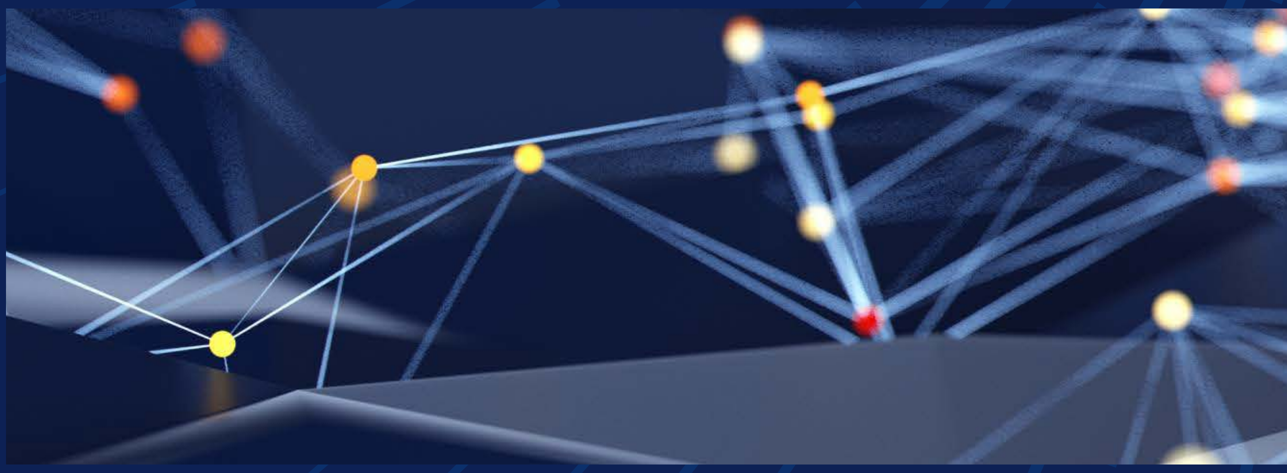
The Future of Cybersecurity: Adapting to a New Digital Era



While cybersecurity professionals are often heads-down focused on preventing attacks and building recovery plans, the overall security environment is continually evolving. It's therefore important to plan for what's coming next.

As we look to the future, three areas stand out —post-quantum cryptography, the changing regulatory landscape, and emerging threats. Organizations should act now by planning and implementing solutions as they are available.

The Dawn of Post-Quantum Cryptography

Quantum computing holds the promise of transforming industries, offering astonishing computational power capable of solving problems far beyond the reach of classical computers. However, this same power could render current cryptographic methods obsolete. Algorithms like RSA and ECC, which underpin much of today's secure communications, could be cracked in a matter of seconds by a sufficiently advanced quantum computer. This looming threat has escalated the urgency for post-quantum cryptography.

Post-quantum cryptography (PQC) revolves around developing cryptographic algorithms that remain secure in a quantum computing era. The National Institute of Standards and Technology (NIST) has recognized this impending risk and is leading the charge to standardize quantum-resistant algorithms.

For enterprises, preparing for this transition is non-negotiable. Early adoption of PQC solutions will ensure that data remains secure when adversaries gain access to quantum computing capabilities.

As Bobbie Stempfley, VP of Cybersecurity and a Business Unit Security Officer at Dell points out, organizations should begin the process by focusing on two key areas:

Identifying and inventorying all the cryptographic models currently in use.
Consider data in flight, not just data at rest. Think about key management, code signing, device identifications, secure access and telemetry. Create a comprehensive inventory and then build a roadmap.

Understanding suppliers' status.
Given that modern enterprises can have thousands of suppliers, be aware of the risks that could come from them. Work to ensure that they are also planning for the change.

Beyond these starting points, conduct risk assessments to identify vulnerable systems, look at implementing hybrid cryptographic models to remain operational during the transition, and collaborate with vendors already exploring quantum-safe solutions, but keep in mind that there won't be one vendor or technology that offers a turnkey solution.

Regulatory Shifts in a Globalized World

Another critical driver shaping cybersecurity's future is the changing regulatory environment. Regulations now extend far beyond compliance—they are becoming a key framework for instilling accountability, driving technological upgrades, and protecting citizens in an interconnected, data-driven world. However, they are evolving rapidly and vary significantly across geographies, increasing compliance complexity.

That said, these regulations move beyond just penalties for non-compliance—they serve as catalysts for better cybersecurity practices. Businesses that actively align their policies with regulatory requirements can unlock new levels of trust and operational efficiency. To do so, organizations should establish governance frameworks that remain flexible to adapt to legal changes, conduct regular compliance audits, and invest in training for employees to handle sensitive information in accordance with the latest standards.

As security executives prepare for compliance, it's important that they ensure that they are understandable and understood. Too often security professionals speak in security terms, which may not resonate with customers, regulators, and other stakeholders. The onus is security professionals to ensure that they are understood, not on listeners to interpret them.

> “Think about the shift to post-quantum cryptography like picking up and moving a fully furnished house. It will be that complex, and the challenge is not breaking anything in the process.”
>
> ***Bobbie Stempfley***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

The Evolution of the Threat (and Defense) Landscape

AI is revolutionizing business, increasing productivity, and unlocking new opportunities of human potential. When it comes to cybersecurity, AI is benefiting both malicious actors and defenders:

Adversarial Use: AI is enabling more sophisticated attacks, such as highly convincing spear phishing and deepfakes.

Defensive Use: AI helps defenders by:

- Processing vast amounts of security data quickly.
- Prioritizing threats more effectively.
- Enhancing detection and response capabilities.

Security tools will only continue to improve, however, with natural language processing allowing security professionals to more directly interface with their systems and empowering systems to proactively take corrective cybersecurity actions.

Organizations should work to simultaneously take advantage of the capabilities while ensuring that their training and other defensive mechanisms stay up to date. Training is the best way to prevent employees from falling victim to more sophisticated attacks.

Going Password-less

Passwords are no longer the most secure methods for identity and access management.

Traditional password-based systems present significant vulnerabilities, making them an increasingly inadequate solution for modern cybersecurity needs. Passwords are susceptible to attacks such as credential stuffing, phishing, and brute-force attempts, often exposing organizations to unnecessary risks. Furthermore, poor user behaviors—like reusing passwords or creating weak ones—compound these vulnerabilities.

Password-less authentication methods, such as biometrics, certificates, and hardware tokens, offer a stronger, more secure alternative by eliminating entire classes of password-related threats. Moving to password-less systems represents a critical evolution in identity and access management, aligning security measures with the growing sophistication of cyber threats.

Adopting password-less technologies also provides numerous benefits, including reducing the attack surface, improving user experience through faster, seamless logins, and lowering IT costs by decreasing password-related incidents. The use of advanced methods ensures a stronger security posture and helps organizations achieve compliance with regulatory standards. Transitioning to password-less systems is not merely a trend—it is a necessary step toward building a safer, more efficient digital ecosystem for both individuals and organizations.

Conclusion

Cybersecurity is entering a transformative era, shaped by quantum computing, shifting regulations, and increasingly sophisticated threats. To stay ahead, organizations must embrace innovations like post-quantum cryptography, AI-driven defenses, and password-less authentication. By prioritizing preparedness, collaboration, and strategic investment, businesses can build a more secure and resilient digital environment. The time to act is now.

Dell products and solutions that can help

Featured Dell Solution	Description
Cybersecurity Advisory Services	Expert guidance that can help you plan for the evolving threat landscape, including current and emerging threats.
vCISO	Virtual Chief Information Security Officer and cybersecurity expert who can assist in identifying and managing risk as well as guide strategic decision making.

Learn how to address some of today's top cybersecurity challenges at **dell.com/cybersecuritymonth**

DELL Technologies