DELL Technologies

Ransomware: Strengthening Cybersecurity and Resilience with Dell Technologies

What is Ransomware?

Ransomware is a type of malicious software (malware) that blocks access to a computer system or data until a ransom is paid. It's one of the most disruptive types of cyberattacks. Fifty percent of organizations globally have been hit by ransomware at least once in the past year and the average downtime following a ransomware attack is three weeks, leading to significant operational disruptions

Rising Threat of Ransomware

Ransomware is a type of malicious software (malware) that blocks access to a computer system or data until a ransom is paid. It's one of the most disruptive types of cyberattacks. Fifty percent of organizations globally have been hit by ransomware at least once in the past year and the average downtime following a ransomware attack is three weeks, leading to significant operational disruptions.

How Ransomware Works

Ransomware usually infects organizations when someone clicks a malicious link, opens an infected attachment, or visits a compromised website. It then goes into systems to encrypt files, making them unreadable. Then the ransomware program usually has a message appear demanding payment (often in cryptocurrency) in exchange for a decryption key. If the ransom isn't paid, the attacker may threaten to delete data or leak it publicly. A common example of a ransomware attack that came out in 2017 was the WannaCry attack that spread rapidly across the globe, impacting hospitals, businesses, and government agencies and had a massive financial impact. The global economic impact of the WannaCry virus was between $4B to $8B according to Cyber Risk Management (CyRiM) and Lloyd's of London with over 200,000 systems impacted across 150 countries within a matter of days.

Two of the globes major corporations impacted were FedEx, who reported a $300 million loss due to service disruption and cleanup, and Renault-Nissan who had to temporarily halt production in several plants. The hidden costs of a ransomware attack can be many including things such as:

- Company downtime and loss of productivity
- Reputation damage
- Cost of system recovery and patching
- Legal and regulatory fines

When faces with a ransomware attack, businesses should take the following steps;

- Don't pay unless absolutely necessary – there's no guarantee the attackers will restore access.
- Restore from backup if available.
- Report the attack to authorities.
- Strengthen defenses to prevent future infections (e.g., keep software updated, train staff, use endpoint protection).

Combating Ransomware Attacks with Dell Technologies

Dell Technologies equips organizations with comprehensive, forward-thinking tools designed to help thwart ransomware risks before they cause harm.

Enhanced Endpoint Security with Dell Trusted Workspace

Endpoints are often the primary entry points for ransomware attacks, making endpoint security a critical focus area. Dell Trusted Workspace integrates hardware-enabled security features that protect systems without compromising performance. Solutions like Dell SafeBIOS and SafeID fortify endpoint devices against unauthorized access, while Dell SafeData encrypts data to protect sensitive information even outside the corporate firewall. By embedding security directly into devices, businesses ensure protection at the hardware level, giving attackers fewer opportunities to gain a foothold.

Proactive Detection with CrowdStrike

Ransomware attacks aren't inevitable if organizations use the right tools to detect and respond to threats in real-time. CrowdStrike, offered as part of Dell's solutions portfolio, provides a next-generation endpoint protection platform powered by AI and behavioral analytics. This technology identifies and neutralizes suspicious activity before it evolves into an attack. By integrating seamlessly with Dell infrastructure, CrowdStrike allows IT teams to maintain visibility across their entire environment, delivering immediate and effective threat response.

Comprehensive Data Protection with Dell PowerProtect

Dell PowerProtect solutions are the backbone of ransomware resilience. These advanced data protection tools are designed to secure enterprise data against both internal and external threats. Features like immutable backups ensure your data can't be altered, deleted or encrypted by ransomware, providing a reliable safety net even in the face of advanced attacks. Dell PowerProtect Cyber Recovery Vault, for instance, isolates critical data from the network using air-gapped technology, ensuring it remains untouched even during the most sophisticated breaches. With automated anomaly detection and intelligent workflows, organizations gain the ability to detect malicious activity early and respond before ransomware spreads.

Advanced Network Security and Micro-Segmentation with Dell PowerSwitch Networking & SmartFabric OS

Strengthens defenses against ransomware attacks by delivering advanced network segmentation, strict access controls, and real-time traffic analytics across your infrastructure.

Recovery at Scale with Dell Data Protection Services

Dell understands that while prevention is critical, recovery is an equally important aspect of ransomware readiness. Dell Data Protection Services provide not only automated backup and recovery solutions but also expert-led consulting to ensure businesses can recover quickly and minimize downtime. Services such as Remote Data Recovery and Incident Response ensure organizations have the support they need during peak moments of crisis. This comprehensive approach guarantees that data integrity is preserved and recovery times are reduced, preventing operational disruptions.

These are just a few examples within the Dell portfolio of solutions that can help with malicious insider threats.

Strength Through Partnerships

Dell's collaborative approach extends its protection beyond Dell-only technology. Through partnerships with leading cybersecurity firms like CrowdStrike and Secureworks, Dell offers an ecosystem of integrated solutions that address every possible attack vector. Together, these solutions provide end-to-end security coverage, enabling businesses to create multilayered defenses tailored to their unique risk profiles.

Why Choose Dell?

Dell Technologies is more than a technology provider — it's a trusted partner in the fight against ransomware. By combining innovation, expertise and a commitment to empowering businesses, Dell equips organizations with the tools and confidence needed to face evolving threats. Whether securing endpoints, protecting critical data, or enabling rapid recovery, Dell's products and services ensure operational continuity and peace of mind.

Building a Resilient Future

Ransomware attacks continue to evolve, but with Dell Technologies, businesses can stay one step ahead. By leveraging advanced hardware, software and services, organizations can build a cybersecurity framework that's resilient, adaptable and dependable. Safeguard your data, protect your operations, and future-proof your business today with Dell's comprehensive solutions against ransomware.

To ensure the resilience of your business, it's vital to understand the current threat landscape and stay informed about emerging threats. Dell Technologies' cybersecurity experts constantly monitor for new attack vectors (what do we call this?) and work to proactively address potential vulnerabilities in our products and services. This allows us to provide you with the most up-to-date protection against ever-evolving ransomware threats.

In addition to staying informed, businesses must also start a multi-layered security approach. This means deploying a range of security measures such as firewalls, anti-malware software, intrusion detection systems and data backups. By diversifying your defense strategies, you can minimize the impact of any one attack and ensure that your business remains operational even in the face of a successful ransomware attempt.

It's also important to regularly test and update your security measures (both patch your systems and update your policies). Hackers are constantly finding new ways to bypass traditional security measures, so it's crucial that businesses stay ahead of the curve by regularly testing their defenses and updating them as needed. This includes conducting regular vulnerability assessments, penetration testing and patch management.

Another key aspect in protecting your business from ransomware is educating your employees on best practices for cybersecurity. Many ransomware attacks are initiated through social engineering tactics such as phishing emails or malicious links. By educating your employees on how to spot and avoid these threats, you can greatly reduce the likelihood of a successful attack.

Furthermore, having a disaster recovery plan in place can greatly mitigate the impact of a ransomware attack. This plan should include regular backups of important data and systems, as well as a clear procedure for responding to an attack and recovery.

In addition to these proactive measures, it is also important to have a strong incident response plan in place. This includes clearly defined roles and responsibilities for handling a ransomware attack, as well as communication protocols for notifying stakeholders and mitigating damage.

Finally, staying informed about the latest trends and developments in ransomware attacks can help you stay one step ahead of potential threats. By regularly reviewing industry reports and updates from security experts, you can proactively implement new security measures to protect your business.

Remember that no business is immune to ransomware attacks, but with the right strategies and tools in place, you can minimize the risk and impact of such attacks. By taking a proactive approach towards cybersecurity, you are not only protecting your business but also building trust with your customers and stakeholders.

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

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellSecurity

DELL Technologies