POINT OF VIEW

Seven Major Challenges Impeding Digital Acceleration

The Era of Digital Innovation

In today's digital marketplace, speed and availability are essential. Organizations turned to digital innovation to remain competitive, trading their legacy systems for hybrid networks and digital processes, including cloud and business application adoption. The success of this transition, both in terms of customer satisfaction and user productivity, resulted in the most sweeping transformation of business networks in 40 years. And this journey has just begun.

Digital Acceleration and Hybrid IT are Transformational

Today's digital acceleration and hybrid IT architecture strategies enable organizations to roll out new products and services at increasing speed, streamlining time to market, and optimizing user and customer experience. The ongoing objective is to establish and maintain market differentiation by improving processes faster than competitors, allowing organizations to improve efficiency while improving stakeholder value.

Digital acceleration enables organizations to build processes and systems that will help them do more, faster. This requires converging traditionally separate networks to create highly efficient hybrid environments. This includes seamlessly tying physical campus and data center networks to private and public cloud environments, interconnecting branch offices, and providing ubiquitous access to the rapidly growing number of remote users. These hybrid, dynamic environments allow IT teams to create fast lanes for building, implementing, interconnecting, and managing critical technologies and processes, whether internally or externally based, to deliver better outcomes.

The Impact of Digital Transformation

Digital acceleration is transforming how organizations conduct business. Online retailers now allow customers to place orders using a variety of apps, enabling such things as online ordering, same-day delivery, and touchless curbside pickup. Most insurance companies now offer no-touch claim filing and inspection. And enterprises can support a hybrid, work-from-anywhere workforce with secure access and consistent security. Regulations have also changed to support these innovations. For example, e-signatures now meet compliance regulations, enabling people to engage in legal transactions remotely. Even traditionally stoic OT networks have embraced digital innovation, enabling real-time production using Industry 4.0 AR/VR-initiated design and manufacturing.

Hybrid IT is Essential to Successfully Compete in Today's Marketplace

Implementing digital acceleration has required traditional IT to evolve. Static perimeters and fixed networks are being disrupted with new applications and services that provide greater access to critical information for any user on any device from any location. The adoption of hybrid IT architectures interconnects traditionally fixed network environments such as campuses, data centers, branches, and retail locations. By combining physical and virtual networks across private and public domains, hybrid IT offers true end-to-end, scale-on-demand capabilities to meet escalating business needs.

Hybrid IT Must Include Hybrid Cloud

But interconnected networks are not enough. To ensure a consistent user experience for users and devices everywhere, especially for the sudden growth of a hybrid workforce splitting time between on- and off-premises offices, IT teams have had to interconnect their hybrid IT networks with the cloud. Hybrid cloud connects traditional networks and private cloud environments to public clouds. Open and integrated APIs have allowed IT teams to combine resiliency and operational efficiency with agility and availability. Hybrid data centers, for example, can now deliver critical data to distributed users and devices anywhere. This has enabled streamlined workflows and allowed networks to adapt to shifting business demands in real time.

Seven Security Challenges That Can Disrupt Hybrid IT Digital Acceleration

The transition to hybrid strategies—networks, clouds, and users—has stretched legacy security systems to the breaking point. Most traditional security systems were designed to analyze and secure data at fixed points in the network, with clearly defined perimeters and reliable sources and destinations. New hybrid environments, spurred on by the need for ongoing digital acceleration, have changed all that. Rather than protecting businesses, the inherent limitations of traditional security systems now restrict an organization's ability to securely evolve its networks at the speeds that today's digital marketplace demands.

There are seven critical security issues that any organization looking to successfully adopt digital acceleration strategies and deploy hybrid network solutions must address:

- **Increased attack surface:** Hybrid networks and a diverse workforce mean that today's networks have more locations, applications, and services to protect. The effort to continually deploy new security technologies to protect the expanding network has overwhelmed many IT teams already struggling to cope with the ongoing cybersecurity skills gap.
- **Diverse and sophisticated attacks:** Today's threats not only employ increasingly sophisticated attack strategies to exploit vulnerabilities and evade detection, but they also target multiple points across the network, looking for the weakest link in the security chain. And new API-based attacks specifically target applications designed to interact with each other within the same domain or that work with partner applications using vulnerable APIs to quickly spread from one area of the network to another.
- **New threats targeting OT networks:** IoT/IIoT-based attacks are emerging designed to target Industry 4.0 and such things as AI for robotics control, near-real-time digital twins, production line automation, and more. And because of the growing number of high-profile OT and critical infrastructure attacks, we have also begun to see OT attacks—traditionally the domain of very specialized criminals—being sold on the dark web as a service. This means that organizations should expect to see the volume of OT-targeted attacks rise as novice cybercriminals gain access to sophisticated attack technologies.
- **Inconsistent security:** Users, devices, and applications can be anywhere. Not all security solutions can say the same. And when security solutions and platforms cannot be universally deployed or centrally managed and orchestrated, it can be impossible to deliver consistent and location-agnostic security across the hybrid network.
- **Lack of visibility:** The growing number of security systems that cannot interoperate, combined with the ever-increasing volume of encrypted traffic, means that IT teams are increasingly trying to combat today's threats while blindfolded. Multi-vector attacks exploit the inability of security solutions to share and correlate threat data. And attackers know that most security solutions cannot inspect encrypted traffic to find malware or exfiltrated data without seriously impacting network performance and user experience. And that when it comes to choosing performance or protection, most organizations opt for business expediency.

- **Complexity:** With few exceptions, multivendor security systems cannot talk to each other, which means IT teams must rely on hand-correlating threat intelligence to detect and respond to threats. And trying to stay ahead of an ever-evolving threat landscape using multiple management consoles not only increases operational costs but also makes it difficult to troubleshoot issues, identify exploitable configuration gaps, or initiate a timely response to identified threats.
- **Lack of integration and coordination:** Disparate security systems that do not share information can make it impossible to make effective decisions. In most networks, on-premises applications and physical infrastructures struggle to coordinate and communicate with cloud applications and networks. As a result, if one gets attacked, there is no integrated mechanism to even notify the other, let alone initiate appropriate protections.

Hybrid Environments Require Integrated Security

Protecting today's networks requires an integrated approach to security. That starts by developing and deploying a security fabric that can scale in lockstep with the network to provide consistent protection and policy enforcement everywhere. This requires two things. The first is tools able to converge networking and security into a single solution so protections can seamlessly adapt to changes in the underlying network. And the second is a security platform that includes a full suite of security tools designed to work together as a single system, along with open standards and APIs so it can also interoperate with third-party solutions. It also needs to be deployed anywhere, in any form factor, from home offices to large campuses and hybrid data centers to distributed branches and across every public cloud. This enables things like true end-to-end automation for the rapid detection and coordination of response to threats, centralized management and orchestration to eliminate troubleshooting and configuration errors, and hyperscalability so security can quickly and easily adapt to ongoing digital innovation efforts.

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 3, 2022 11:02 AM
1500053-0-0-EN