Protecting Data at All Cost

MARKET TRENDS REPORT
Executive Summary

In recent years, federal agencies have been hit with tens of thousands of cyberattacks, some relatively small and some large enough to warrant significant news coverage. There are now so many different types of attacks – coming so quickly and so unexpectedly – that agencies are having difficulty keeping up.

Today, cyberattacks are a fact of life for all organizations. But the stakes are particularly high for federal agencies. As stewards of citizens’ sensitive and private data, there is little tolerance for failure. And then there are agencies’ missions – cyberattacks can cause agencies to slow or halt, and that simply cannot happen.

Hackers are getting smarter, infiltrating what used to be considered unreachable. For example, cybercriminals have become experts at inserting malicious software inside backup data that will eventually disrupt agencies unless a ransom is paid.

To avoid these issues, agencies are continually searching for ways to protect their data and, if compromised, recover quickly and completely. A comprehensive data protection strategy can be an effective way forward.

To learn more about how a comprehensive data protection strategy can help agencies defend valuable data, GovLoop teamed with Presidio Federal and Dell Technologies, which both provide data backup, management, protection and storage and hyperconverged and compute solutions.

“Our government got hacked last year and we didn’t know about it for months. ...This incident is one of many that underscores a need for the federal government to modernize cybersecurity defenses and deepen our partnerships.”

– Homeland Security Secretary Alejandro Mayorkas
## By the Numbers

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>62%</td>
<td>IT decision-makers are concerned that their organization’s existing data protection may not be adequate for coping with malware and ransomware threats.</td>
<td></td>
</tr>
<tr>
<td>30,819</td>
<td>Information security incidents occurred federal governmentwide in 2020.</td>
<td></td>
</tr>
<tr>
<td>86%</td>
<td>Of security breaches are due to ransomware and phishing.</td>
<td></td>
</tr>
<tr>
<td>47%</td>
<td>Of federal government respondents reported seeing an increase in cyberattacks in the past year.</td>
<td></td>
</tr>
<tr>
<td>38%</td>
<td>Of cybersecurity professionals get 10-20 hours of cybersecurity training annually.</td>
<td></td>
</tr>
<tr>
<td>28%</td>
<td>Of organizations that experienced security incidents also encountered unplanned expenses to fix security gaps.</td>
<td></td>
</tr>
<tr>
<td>42%</td>
<td>Of cybersecurity experts are experiencing cybersecurity fatigue.</td>
<td></td>
</tr>
</tbody>
</table>

**Average Bill for Ransomware Attack:** $1.37 million
- Includes downtime, people time, device and network costs, lost opportunities, and ransoms paid.
Creating the Right Data Defenses

The Challenge: State Actors and Smart Cybercriminals

Keeping data safe has never been more difficult. Here’s why:

- **Attacks on data backups have risen dramatically over the past few years**, and hackers are continually upping their game. Some gain access to networks through phishing schemes, inserting payloads that find backup copies of data and delete them. If a ransom isn’t paid, these backups are destroyed. Newer, more insidious methods have followed. Hackers began inserting “time bombs” into their malware, keeping this malicious software from detonating for months. During that time, any new backups would inadvertently include the malware. At the prescribed time, the bomb detonates, and attackers demand a ransom. An even newer method is an immutable subversion attack, where attackers can change the retention rate from weeks to hours, creating a small window of time for backups to show that they have been successfully completed before they disappear.

- **Traditional security strategies for backups aren’t working.** While backup software is critical for preserving data in case of accidental deletions, data corruption or disaster, it was never designed for cybersecurity. Neither were the processes IT administrators were taught; the typical 3:2:1 backup rule does little to prevent backup malware from being deposited and detonating.

- **Endless threat alerts can become background noise, leading to alert fatigue.** According to recent research, more than 25% of security alerts are false positives. This information overload can easily lead to indifference, exhaustion and ignoring potentially serious threats.

The Solution: A Comprehensive Data Protection Strategy

After a catastrophic attack, recovering as much data as quickly as possible is the top priority. The best way to ensure that data will be fully recoverable is by preparing beforehand with a comprehensive data protection strategy. It has three parts: **data isolation, locked retention policies and effective analytics and forensics tools**.

“At a high level, it’s about ‘sync, copy, lock and analyze,’” said Kevin McDonough, Advisory Systems Engineer at Dell Technologies. “Together, these capabilities are a solid plan for ensuring that data is protected no matter what.”

**Data isolation and governance:** Data must remain secure even when it’s in an unlocked state – while in production, or during synchronization and replication. This requires full data isolation – physically and logically separating data within an air-gapped vault. It is typically an isolated environment disconnected from networks and restricted from those without proper credentials. Governance is an equally important part of this step. To ensure full governance, look for a retention lock that prevents specified files from being overwritten, modified or deleted for a user-defined period, but can also be modified by an administrator with account credentials.

**Automated data copy and air gap:** Traditional immutable storage isn’t enough to preserve data integrity and confidentiality, because if enemies can see the data, they can encrypt or destroy it. The solution is creating immutable, unchangeable copies of data with locked retention policies inside a secure, air-gapped digital vault. The air gap provides network isolation and eliminates management interfaces, which could be compromised.

**Analytics, machine learning and forensics tools to quickly detect and recover from cyberattacks:** Tools that use machine learning and full content indexing can diagnose attack vectors within the confines of the vault and alert administrators when suspicious behavior is detected. When an attack occurs, the analytics engine should be able to provide detailed forensic reports to help administrators understand the details of the attack, along with a list of the last good backup sets before corruption to aid in the recovery process. Because intelligent analysis tools can also incorporate historical data and indicators of compromise, they can root out many false positives and help avoid alert fatigue.
Best Practices for Data Protection Strategies

Learn before acting. Before jumping into any new technology or approach, take the time to understand your current cybersecurity resilience and what’s missing. There are many ways to do that, like taking advantage of the federal Cyber Security Evaluation Tool (CSET) or Dell Technologies’ Cyber Resiliency Assessment. These tools can provide valuable information on how ready the agency is and what’s left to be done.

Make sure the data protection solution you choose supports the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework. There is a lot of conflicting information about the best way to secure environments. That’s why following a framework like the NIST Cybersecurity Framework is so critical. It sets up “swim lanes” that help break things down into manageable segments. “When you’re talking to executives or security personnel, you can break up the defense-in-depth into smaller bites,” McDonough said. “Each of those groups has a role and perspective on identification, detection, protection and recovery, and the framework can help ensure that all of those groups are coordinated, and that the right people, processes and technology are in place.”

Use the “sync, lock, copy, analyze” method to stop insider threats. Security incidents involving insiders can include malicious data exfiltration and accidental data loss. With appropriate air-gapping and locked retention policies, it’s more difficult for anyone – even insiders – to attack in the first place. If they succeed, some techniques that help agencies recover from external attacks can be used to recover from insider attacks. “You can see whose credentials are being used, and while it’s often an outsider compromising those credentials, it can also be an insider,” McDonough said. “With the right analytics, you can dig deeper to determine if it was actually an insider, which can prompt the agency to take the right steps.”

There are no shortcuts. Implementing technology is only the first step; testing and training are also key. Before starting the engine, test the full solution. That includes creating if/then scenarios and testing each one. These tabletop exercises can provide a lot of good information to help agencies fine-tune permissions, policies and processes. Once the system is working well, take the time to fully train users on how to use it, what to expect and how to respond.
How Presidio Federal and Dell Technologies Can Help

Presidio Federal’s certified team of solutions architects, engineers and developers work alongside Dell Technologies to provide effective solutions for federal agencies. Together, Dell Technologies and Presidio Federal help agencies deploy tools that protect mission-critical data and accelerate data recovery after cyberattacks.

For instance, Dell Technologies’ PowerProtect Cyber Recovery solution isolates critical data from ransomware and other sophisticated threats with immutability to preserve data integrity and confidentiality with layers of security and controls. Machine learning identifies suspicious activities and allows agencies to recover known good data and resume normal business operations with confidence. Many organizations also choose to run Cyber Recovery on Dell Technologies’ Data Domain appliances, which consolidates both backup and archive data on the same infrastructure.

Cyber Recovery is commonly paired with Dell Technologies’ CyberSense, which monitors backup data to understand how it is changing over time. CyberSense alerts administrators when it finds corrupted data and provides post-attack diagnostics to determine when the attack occurred, how much damage was done, what data was attacked, the source of the corruption and the last viable backup sets generated before the attack.

Learn more about how Presidio Federal and Dell Technologies can assist your agency with data protection and accelerating data recovery at https://presidiofederal.com/partners/dell/.
Conclusion

New cyber realities call for a new game plan – one that takes a comprehensive and decisive approach to locking down data so that even if an attack succeeds, agencies can still recover current data.

“Instead of the method that everybody has been taught – keep three copies of data on two different media with one copy off-site for disaster recovery – you need one more copy of your critical data that stays isolated, air-gapped and immutable,” McDonough said. “Adding machine learning and forensics tools to identify anomalies is the final piece of the picture, providing the information necessary to recover safely and remediate as necessary.”

ABOUT PRESIDIO FEDERAL
Presidio Government Solutions, branded Presidio Federal, is an IT services and solutions provider focused on federal mission outcomes. We are a wholly-owned subsidiary, and fully independent entity of Presidio, dedicated to servicing the needs of our federal customers through expert knowledge centers in automation, augmentation, cloud, cybersecurity, digital infrastructure, and collaboration.

For more information please visit www.presidiofederal.com.

ABOUT DELL TECHNOLOGIES
Dell Technologies is a unique family of businesses that provides the essential infrastructure for organizations to build their digital future, transform IT and protect their most important asset, information.


ABOUT GOVLOOP
GovLoop’s mission is to “connect government to improve government.” We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.