White paper

New technologies require a modernized security approach.

verizon

Cybersecurity demands C-level attention as part of your digital innovation strategy.

Transformational new technologies are moving companies closer to being real-time enterprises that are capable of operating in ways that were once unimaginable. Artificial intelligence (AI), 5G networking, blockchain and machine learning (ML) all enable companies to run faster, smarter and better than ever before.

But digital transformation also brings risk. As networks become more complex and torrents of customer data become a core corporate asset, security is more important than ever, and smart companies know not to let innovation outpace security oversight.

You can't embrace the future if your security approach is stuck in the past.

Cybersecurity practices need not interfere with outcomes or operations. The trick is to align them, not put them in opposition. Legacy organization can hold you back as surely as legacy technology. When you modernize your organization along with your infrastructure, you can anticipate threats, prevent breaches, and detect and respond to them when they occur.

How new technologies can help

New technologies can help you build a secure business, although it's important to remember that security lies not in the technology itself but in the way it's implemented. Even the most secure technology will be vulnerable in a flawed deployment.

You have certainly heard of the bandwidth, speed and latency advantages of 5G networks. From autonomous and connected vehicles to remote surgical tools, 5G-fueled applications will fundamentally transform every industry.

A poorly secured database or misconfigured application remains a security risk under 5G, as it would on any network. But you should also know that 5G networks are being built with multiple layers of inherent security, from vigorous supply-chain scrutiny to ensure that only secure components are used, all the way through to complex authentication and data encryption techniques for devices connecting to 5G.

5G networks are built with security in mind, from the sourcing of components to authentication and encryption of endpoint devices.

Blockchain has an undeserved reputation for mystery and complexity. But the possibilities of blockchain—a distributed and unalterable database of transactions—go far beyond cybercurrency into the realm of managing digital identities and securing supply chains. A security technology leveraging the characteristics of blockchain called Machine State Integrity can help detect cloud misconfigurations and evidence of tampering with the assets connected to your network in near real time.

Don't get caught up in the math and hype behind the tool. When a partner vendor proposes a blockchain-based solution, focus on the measurable and practical security benefits and results it delivers.

Use blockchain's secure ledger to make sure that system configurations haven't been hacked

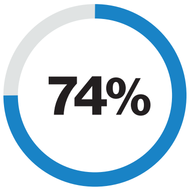
AI and ML are increasingly the driving forces behind a number of advanced cybersecurity tools. ML automates many facets of threat hunting, a critical but time-consuming security activity designed to find bad actors who have compromised corporate IT systems. ML-driven threat hunting systems may reduce time to detection from 200-plus days on average to just a few hours.

Secure innovation demands top-level attention.

With new transformational networks come floods of new endpoint devices like bring-your-own-device (BYOD) smartphones or sensors on the Internet of Things (IoT). They present a problem not because they're inherently insecure (although badly managed IoT devices are notorious for being hijacked by botnets). Rather, chronically underfunded security teams are too often forced to use last-gen tools to manage next-gen networks, like playing Whac-A-Mole® to respond to threats instead of taking a long-term strategic view that will ultimately save money and improve outcomes.

Another operational threat is a global shortage of qualified security workers. Too many companies are struggling to cover the cybersecurity basics, including vulnerability management, risk assessment and incident response planning. If your company is one of them, you can't move forward with transformation because you can't safely manage what you have. Consider partnering with a trusted advisor or managed services company to take on some of the day-to-day security work so you can focus on larger, more strategic issues.

Ultimately, underfunded and overlooked security efforts are often a symptom of organizational misalignment. The security of your data and networks is as important as—if not more important than—the security of your physical assets. It demands C-suite attention, not just during the transformation process but on an ongoing operational basis.



Seventy-four percent of healthcare leaders report that security concerns frequently or occasionally stall digital transformation initiatives.[1]

Figuring out how to successfully leverage advanced technologies for business gain is the responsibility of all leaders in an enterprise, not just the IT department. Some of the solution lies in thinking about security in every technology discussion. But also key is fostering a learning culture where people in disparate roles make an effort to better understand the business context and security ramifications of next-gen tech. If businesses embrace new and exciting technologies hastily, they run the risk of innovating themselves directly into a major cyber incident—another reason that outside help from a partner may be valuable.

AI-driven security solutions enable organizations to accelerate and, in many cases, automate their response to incidents.

Conclusion

Innovations like blockchain, 5G, AI and IoT can drive big results for your business, but they can also put it at risk if you don't take a proactive approach to cybersecurity—one that enhances visibility, protects expanding attack surfaces and improves your ability to detect and respond.

Too many security teams today can't even keep up with the fundamentals, let alone find the time to evaluate next-generation tools. They don't have time to engage with stakeholders, so they fail to understand the objectives of leaders who want new technologies to grow their business. And that means innovation is derailed as security gets bolted on piecemeal at the last minute, instead of being baked in from the beginning, when new applications are being designed.

The right security protects you while supporting your corporate goals.

Strategic outsourcing is more than just filling empty seats with warm bodies; it's about bringing in experts who can support strategic decision-making and help extract maximum value from your security investments.

Take advantage of technology and services that protect your business from threats while balancing your customers' experiences and business outcomes

Pursuing a next-gen technology strategy without thinking about security is like building a new mansion without locks. Transformational technology requires transformational thinking; that includes not only new technologies, but also new security practices to keep your business safe.

Access the expertise you need for advanced security ›

verizon✓

1 https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf