POINT OF VIEW

Digital Acceleration Requires Converged Security and Networking

Executive Summary

Today's businesses are under pressure to establish and maintain market differentiation by improving processes faster than competitors and delivering higher efficiency, while increasing stakeholder value. Digital acceleration is necessary to achieve these objectives. It enables organizations to roll out new products and services at the speed business requires, while delivering the optimal experience for all types of users.

For digital acceleration to succeed, however, networks must do more than they did in the past—often much more than they were originally designed to do. Pushing networks beyond their limits generally results in increased risk of network downtime and security breaches.

That's why a new approach is needed that converges networking and security into a single solution. Secure networking minimizes risk while enabling the key functions that digital acceleration requires in order to meet business goals.

"When asked about the biggest challenges to digital transformation, the top responses include: cybersecurity (37% of respondents), data interoperability (29%), and legacy technology (22%)."[2]

Increasing Demands on the Network

Digital acceleration brings many benefits, but it also negatively impacts the network, which is being asked to take on more roles than ever before.

Organizations add solutions to improve business agility, but those applications are not all structured the same way or hosted in the same location. They may be available only to those on the corporate network or available to everyone, and they may be hosted in a public or private cloud, or on-premises. This variance creates complexity for IT, and an increased risk of mis-applying permissions or security settings for these applications.

In conjunction with this, the workforce is becoming more mobile and moves between locations far more fluidly than in the past. This hybrid workforce still needs constant, secure access to resources both inside and outside the corporate network. This mobility brings more security and network access challenges than on-site workers created in the past.

Another new development is the installation of automated control systems in buildings, such as air conditioning and lighting. These systems often leverage Internet-of-Things (IoT) devices with various capabilities and security postures that are spread throughout the site. In some cases, these IoT and system footprints can start to blur the previously established lines so much that they cause challenges that were previously limited to operational technology (OT) installations beyond the carpeted space.

Compounded Risk

A key downside to digital acceleration is the increased risk to the network. Oftentimes when IT teams are moving fast, security comes as an afterthought.

Cybersecurity risk from digital acceleration comes from several factors:

Network downtime is a common occurrence, whether it stems from an attack or just something complicated going wrong with the infrastructure. This can easily happen with digital acceleration, as quite often, disparate systems are not adequately tested with one another, leading to an interoperability issue. Network downtime brings digital acceleration technologies to a screeching halt, greatly impacting productivity.

Complexity of the overall system increases as more and more new applications and technologies come online, making it difficult to maintain effective security. This increases risk to any digital acceleration initiative as there often isn't time to go back and secure everything. These insecure networks are vulnerable to attacks and data loss. IT needs the ability to set policy centrally and reliably push it to all corners of the network so settings don't drift and leave security gaps.

Internet-of-Things devices are being added in campus environments to control systems that in the past were primarily seen in only in OT deployments. These devices are notorious for their lack of security. And in situations like this, any risk to the network can also become a risk to personal comfort and (in extreme cases) personal safety.

On a more individual level, the IT team is responsible for keeping up with all these changes. If anything is missed or problems arise, jobs could be at stake. There is a level of professional risk that IT teams should be aware of as well.

Benefits of Secure Networking

By bringing together networking and security equipment in a converged solution in a hybrid mesh firewall (HMF) environment, secure networking creates unmatched efficiency and closes security gaps. Only secure networking can solve the challenges brought by digital acceleration's rapid expansion of attack surfaces, creation of new edges, and remote access requirements, while delivering a better user experience. An HMF environment:

- Provides more effective security
- Eases management of networking and security with unified management and policies
- Reduces the chances for misconfiguration
- Eliminates confusing licenses and subscriptions
- Leverages artificial intelligence (AI)-based insights
- Lowers total cost of ownership (TCO)

With secure networking, IT groups can reduce the risk to their networks by installing an intuitive architecture that includes the necessary security and management features in one centrally managed solution.

[1] "Accelerating digital: a win-win-win for customer experience, the environment, and business growth," The Economist, 2022.

[2] Ibid.

FORTINET

www.fortinet.com

May 26, 2023 2:56 AM

1950331-A-0-EN