DELL Technologies

Backup Infiltration: Strengthening Cybersecurity and Resilience with Dell Technologies

Executive Summary

Backup infiltration poses a growing threat to businesses in every sector, exploiting vulnerabilities in the very systems designed to safeguard critical information. These attacks compromise data recovery systems, undermining trust and jeopardizing operations. From significant financial losses to extended downtime and reputational damage, the consequences can be severe.

Dell Technologies provides an end-to-end suite of defenses to protect sensitive data and prevent these attacks, including Dell Trusted Workspace, Dell Trusted Infrastructure, and extensive security capabilities integrated into all of our solutions. With the addition of strategic partnerships and professional services, Dell helps organizations establish a resilient multi-layered security frameworks to detect, thwart, and recover from backup infiltration incidents efficiently.

By implementing Dell's innovative solutions and expert support, businesses will be better prepared to secure their infrastructure and maintain operational continuity.

Rising Threat of Backup Infiltration

Backup systems are essential for business continuity, instrumental in recovery after cyber events such as ransomware or hardware failure. Unfortunately, these very lifelines have become increasingly targeted by cybercriminals. Backup infiltration corrupts or deletes backup data, rendering it inaccessible when it's needed most.

These evolving threats demand proactive measures. Failure to protect backup systems jeopardizes operations and exposes sensitive data. Businesses of all sizes, from small enterprises to multinationals, are potential targets, with industries such as healthcare, finance, and manufacturing particularly at risk.

Dell Technologies recognizes the urgency of fortifying backup environments, offering advanced tools and guidance to counter these sophisticated attacks.

Backup Infiltration Attacks

Backup infiltration occurs when cybercriminals exploit vulnerabilities in backup systems to compromise, destroy, or encrypt critical recovery data. These sophisticated attacks may coincide with or follow other incidents, such as ransomware or malware deployment, amplifying the operational and financial fallout.

How Backup Attacks Work

1. **Initial Breach:** Attackers gain unauthorized access to the network, often through phishing, weak credentials, or unpatched vulnerabilities.
2. **Lateral Movement:** Once inside the network, attackers use tools to move undetected, targeting backup repositories and critical data sets.
3. **Backup Compromise:** Key tactics include encrypting backup files, deleting recovery points, or corrupting data.

Common Techniques

- **Credential Theft** breaches administrative accounts to enable full access to backup systems.
- **Ransomware Deployment** encrypts both live data and backups, demanding payment for decryption.
- **Timed Corruption** compromises backups gradually to escape detection while leaving businesses exposed when recovery is required.

Such techniques highlight the sophistication and severity of these threats, demanding preemptive action.

The Impact on Businesses

Financial Loss

Backup infiltration amplifies recovery costs and downtime, often doubling or tripling response expenses. Recovery from encrypted or compromised backups may require payments to attackers, new infrastructure, or expensive consultants.

Operational Disruption

Without viable backups, organizations face lengthy recovery times that disrupt services, delay projects, and halt critical functions.

Reputational Consequences

Permanent data loss or extended downtime erodes stakeholder trust, potentially damaging a business's long-term viability.

Real-World Example

A global healthcare provider discovered its backups had been corrupted during a ransomware attack. Despite paying the ransom, three weeks of patient data were permanently lost, delaying surgeries and triggering lawsuits. Total recovery costs exceeded **$50 million.**

Alarming Statistics

Recent studies estimate the average financial hit from a compromised backup system exceeds **$4.45 million**[1], including fines, downtime, and recovery expenses. Particularly alarming is the rising frequency of such incidents, with global reports showing a **39%** year-over-year increase in backup-related threats.

57% of backup-targeting attacks successfully infiltrate backup repositories

Source: 2024: Index Engines

Combating Backup Infiltration with Dell Technologies

Dell Technologies provides a robust suite of tools and services that address the unique challenges posed by backup infiltration attacks, enabling businesses to prevent, detect, and recover effectively.

Server and Storage Security Solutions

Dell's server and storage solutions provide unparalleled resilience against backup targeting efforts. Built-in features ensure backups remain secure, and snapshots are not compromised.

- **Immutable Backups / Snapshots** create tamper-proof restore points.
- **Air-Gapped Recovery** isolates data from live networks to prevent corruption.

[1] Ponemon - Cost of a Data Breach Report 2024

Fortify Dell Data Protection Appliances

Dell data protection appliances are embedded with capabilities that include Dell SafeBIOS for firmware integrity and SafeData for secure encryption to help protect against backup attacks. In addition, these solutions have capabilities such as multi-factor authentication (MFA), roles-based access controls (RBAC) and dual authentication to keep threat actors out.

Advanced Threat Detection with CrowdStrike

The integration between CrowdStrike and Dell Data Protection focuses on enhancing the security and monitoring of data protection environments through a set of advanced capabilities.

1. **Endpoint and Data Protection:** Dell integrates CrowdStrike's endpoint security and extended detection and response (EDR/XDR) with its data protection solutions. This includes telemetry collection from Dell PowerProtect Data Manager and PowerProtect Data Domain, alongside security insights from the CrowdStrike Falcon console and next-generation SIEM software
2. **Monitor and Respond:** Dell Managed Detection and Response (MDR) service manages the CrowdStrike software on behalf of customers, collecting logs and investigating any Indicator of Compromise (IoC) or anomaly detections. This integration allows Dell to provide continuous monitoring and collaborate with the customer's SOC to ensure rapid and effective remediation of threats
3. **Real-Time Visibility and Data Movement Control:** The CrowdStrike Falcon Data Protection platform offers real-time visibility into data movement across various sources and channels, classifying data by both content and context. This helps in preventing data theft and ensuring data protection policies are enforced effectively by combining content with contextual analysis
4. **Unified Management and Simplified Deployment:** The integration allows for a single platform and agent to manage both endpoint and data protection, reducing complexity and operational overhead. This is facilitated by the lightweight and cloud-native approach of the CrowdStrike Falcon platform, enabling rapid deployment and minimal disruption

The integration between CrowdStrike and Dell Data Protection leverages advanced EDR/XDR capabilities, real-time monitoring, and comprehensive data management to enhance overall security and resilience of data protection environments.

A leading financial institution recently deployed PowerProtect Cyber Recovery, preventing attackers from accessing 90% of critical backups during a breach, allowing seamless restoration without ransom payments.

Dell PowerProtect Solutions for Backup Integrity

Dell PowerProtect delivers comprehensive backup protection, leveraging immutability, isolation, and compression to prevent backup system compromises. By integrating with ransomware detection tools, PowerProtect ensures that suspicious changes trigger alerts for immediate action.

The Multi-Layered Security Approach

Protecting data requires coordinated, multi-faceted security strategies. Dell helps businesses implement industry best practices to build a resilient backup environment.

Key Steps to Enhance Defense

- **Adopt Zero Trust Principles:** Continuously validate all users, devices, and processes, reducing the risk of unauthorized access.
- **Encrypt All Backups:** Ensure data remains unreadable if compromised, both in transit and at rest.
- **Educate Employees:** Teach employees to recognize phishing attempts and other social engineering tactics that lead to initial breaches.
- **Regular Vulnerability Testing:** Frequent tests help organizations identify and patch weak areas before attackers exploit them.

Dell pairs these practices with cutting-edge solutions, building a robust and responsive infrastructure ready to meet emerging challenges.

Strategic Partnerships that Enhance Security

Dell works alongside cybersecurity leaders such as Microsoft, CrowdStrike, and Secureworks. Each partnership enhances Dell's solutions, offering customers unmatched protection capabilities like advanced threat intelligence, endpoint monitoring, and comprehensive response strategies.

Leveraging Dell Professional Services

Dell Technologies' Professional Services provide expertise and guidance to help businesses tackle complex cybersecurity challenges effectively. From creating incident response plans to implementing zero-trust architectures, Dell specialists ensure client environments remain resilient against modern threats like backup infiltration.

Build Business Resilience with Dell

Choosing Dell positions businesses to outmaneuver sophisticated attackers while maintaining operational continuity. Through innovation, partnership, and expertise, Dell ensures organizations can prevent, detect, and recover from even the most severe backup infiltration attacks.

Take the Next Step

Contact Dell Technologies today to safeguard your business. Together, we'll secure your critical assets, protect your reputation, and build a resilient future.

Dell remains committed to fostering confidence in the digital age, bringing organizations the tools, knowledge, and support they need to operate securely and thrive.

Backup resilience begins with Dell Technologies. Act now to future-proof your operations and build confidence in your cybersecurity posture.

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

Learn more about Dell Cybersecurity solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellSecurity

DELL Technologies