CYBERSECURITY AS A BUSINESS GROWTH ENABLER

What's Inside

Digital Solutions Help Businesses Remain Relevant

In recent years, rapid digital transformation and cloud innovation have become integral factors empowering organizations to become more agile and adaptive to changing market demands. The ability to simultaneously boost profits, improve customer and partner engagements, and increase employee productivity speaks to the value of using new cloud services and applications.

Organizations must respond to new customer and employee behaviors and shift business models by continuously launching web applications, building application programming interfaces (APIs), and deploying Internet of Things (IoT) networks.

IoT devices are everywhere, and with 5G, they are reshaping how we connect.

Developers deploy code multiple times a day, once a day, or once every few days.[1]

More than 70% of all departments and teams are expected to have remote workers by 2028.[2]

IT and security teams need to protect their diverse network infrastructure, edge computing devices, remote users, and IoT devices that present new security vulnerabilities. The pressure to proceed with digital transformation initiatives continues to intensify, yet 62% of businesses have delayed application rollouts because of API security concerns.[3]

At the same time, IT and security teams lack the people, processes, and technology to stay ahead of continually evolving, sophisticated threats. The risk of cybersecurity threats is a constant source of delays in moving forward with transformation.

1. "DevOps is getting code released faster than ever. But security is lagging behind," TechRepublic, 2021.
2. "4 Reasons Cybersecurity Attack Surfaces are Expanding," DEVFUZIN, March 16, 2022.
3. "Concerns Over API Security Grow as Attacks Increase," DARKReading, 2021.'
4. "The Forbes CxO Growth Survey," Forbes, February 11, 2021.
5. "37 Digital Transformation Statistics," Zippia, April 26, 2022.
6. "How Security and Risk Leaders Can Prepare for Reduced Budgets," Gartner, July 7, 2020.

The C-suite is finding new ways to build resiliency into its business

70%+

More than 70% of CIOs increased technology investments to improve the customer experience and drive digital transformation.[4]

56%

56% of CEOs said that their digital improvements have already improved their profits.[5]

2023

Gartner found that by 2023, 30% of CISOs will be measured on their ability to create value for their business.[6]

Cybersecurity Remains a Top Challenge

The rise of ransomware attacks, email-borne threats, and simple user error puts assets and data at greater risk, whether on-premises, in the cloud, on devices, or at the enterprise edge. Networks are more distributed than ever before—creating new network edges and a much expanded attack surface. According to the 2021 Flexera State of the Cloud report, 92% of enterprises have a multi-cloud strategy, and 80% have a hybrid cloud strategy in place.[7] On average, enterprises use at least two public and two private clouds.

The current trend of digital acceleration and hybrid work models has accelerated the expansion of the traditional local-area network (LAN), wide-area network (WAN), and data center edges. The new landscape includes multiple hybrid cloud environments, more agile WANs, Software-defined (SD)-Branches, and IoT networks.

Organizations become burdened with disparate security tools and are unable to consolidate policy management or use consistent security intelligence across their ecosystem. Keeping up with the speed and scale of cyberattacks is not easy, and organizations of all sizes are facing a number of challenges, including:

Sophisticated Cyberattacks

Cyber-threat actors use formal and informal teaming arrangements, as well as machine learning and AI to continually refine their tactics, techniques, and procedures. From automated, opportunistic attacks to targeted campaigns—there's no letup in the speed and sophistication of threats.

Anywhere, Everywhere Infrastructure Security

From multi-cloud, hybrid cloud, edge computing, BYOD, and IoT to work-from-anywhere (WFA), computing is more distributed and decentralized than ever before. This drives a requirement for consistent network and security performance for any user, from any location, on any device. Traditional siloed solutions simply can't keep pace with the volume, variety, and velocity of today's network challenges and cyberattacks.

Strained IT and Security Teams

Accelerated cloud adoption and digital acceleration is generating more complexity and alerts than security teams can manage. Overwhelming workloads, compounded by a lack of skills and expertise, strain the ability of even the largest teams to manage risk.

7. "Flexera 2021 State of the Cloud Report," Flexera, 2021.

Why the C-Suite Has Its Eye on Security

Connecting customers, employees, and partners from any location and any device expands the attack surface and creates new risks. New software development can expose sensitive data to potential cyber threats. Security is the biggest challenge for 66% of companies using the public cloud.[8] Moving from legacy providers and expensive multiprotocol label switching (MPLS) circuits to support digital transformation is only possible if security can be assured.

New CISO Responsibilities

The primary responsibility of CISOs has evolved from company-wide cybersecurity to business enablement and risk management. CISOs convey cyber risk in financial terms to both the C-suite and boards. They are expected to demonstrate cybersecurity return on investment (ROI) and how their initiatives support better business outcomes and user experiences.

Security is a Priority

Security can no longer be an afterthought. Security needs to be integral across the entire software development life cycle—not just when it goes into production. Indeed, from the DevOps process to life cycle management, security should be built into every part of the digital enterprise.

IT/OT Convergence

Digital innovation is driving more integration of operational technology (OT) systems with information technology systems. OT network components like control systems, supervisory control and data acquisition (SCADA), and industrial networks now connect to IT network components such as processors, storage, and systems management. OT systems are also interacting with cloud–based corporate resources—expanding the attack surface and increasing the level of complexity facing CISOs and their teams.

75%

CEOs

75% of CEOs believe a strong cyber strategy is critical to engender trust with key stakeholders.[9]

57%

CIOs

57% of CIOs said the current socioeconomic pressures caused them to increase cybersecurity protections.[10]

CISOs

CISOs can expect increased scrutiny and expectations, alongside an increase in support and resources.[11]

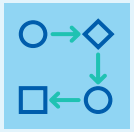
8. "Cloud Vision 2020: The Future of the Cloud," LogicMonitor, 2019.
9. "Cyber security considerations 2022," KPMG.
10. "How to balance security and agility in the cloud," Ernst and Young, 2021.
11. "Proving the ROI of Cybersecurity," MSSP Alert by Fortinet, December 3, 2021.

Obstacles to Business Growth

As organizations accelerate digital transformation, their cyber landscape expands, and network complexity increases. At the same time, cyber threats are becoming increasingly automated and innovative. Delivering the expected secure, high-performing user-to-application connection can be categorized into these three significant challenges for most organizations.

People

IT and security teams find it more challenging to keep up with the growth in digital projects. A study found that the cybersecurity talent shortage has affected more than half of organizations,[12] and the cyber professional shortfall could rise to 3.5 million by 2025.[13] The talent shortage is the most significant adoption barrier to 64% of emerging technologies.[14]



Processes

Many organizations work without automated processes, relying on clunky manual administration, which leads to significant security risks by human error. Cybersecurity professionals (67%) stated that misconfigurations remain the most significant cloud security risk facing their companies,[15] and reports say that 95% of cybersecurity breaches were made possible by human error.[16]

Technology

Cyberattacks are rising globally; ransomware attacks happen every 11 seconds,[17] and cyber criminals are well-organized, earning $1.5 trillion every year.[18] The best way to outsmart cyber criminals is to provide comprehensive cybersecurity protection for all users, devices, and applications across all network edges.

12. "Upskilling, better training keys to increasing cyber talent pool," Technology Executive Council, 2022.
13. "Hackers' Path Eased as 600,000 U.S. Cybersecurity Jobs Sit Empty," Bloomberg, March 30, 2022.
14. "Gartner Survey Reveals Talent Shortages as Biggest Barrier to Emerging Technologies Adoption," Gartner, 2021.
15. "3 Cloud Security Challenges for CISOs to Address," Fortinet blog, December 15, 2021.
16. "CISOs: Top Cloud Security Threats You Should Know About," Security Boulevard, February 24, 2022.
17. "Ransomware Statistics in 2022: From Random Barrages to Targeted Hits," DataProt, April 20, 2022.
18. "More Than 70 Cybercrime Statistics – A $6 Trillion Problem," DataProt, March 14, 2022.

4 Ways Cybersecurity Helps You Exceed Business Goals

Organizations that prioritize cybersecurity are positioned to overcome the challenges of people, processes, and technology, allowing them to stay competitive and relevant in their industry.

1 Enable a Secure Working Environment

Challenge

The demand for secure remote access has shifted IT operations to support WFA practically overnight. In favor of speed, many businesses opted for ad-hoc solutions. Now organizations need a more measured approach as WFA becomes a more permanent part of the landscape.

Solution

WFA increases the need for consistent networking and security from any location. It is crucial for organizations to provide advanced security against ransomware and other risks associated with remote work and distributed computing. Insider threat incidents have risen 44% over the past two years. Securing WFA prevents financial losses from a cybersecurity breach, eroding customer trust, and reputation damage.[19]

19. "2022 Ponemon Cost of Insider Threats Global Report," Ponemon Institute.

2 Provide Holistic Visibility and Control Across the Enterprise, Allowing IT Teams to Spend More Time on Strategic Projects That Drive Your Organization Forward

Challenge

Organizations no longer have physically defined perimeters. This means that the attack surface extends well beyond traditional boundaries due to the expansion of cloud adoption, WFA, connected platforms, and edge computing. As a result, most organizations end up with heterogeneous technologies with disparate security controls in various cloud environments.

Solution

A Cybersecurity Mesh Architecture (CSMA) provides integrated security tools that work as a collaborative ecosystem. This approach enables centralized management for security consolidation to deliver a simplified, end-to-end security infrastructure. By 2024, organizations adopting a CSMA will reduce the financial impact of security incidents by an average of 90%.[20] CSMA frees internal resources to future-proof your environment as you scale and brings new digital priorities online.

20. "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Gartner, 2022.

3 Reduce the Risk of Security Breaches

Challenge

Managing risk can be difficult and ineffective because many built-in security tools for various cloud providers are proprietary and incompatible. The shortage of cybersecurity professionals substantially compounds the risk. In fact, worldwide, 80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills or awareness.[21]

Solution

Consolidating security technologies and use cases into a simplified, single policy and management framework enables organizations to provide comprehensive, real-time cybersecurity protection for users and applications. Cybersecurity that correlates events through machine learning and workflow automation eases demands on security skills, sandboxing can defend against zero-day threats, and honeypots provide additional protection.

21. "2022 Cybersecurity Skills Gap," Fortinet Global Research Report, 2022.

4 Deliver Continuous Security Compliance While Protecting Customer Data

Challenge

Organizations are subject to regulatory and standards compliance requirements ranging from the Payment Card Industry Data Security Standard (PCI DSS) to the European Union's General Data Protection Regulation (GDPR), with the latter affecting every organization with European customers.

Solution

Complying with PCI DSS, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), GDPR, and other regulatory mandates that are designed to protect organizations. Compliance failures can lead to unauthorized disclosure of personal information, identity theft, and potential lawsuits. Implementing cybersecurity practices enables organizations to mitigate risk and maintain business continuity.

Drive Business Growth and Cyber Resilience With Hughes and Fortinet

With continued pressure to accelerate time-to-market, improve innovation, and deliver consistent user experiences, organizations need partners to help ease the process. Here's how Hughes and Fortinet can support your digital transformation initiatives and journey.

Tap Into Resources

Hughes, a Managed Security Service Provider (MSSP) with more than 40 years of experience, can help you manage some or all of your cybersecurity, freeing your internal staff to focus on strategic projects that drive your organization forward. With a deep knowledge of customers' business models, Hughes is a true partner with the ability to help you implement your business initiatives securely, with predictable outcomes. Hughes can also partner with you at a strategic level with networking, broadband, and security experts using Fortinet's best-in-class security solutions and leading threat protection.

Manage Risk and Conduct Business with Confidence

As you prepare for new application launches to meet business and customer demands, you need to minimize the risk of a cyberattack. Domain experts within Hughes' Security Operations Center combine event data, analytics, and discovery tools to create a strategy that maintains your security visibility and protects your data, your customers, and your reputation. Paired with Fortinet's security solutions and threat protection, services from Hughes can empower your developers to focus on delivering code without worrying about security. At the same time, your IT teams can shift their focus to strategic projects that help drive your organization forward.

Go From Legacy Providers to Secure SD-WAN

With Hughes, security is never an afterthought. Get the essentials for better business outcomes and user experience with a complete SD-WAN offering from Hughes that integrates security and networking solutions to ensure seamless visibility, control, and responsiveness. Security is built into every SD-WAN solution with Hughes and tailored to your specific business needs. This means that leaving MPLS doesn't mean giving up on effective cyber defense.

Protect Your Infrastructure

Together, Hughes and Fortinet provide services and solutions that help you enhance your ability to quickly embark on new transformation initiatives while keeping your infrastructure protected from cyber criminals. As an "Expert" level Fortinet Partner, Hughes can help you create purpose-built and tailored solutions with security at the forefront.

Accelerate Your Digital Journey With Confidence

Hughes and Fortinet can help your organization enhance your ROI by adopting a broad, integrated, and automated security fabric supported by customized solutions to meet your needs and accelerate your digital journey.

Hughes integrates broadband and WAN technologies with Fortinet's best-in-class security solutions to exceed your business goals. As a Fortinet Partner, Hughes has a proven track record, highly skilled and experienced security consultants, and security-certified SOC engineers to customize a solution to meet your business needs. Complement your staff's expertise with the Hughes Managed Services portfolio of turnkey, fully managed enterprise solutions and gain predictable operational and financial outcomes.

When you have confidence in the security and compliance of your entire IT ecosystem, you will be able to bring new applications and solutions to market faster and get on a path to exceeding the expectations of your customers, partners, and employees.

To get started on your digital transformation journey, just complete Hughes' Cloud Security Posture Assessment for an evaluation of how to improve your overall security posture.

Learn more about Hughes Managed Cybersecurity Services

HUGHES
An EchoStar Company

FORTINET