FCW | VEEAM

WHITEPAPER

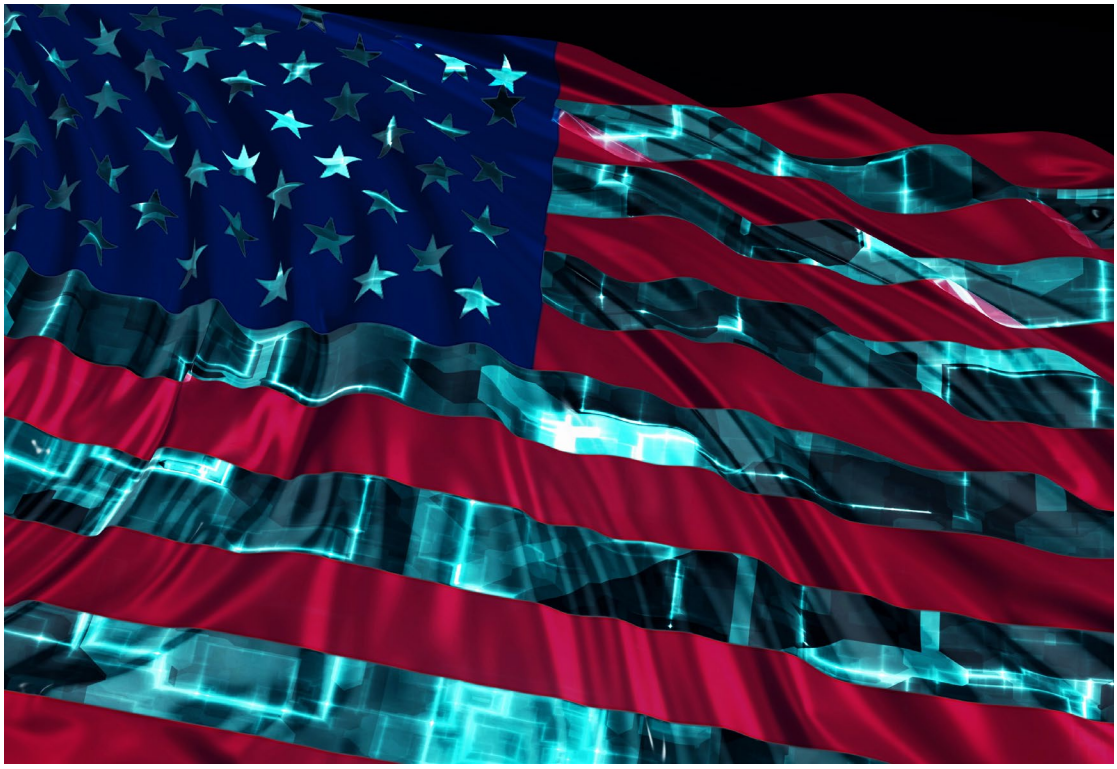
# Bringing Backup and Recovery Forward in Your Cybersecurity Strategy

**With the rise in ransomware attacks,** federal agencies are escalating cybersecurity efforts to keep pace. Government technology leaders recognize the operational consequences of a ransomware attack — mission-critical data and systems offline for days or weeks — can be catastrophic. Spurred on by the recent cybersecurity memorandum, agencies are looking for a path forward.

The implementation of robust backup and recovery strategies is key to tackling the ransomware threat. "Having backups of all data to avoid being shut down by an attack," is a primary safeguard, according to Forrester. Meanwhile Gartner highlights "frequent and reliable backup and recovery capabilities" as a core element in ransomware defense.

The Cybersecurity and Infrastructure Security Agency (CISA) likewise calls for regular backups in support of its zero trust data-protection protocols, which work hand-in-glove with ransomware defenses.

Here, we explore the ransomware landscape, including stumbling blocks to effective federal defense against such exploits. We describe a modernized approach — one grounded in application-level data protection that operates across domains and includes automated recovery testing. And, finally, we outline best practices for agencies looking to shore up backup and recovery efforts.



Cover Image: Laurence Dutton / iStock
vitacopS / iStock

# The current landscape

Bad actors, from criminal gangs to nation-states, have been deploying ransomware at an alarming rate. In its 2022 Data Protection Trends report, Veeam found 76% of 3,393 organizations surveyed had suffered at least one attack.

Moreover, the pace of such attacks is increasing. Research from Sophos finds 66% of organizations were hit by ransomware in 2021, increasing 78% in just one year, showcasing that "adversaries have become considerably more capable at executing the most significant attacks at scale."

Government's high-value data stores and mission-critical operations make it a prime target for ransomware. From 2018 to 2022, U.S. government organizations experienced 330 individual ransomware attacks, potentially impacting more than 230 million people and costing an estimated $70 billion in downtime. At the national level, there were at least 30,000 cyberattacks against federal government in 2020, according to the most recent data.

The White House has identified this as an urgent concern, noting ransomware incidents "have disrupted critical services and businesses worldwide – schools, banks, government offices, emergency services, hospitals, energy companies, transportation, and food companies have all been affected."


Zephyr18 / iStock

# Boosting your backup strategy

Backup and recovery are key to meeting this emerging threat. This was demonstrated in the starkest geopolitical terms recently, when Ukraine's backups effectively stopped a Russian effort to disrupt satellite communications just hours before the invasion began. Ukraine is set up to repair and rebuild networks quickly after an attack — the result of combatting Russian malware, like NotPetya, which wiped data from energy firms and banks, for the last eight years.

"So it's really not a big deal to see a network wiped out because they are ready for it," said Dmitri Alperovitch, a co-founder and former CTO of CrowdStrike and chair of security-centric think tank Silverado Policy Accelerator. "They've got backups ready to go, and they can rebuild it very quickly and very efficiently."

It is not clear that all federal agencies currently operate at this level of cyber resiliency. However, with reliable system backups and well-tested recovery protocols, agencies can outflank attackers who try to hold data and systems hostage. They can restore mission-critical functionality and resume citizen services with minimal downtime. An approach grounded in a vigorous backup and recovery strategy also aligns with calls for agencies to take a zero trust approach to cybersecurity, in accordance with a recent White House memorandum.

While zero trust conversations typically focus on access controls, the overall goal is to protect the data that may be at risk in a ransomware exploit. When bad actors circumvent access controls, robust backup and recovery act as the ultimate failsafe.

# Hurdles to effective defense

A number of factors can make it difficult for agencies to forge an effective strategy around backup and recovery, including: data criticality, data growth and data sprawl.

- **Criticality:** In the past, data may have been ancillary to an agency's mission, but it wasn't critical to citizen service or national security. Today, data drives the federal mission. As data has become more central to the mission, the requirements to protect it have increased. However, the technology investments to meet those requirements have often not kept pace.

- **Growth:** Data is generated at an ever-increasing rate, with the global rate of data creation expected to top more than 180 zettabytes by 2025, according to Statista research. In government, data isn't just being created by humans, it's generated by machine sources, from cameras to satellites to Internet of Things devices. The sheer volume of information compounds the difficulties around backup and recovery.

- **Sprawl:** No longer confined to the on-premises data center, federal data today increasingly lives in multiple cloud environments. Agencies that had workable on-premises backup solutions may struggle with the move to cloud-based workloads. They may have embraced the inherent resiliency and security of cloud platforms, but they still need a modernized solution to back up those many and disparate cloud-based operations.

ipopba / iStock

With data and applications residing in different places, IT teams often must apply and coordinate multiple backup tools and methods. With recovery, they need to cobble together these disaggregated backups, which can make it difficult or impossible to fully restore data and operations.

Equally concerning, many agencies don't have a clear read on whether their backup and recovery methods would even work if put to the test. Veeam research found only a slim percentage of IT executives know whether their systems are routinely tested. Asked about their uses of automated recovery verification or validation of backups, only 400 out of 1,000 replied, and of those, only 9% of public-sector respondents did automated testing. Yet, routine validation is key to success: In CISA's ransomware guidance it urges organizations not only to maintain offline, encrypted backups, but to "regularly test your backups."

# Bolstering effective backup and recovery

What does a modernized approach to backup and recovery look like? To safeguard against the potentially mission-killing impact of ransomware, agencies should achieve these key goals:

- **Application-aware data protection:** With applications increasingly hybridized, residing on-premises and in the cloud, it's no longer sufficient to back up merely at the storage level. An effective strategy allows application-level monitoring, giving the team in-depth vision into, and control over, its infrastructure's resources and workloads. In case of a ransomware attack, application-level backup drives operational resilience by allowing administrators to recover data for a specific application.

- **Automated recovery testing:** The point of backing up is not just to have the data on hand, but to be able to use it to resuscitate compromised systems. To ensure that will work, agencies need to regularly test backup and recovery systems. Yet, only one in six organizations test their backup solutions by restoring and verifying data, according to Veeam's 2022 Data Protection Trends Report. In a modernized solution, automation makes it possible to run these validations in the background, during the normal course of business. Such automated testing ensures backup will be available and readily usable should a ransomware attack take down systems. Automated testing will also help agencies comply with the zero trust memorandum's call for auditable and verifiable protections.

- **Security integration:** Backup and recovery tools should be integrated with the broader security tool set and work seamlessly across an agency's on-premises and cloud deployments. To that end, a solution should be cloud-agnostic and hardware-agnostic, enabling the agency to safeguard data wherever it resides.

KrulUA / iStock

This becomes especially important in a ransomware scenario. Law enforcement may declare impacted systems as part of the chain of evidence, in which case those systems may be unavailable for weeks or even months. In that case, recovering seamlessly into an alternative IT environment is vital to operational resiliency.

What does such a solution look like in action? Consider the case of one organization that recently experienced a ransomware attack.

Law enforcement sealed off the server room as part of the chain of evidence in an attack that compromised 70 virtual machines. That made recovery within the physical data center impossible. The agency has in place a modernized, hardware-agnostic backup solution from Veeam. With this, IT leaders recovered 70 virtual machines in the cloud.

The team tested as it proceeded, to ensure it didn't carry over the malware into the restored environment. It completed a cross-platform restore from the on-premises system into the Azure cloud in just 72 hours, while law enforcement kept the data center locked up for a month.


Maxiphoto and RichLegg / iStock

# Best practices

At the organizational level and the operational level, there are steps agencies can take today to begin moving in the right direction and implement backup and recovery best practices.

**Integrate the teams:** The cybersecurity and IT teams generally operate in silos. With the growing ransomware threat, it's important these two teams come together to support effective backup and recovery strategies.

> **In our research, we asked: How much improvement do you believe is required for your organization's IT backup team and your cybersecurity team to be fully aligned? More than half, 52% of respondents, said that either a complete overhaul or significant improvement is required."**
>
> *— Jeff Reichard, Vice President of Solution Strategy, Veeam*

For many, this will be a major lift. "In our research, we asked: How much improvement do you believe is required for your organization's IT backup team and your cybersecurity team to be fully aligned?" said Jeff Reichard, vice president of solution strategy at Veeam. "More than half, 52% of respondents, said that either a complete overhaul or significant improvement is required."

While it may require a culture shift, such alignment is critical. "Historically, you would restore a single system, or at most a rack of servers that were affected by a power outage," Reichard said. "We are now in a world where you are restoring your entire data center, and you have to have a way to 'clean' that restore as it's happening. That means your security team has to be involved. You'll also find security teams looking to backups to see when a compromise first took place. All those things mandate that your security team and your backup team are working hand in glove. At this point they're essentially one big team, instead of two different teams."

**Dig into the data:** To effectively safeguard data and systems, agencies must know what they are protecting. "You need to figure out what your most critical data is for the mission, and the order in which systems need to be brought up," Reichard said. That's increasingly a team effort.

Too often, "agencies have the IT folks defining how data needs to be protected, how long data needs to be retained, where it needs to go as part of that protection scheme,"

Reichard said. "But the IT team doesn't own the mission."

The agency's executive leadership — the actual line-of-business owners — should be involved in determining what are the most critical applications, the order in which they need to be recovered, where that data can go and where it can't go, Reichard added.

> **A basic tenet of zero trust architectures is that you presume a breach. You act as though the adversary is already on your network and active on your network."**
>
> *— Jeff Reichard, Vice President of Solution Strategy, Veeam*

Once decided, IT leaders can implement modernized backup and recovery tools in support of a tiered approach, ensuring the highest-value data is readily available and effectively protected.

**Protect the backups:** Bad actors know backups are an agency's best defense, and they'll go after them: Veeam research found backup repositories were targeted in 94% of attacks. A robust backup strategy therefore will include secure and resilient copies of the backups.

"A basic tenet of zero trust architectures is that you presume a breach. You act as though the adversary is already on your network and active on your network," Reichard said. That's literally true in a ransomware attack, where the bad actors will escalate their own privileges and use those to disable backup and recovery safeguards.

"That means you have to manage your backups in such a way that even an administrator can't delete them," Reichard said. "To protect the data from attackers, you need resilient copies of the backup data, copies that even the backup-admins themselves can't delete."


ATHVisions / iStock

# How Veeam helps

With over 1,400 active federal customers, Veeam has deep expertise in the government space. Veeam's federal clients include civilian and defense organizations with the highest requirements for data security and integrity across their on-premises and cloud data infrastructures.

Image Source: Space Force Tech. Sgt. Luke Kitterman

Veeam Platform provides agencies with data resiliency through secure backup and fast, reliable recovery solutions for their hybrid cloud. Veeam integrates seamlessly with AWS, Azure and Google cloud, offers native backup and application mobility for Kubernetes, and has integrations with some of the most data-intensive SaaS workloads such as Microsoft 365 and Salesforce.

Veeam Backup & Replication is the single backup, recovery, and data security solution for all workloads on-premises and in the cloud. As the foundation of Veeam Platform, it delivers simple, flexible, reliable, and powerful data protection, enabling agencies to eliminate downtime with instant recovery and stay safe from cyberthreats with native immutability and tested backups — all from one software-defined, hardware agnostic solution.

With secure backup the last line of defense against ransomware attacks, Veeam enables agencies to protect their mission-critical data with trusted immutability and instantly recover at scale when other defenses get breached.

**Learn more about how Veeam Government Solutions can help your agency protect sensitive data while driving the mission forward.**