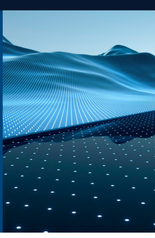
10 Cybersecurity Recommendations

Technology is advancing at such a rapid rate, and as we embrace new tools and systems that enhance our capabilities, we simultaneously create new opportunities for cyber threats that seek to exploit vulnerabilities. In this landscape, it's crucial to implement robust cybersecurity measures to help safeguard against these emerging threats, ensuring that innovation can thrive in a secure environment. As organizations adapt to the new risks, cybersecurity experts from Dell Technologies recommend 10 fundamental actions to advance your cybersecurity maturity.



1 Understand your threat risk landscape.

Experienced cybersecurity partners can provide valuable expertise and resources to help navigate the rapidly evolving threat landscape.

- Conduct thorough vulnerability assessments and penetration testing to identify potential weaknesses that need to be addressed and identify any gaps you may have in your strategy.
- Benefit from specialized skills and knowledge that may not be available in-house, such as insights into emerging risks, advanced attack techniques, and the very latest security strategies and best practices.
- Define access privileges and rationale, allowing you to establish the appropriate security framework for implementing your business controls and governance.

2 Create a comprehensive cybersecurity strategy.

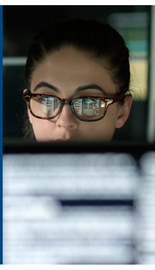
Ensuring cyber resilience requires a coordinated effort involving IT teams, cybersecurity professionals, management, and, at times, external experts.

- Promote enablement of the whole company – security is everyone's responsibility.
- Leverage automation where possible.
- Ensure you have a well-rehearsed IRR plan that lets all the right people know when a cyberattack happens.

3 Work with suppliers who have a secure supply chain.

Security begins earlier than you may think. Ensure a trusted foundation by partnering with suppliers who prioritize security in the design, manufacturing, and delivery of devices and infrastructure. Suppliers that offer a secure supply chain, secure development lifecycle and rigorous threat modeling can help stay ahead of threat actors.

- Provide the confidentiality, integrity and availability of information that describes or traverses the IT supply chain, as well as information about the parties participating in the IT supply chain.
- Ensure that IT products or services in the supply chain are genuine, unaltered, and meet the specifications of the acquirer without any additional unwanted functionality.
- Reduce vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation.



4 Embrace zero trust principles.

Zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify everything trying to connect to its systems before granting access.

- Move away from a perimeter-based security model and adopt zero trust principles.
- Implement the principle of least privilege, which restricts user and system accounts to only have the minimum access rights required for their tasks. This approach reduces the attack surface and the potential impact of unauthorized access by attackers.
- Incorporate solutions like micro-segmentation, identity and access management (IAM), multi-factor authentication (MFA), and security analytics, to name a few.

5 Reduce the attack surface.

The attack surface represents potential vulnerabilities and entry points that can be exploited by malicious actors. To enhance their security posture, organizations must minimize the attack surface, mitigating risks and enhancing overall cyber defenses against new and emerging threats.

- Train employees and users to recognize and report potential security threats, phishing attempts, and social engineering tactics to help minimize the risk of successful attacks that exploit human vulnerabilities.
- Implement preventative measures, such as comprehensive network segmentation, critical data isolation, enforcing strict access controls, and regularly updating and patching systems and applications.
- Ensure that systems, networks, and devices are correctly configured with security best practices, such as disabling unnecessary services, using strong passwords, and enforcing access controls.

6 Detect and respond to cyber threats.

In the face of sophisticated threats, traditional security measures are no longer sufficient. Organizations should leverage advanced threat detection technologies and methodologies to effectively identify and respond to both known and unknown threats.

- Monitor and analyze network traffic, system logs, and other areas, as well as security data to proactively identify signs of unauthorized access, intrusions, malware infections, data breaches or other cyber threats.
- Implement a response plan to promptly investigate and mitigate confirmed security incidents. This includes containing the impact, identifying the root cause and implementing necessary actions to restore systems and prevent further damage.
- Leverage AI/ML to swiftly detect cyber threats through real-time analysis of unusual data patterns or behaviors. These technologies also facilitate rapid response by assessing threat severity, predicting impacts, automating certain defensive actions and scaling security practices, thus minimizing potential damage.

7 Recover from a cyberattack.

Even with critical proactive measures in place, organizations should always assume they have been breached and must have resilient capabilities in place that are frequently tested to ensure effective recovery from a successful cyberattack.

- Take immediate action to mitigate the damage caused by a cyberattack by isolating and containing the impact.
- Disconnect affected systems from the network, disable compromised accounts and implement measures to prevent further spread or damage.
- The use of AI/ML can expedite recovery by swiftly identifying affected systems and data, and automating the restoration process from backups.

8 Leverage experienced partners.

No single vendor has all the necessary capabilities needed to provide end-to-end security, including people, processes or technology; it takes a village. Therefore, it is essential to collaborate with a network of experienced partners.

- Engage with experienced cybersecurity partners who bring valuable expertise and resources to help navigate the rapidly evolving threat landscape.
- Benefit from specialized skills and knowledge that may not be available in-house, including insights into emerging risks, advanced attack techniques and the latest security strategies and best practices.
- Leverage the expertise of experienced professional services and establish collaborative relationships with trusted business partners to establish a comprehensive security posture that effectively protects against evolving cyber threats.

9 Extend cybersecurity to edge and cloud environments.

As networks spread from the core to the edge and to the cloud, they have all become a crucial part of vulnerability. Regardless of how applications are deployed, they require the same level of security and alignment with business policies to ensure consistency for both application users and management.

- Ensure that zero trust principles are extended to cover edge and cloud environments, providing robust access controls, continuous authentication and comprehensive visibility and control over network traffic.
- Implement security measures, such as network segmentation, encryption and continuous monitoring, in both the core network and cloud environments to safeguard against potential threats.
- Collaborate with experienced professional services specializing in edge, core and cloud security to leverage their expertise in implementing effective measures that protect your organization from all angles.

10 Manage proactively and increase end-to-end resilience.

Managing threat intelligence, incident and response and security operations can enhance an organization's capabilities in detecting and responding to cyber threats.

- Establish proactive incident response and recovery protocols that clearly outline roles and responsibilities, ensuring seamless communication and coordination between team members.
- Enhance visibility of the environment to enable organizations to proactively monitor and respond to threats within their networks, while also providing alerts for recovery when necessary.
- Strengthen your ability to proactively detect and respond to cyber threats by leveraging advanced threat intelligence, Security Information and Event Management (SIEM), endpoint protection solutions and behavioral analytics.

Don't let security stifle your innovation.
Learn how you can advance your cybersecurity and zero trust maturity at dell.com/SecuritySolutions

DELL Technologies