of misconception or confusion regarding who's responsible for what, with many IT and business executives thinking it's up to the service providers to handle all cybersecurity provisions. They don't have a clear sense of the various roles and responsibilities, including what cloud customers should be doing and what can be left to cloud providers to handle.

Good management in a cloud environment includes having a thorough understanding of what has to be handled internally with regard to:

- Security networks
- Applications
- Data

There are also performance issues to consider. As more data is moved to the cloud, that means larger volumes of data are traversing the network. As a result, networks have to be architected differently in order to accommodate this increased volume, and organizations will need to turn to new solutions such as software-defined WANs to help them deal with the demands while keeping costs low and bandwidth high.

One big network refresh

Post-audit, a large multinational conglomerate deemed its network architecture inadequate and high-risk. Learn how we designed and deployed a compliant solution architecture that effectively segmented growing and diverse data and users.

Read the case study

Organizations need to make sure that their networks are ready for the cloud, including re-architecting to manage the change in traffic flow, inclusive of security considerations. The move to the cloud, whether it's a public, private, or a hybrid cloud approach, is driving change in the way networks are designed and architected. On-demand data gathered from a multitude of sources requires an overhaul of legacy approaches.

From an organizational standpoint, enterprises also need to make sure they have the management structure and internal expertise in place to manage multiple cloud services, migrate data and workloads from on-premises systems to the cloud, and maintain those resources following the move to the cloud.

IT modernization

The third key area organizations need to focus on is the modernization of their IT environment, including the data center. Aging networking technologies were not designed for today's fast-growing data transmission demands, and because of this, legacy technologies can have a negative effect on organizational performance.

In a 2018 report, IDC noted, "given the imperative of digital transformation and the need to support cloud-native applications and to deliver cloud-like agility, enterprises are compelled to modernize their data center network architectures and operational models." Fortunately, the firm said, practical and viable options for data center software-defined networks are available that address the requirements associated with a broad range of workloads and use cases.

To fully succeed in realizing their digital transformation objectives, enterprises must modernize and transform their network infrastructure, IDC said. Nowhere is this truer than on the WAN, the firm noted, which is critical to the productivity of employees, the satisfaction of customers, and the execution of transactions at branch offices and remote sites.[5]

An IDC Market Forecast in 2018 reported "striking growth" in the SD-WAN infrastructure market, and there is more to come, driven by the increasingly sophisticated requirements of organizations.[6]

Research firm Vertical Systems Group in December 2018 released a report **estimating that the carrier-based managed SD-WAN services market would reach more than $282 million in 2018.**

The firm defines a managed SD-WAN service as a carrier-grade network offering for enterprise and business customers, managed by a network operator and delivered over a software-defined network (SDN) service architecture that has separate control and data planes.

In 2019 Vertical Systems Group expects a major boost in revenue, with network operators fully ramped up to sell, deliver, and support managed SD-WAN services.[7]

Enabling 3X growth

Exponential business expansion was imminent for a large U.S. bottler and distributor, however its network infrastructure had significant shortcomings. Discover how we helped them build a scalable and fault-tolerant infrastructure.

Read the case study

With the exponentially growing number of users needing access at an all-time high, more people are connected directly to critical data within networks than ever. A non-modernized network can result in system crashes and downtime, cybersecurity gaps, decreased worker productivity, and growing costs associated with maintenance and support.

Without modernizing their IT infrastructures, including corporate networks, organizations will not be prepared to handle the growing volume of mobile traffic or the increasing demands for IoT-related data.

As part of IT modernization, the approach to securing networks needs to change dramatically. High-definition wireless is replacing the traditional wired LAN, and software-defined fabric is quickly replacing traditional architectures.

Deploying the right solutions

For organizations to be able to address the expanded attack surface that results from digital transformation, it is important to have a solid network security infrastructure in place. This can help companies deal with the issues of compliance, cloud readiness, and modernization.

Companies seeking third-party support should look for an integrated networking and security portfolio that ideally includes not just the technology components, but consulting and managed services as well. This includes network assessments, strategic planning, network design, deployment of equipment, adoption of new technologies such as SD-WAN, and support around these solutions.

The reason why comprehensive support is needed, is the growing complexity of the IT and networking environment. Few organizations have the in-house expertise and experience to fully understand the interplay of areas such as IoT, mobility, and the cloud. Even the largest enterprises are likely to find skills gaps when it comes to newer areas such as IoT.

The network security technology itself should include features and capabilities such as software-defined networking and software-defined data centers, analytics based on machine learning (ML) and artificial intelligence (AI), network access control, next-generation firewalls, endpoint security, microsegmentation, and cloud security.

Because few IT and security vendors offer such a broad array of technologies, organizations will likely need to tap solutions from multiple vendors that come packaged as an integrated solution. Given this scenario, strong integration among these various components will be vital.

The technology exists today to enable organizations to deploy a secure network solution stack that addresses existing and emerging compliance requirements, and at the same time enables enterprises to modernize their networks and prepare for the growth of cloud services.

These solutions include software-defined networks and SD-WANs to deliver software-defined capabilities; anti-malware and other tools to provide endpoint security; machine learning and artificial intelligence to provide behavioral analytics; monitoring, authentication, authorization, and microsegmentation to provide network visibility, access control, and richer context; and virtual private networking to provide network access.

Something important to consider when deploying all of these new technologies:

Network security solutions should provide the ability to protect systems and data in growing environments while not impeding performance or increasing complexity.

If new solutions degrade network performance or user experience, they will not be embraced by end users and could end up costing organizations a lot of money in the long run through lost productivity. Adding more complexity could also lead to higher costs.

Summary and conclusion

As part of their efforts to help launch digital transformation strategies at their organizations, CIOs and other IT executives, as well as network managers, need to ensure that the enterprise network is ready for the changes.

Many companies today are facing challenges such as frequent network events that impact performance and reliability; a lack of network architecture standardization and consistency; a lack of centralized network device authentication, which creates vulnerabilities; and a lack of visibility, monitoring, and segmentation of users on the network that they need to proactively identify and mitigate security threats.

They also are struggling to keep up with new and increasingly complex requirements, as well as pass required audits; and are grappling with the problem of having end-of-support technologies that are causing frequent downtime for users in the organization and impeding the ability to do business.

All of these challenges can hinder a company's digital transformation initiatives. The good news is, with the right technology and process solutions in place, these hurdles can be effectively addressed.

Additional resources

It has never been more important for organizations to integrate networking and security technologies. They need to have visibility into what is happening on their networks at all times, the ability to defend their networks against increasingly complex and persistent threats, and the automation to streamline the response to and containment of threats.

You probably have questions of your own about network security and may benefit from expert guidance. Visit us at solutions.insight.com to request a meeting and/or find out about our assessments, solutions, and consulting services for secure networking.

You might also find the following resources helpful:

- Whitepaper: "Transforming Network Security: How to Win Against Cyberthreats"
- Whitepaper: "Moving Workloads to the Public Cloud? Don't Forget About Security."
- Whitepaper: "Building a Strong Cyber Security Program During IT Transformation"

Follow us online to stay up to date and receive the latest news in data center technologies and practices:

1 Cisco. (2019, Jan. 24). Cisco 2019 Data Privacy Benchmark Study Shows Organizations Gaining Business Benefits from Data Privacy Investments.

2 Liu, J. (2017, Jan. 9). 2017 Enterprise Network Security Trends. Cisco.

3 Gartner Press Release, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", November 7, 2018. https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

4 Gartner Press Release, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019", September 12, 2018. https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019

5 IDC, IDC Innovators: Datacenter Software-Defined Networking, 2018, Doc #: US43436718, Mar. 2018.

6 IDC, Worldwide SD-WAN Infrastructure Forecast, 2018–2022, Doc #: US44182618, Aug. 2018.

7 Vertical Systems Group. (2018, Dec. 6). STATFlash: Managed SD-WAN Services Market Tops $282 Million in the U.S.

Insight

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes, and technologies. We believe the best path to digital transformation is integrative, responsive, and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at:
solutions.insight.com
insight.com