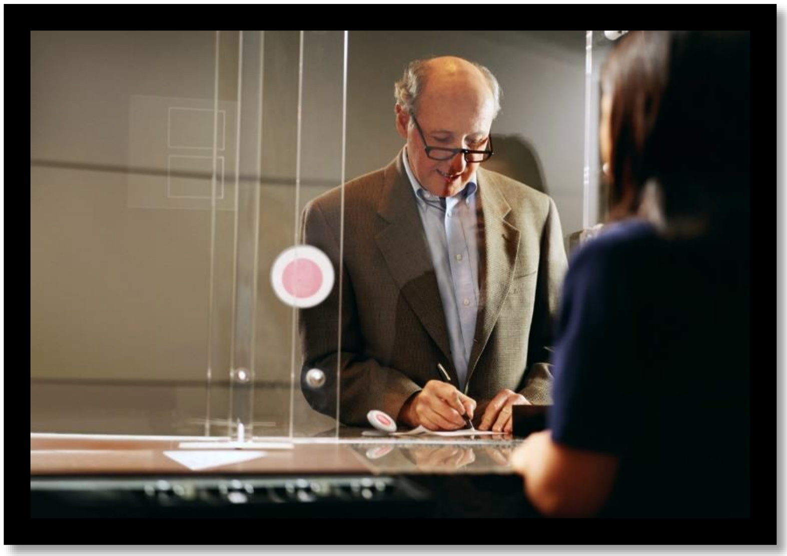
What kind of cybersecurity story will you tell?

By David Noy | October 2022

Some organizations learn about cybersecurity loopholes the hard way. Stories abound about some local municipality or large corporation that has had to pay significant sums to cyber attackers who have found a way into their sensitive data. These attacks can happen unexpectedly. Out of the blue, an ominous email arrives notifying an executive or administrator that their organization's data has been compromised. Within the email, there will be a bitcoin invoice that must be paid in order to resolve the data breach. Organizations can end up paying hundreds of thousands of dollars to unknown assailants.



How is it possible for attackers to silently infiltrate an organization's data? Consider this scenario: An IT department deploys a storage system with special immutable snapshots as the principal technology to protect their data from ransomware attacks. These specially protected snapshots are solidly tamper-proof, so it is impossible to alter them in any way or delete them without layers of authentication and an engagement with product support. However, what if over a weekend a cyber attacker penetrates the organization's filesystem and copies sensitive data from several departments? The organization's tamper-proof and undeletable snapshots alone would not address this kind of attack.

But this type of cyber-attack doesn't have to lead to a disastrous ending. Consider an alternate scenario: Another IT organization receives a warning that an end user has been locked out of the company's human resources file share. A storage administrator goes straight to their cybersecurity analytics interface and soon determines that the end user is an attacker.

In this scenario, the company would need a much broader set of cyber-defenses in their storage system than immutable snapshots. If their file shares resided in a PowerScale cluster from Dell Technologies, their cybersecurity story would be about the world's most secure scale-out NAS.[1]

A PowerScale story would be about advanced analytics with built-in triggers and automation that could send alarms at the

[1] Based on Dell analysis comparing cybersecurity software capabilities offered for Dell PowerScale vs. competitive products, September 2022.

first sign of malicious activity and simultaneously activate a series of automated responses in the company's NAS cluster to help thwart the attackers and protect data. Rather than having a bitcoin payment as the ending, a PowerScale story might end with the attacker being locked out within seconds after they tried to steal data.

The point of these stories is that not all storage-based cybersecurity solutions provide the same level of protection from attacks. All organizations, from local municipalities to large corporations, should secure their data in a storage solution that offers robust cybersecurity capabilities. See below for more details on what makes Dell PowerScale qualified to help you fulfill your cybersecurity requirements.

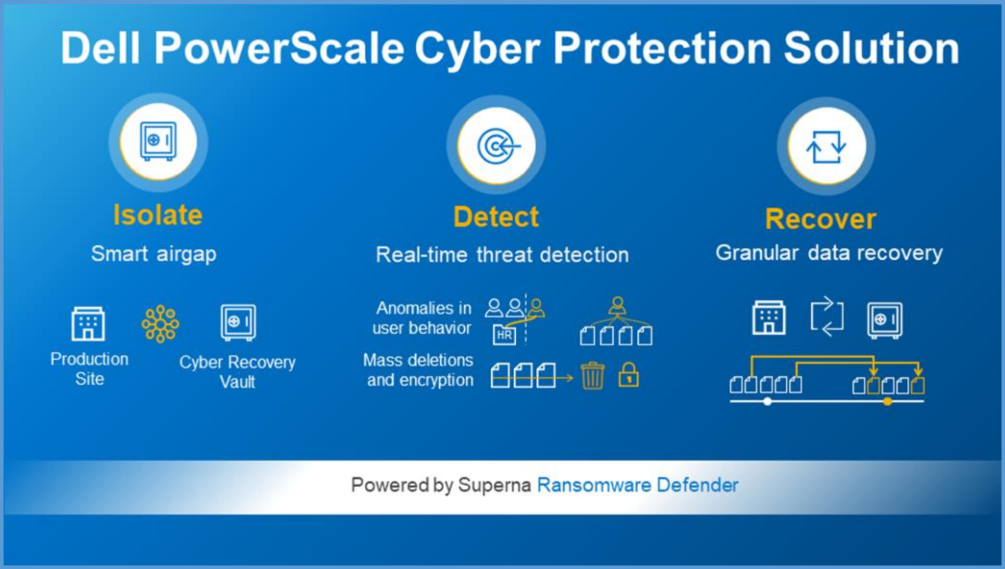
What makes PowerScale the world's most cyber-secure scale-out NAS?

More expansive and vigorous multi-vector analytics, which include network, storage, intrusion detection systems, perimeter, and endpoint analytics to help detect attacks more successfully.

Real-time detection and storage system responses to filesystem anomalies, which help detect attacks faster.

More intelligent automated responses to early-warning anomalies, which include locking out malicious actors and triggering immutable snapshot copies to help thwart attacks and protect data more effectively.

More advanced recovery mechanisms, including smart isolated vault technology enabling operational airgapping, to help speed up recovery and prevent data loss.



Dell PowerScale Cyber Protection Solution

Isolate
Smart airgap

Detect
Real-time threat detection

Recover
Granular data recovery

Powered by Superna Ransomware Defender

#TrustDell

About the author: David Noy brings over 25 years of experience in the storage and data management industry. He spent nearly a decade leading engineering and product management teams for numerous companies, including Dell Technologies, NetApp, Veritas, and Cohesity. Today, David leads product management at two industry-leading divisions at Dell Technologies—Unstructured Data Storage and Data Protection—where he is helping to embolden innovation around data management and hybrid cloud and driving advancement of holistic solutions to help heighten business success for customers worldwide.