veeam Insights

From Risk to Resilience

Proactive Ransomware Defense and Recovery for Federal Agencies

Assessment:

U.S. Federal Ransomware Threats and Defenses in 2025

As ransomware attacks grew more frequent and advanced in 2024, U.S. federal agencies confronted a rapidly evolving threat landscape.

Many federal agencies deliver essential services and process large amounts of sensitive data while navigating operational constraints, resource limitations, and uncertainty about future budgets. These challenges and other factors make federal organizations both vulnerable and high-value targets for threat actors. That's why failing to prepare for the eventuality of a ransomware attack can be costly for federal agencies. Cyber incidents may affect service delivery among constituents as well as credibility among legislators, and they can even impact national security for the U.S. and its allies.

To help organizations address these persistent cyber threats, our 2025 U.S. federal ransomware trends report shows actionable steps agencies can take to reduce risk and recover more quickly and successfully from an attack. Overall, we surveyed 900 respondents, including security professionals and IT leaders in 130 U.S. federal government organizations — comprising 82 defense agencies and 48 civilian agencies — that were affected by at least one ransomware attack resulting in encryption or exfiltration in the past year.

900

security professionals and IT leaders surveyed

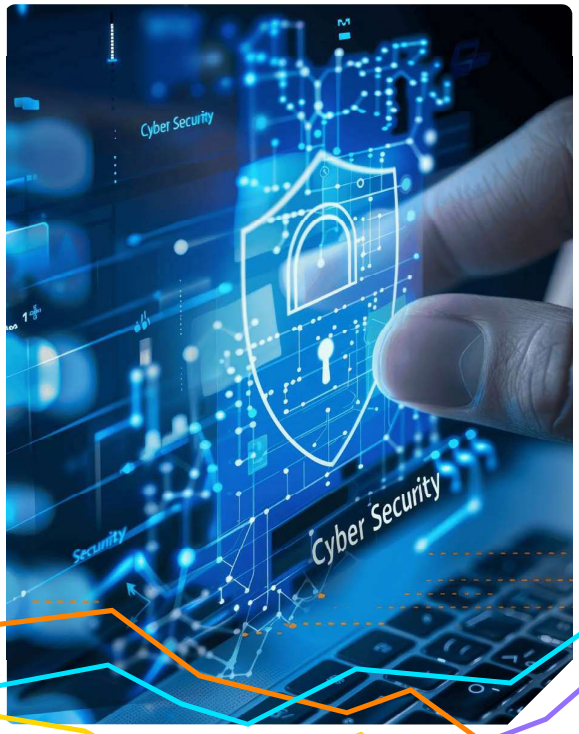
130

U.S. federal government respondents

Lower Attack Frequency, but Challenges Remain

Federal agencies experienced a lower number of ransomware attacks than private companies and other organizations during 2024.

That indicates the progress federal organizations have made in their cyber resilience practices, including with internal alignment of IT and security teams. National governments have also collaborated to disrupt and dismantle major ransomware groups, leading to changes in broader attack dynamics.



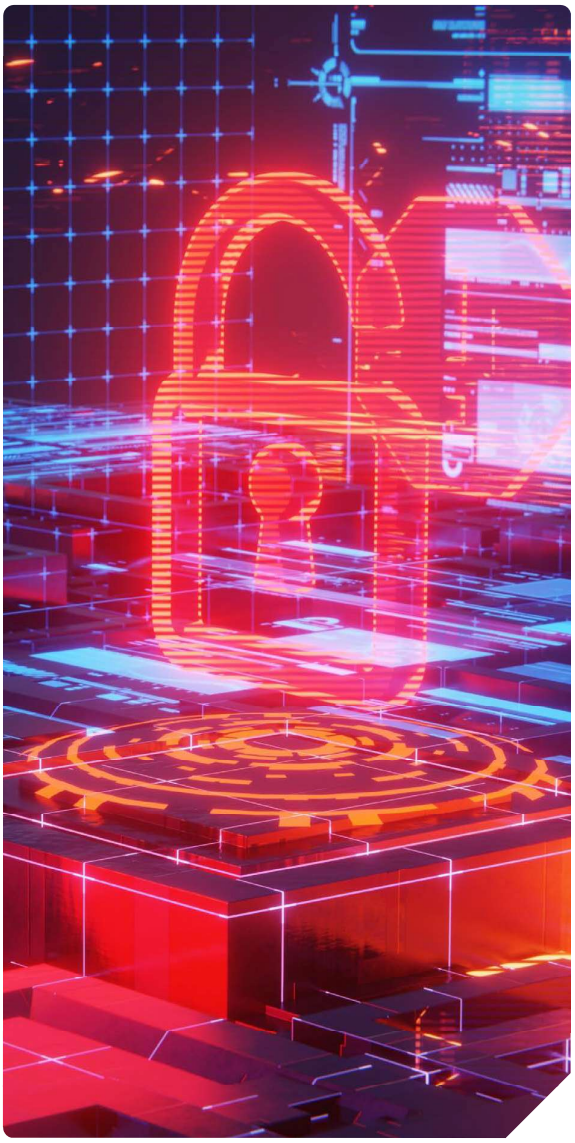
The strategies used by organizations that recovered faster from attacks, and saw better outcomes than others, reflect a set of best practices for cyber resilience that all agencies should consider implementing.

Federal agencies must shift from reactive cybersecurity to proactive cyber resilience strategies to meet the challenges of ransomware. Focusing on improving preparedness, rapid response, and secure recovery measures can significantly help reduce risk.

Our analysis reveals six key trends shaping the ransomware threat landscape in 2025 and the data-backed insights that can help federal organizations enhance resilience. We examine the latest trends across the persistent cyber threat landscape to demonstrate how successful organizations reduce ransomware risks and impacts.

6 Key Ransomware Trends To Watch in 2025

1. Law Enforcement Forces Threat Actors To Adapt
2. Data Exfiltration Attacks Grow
3. Ransomware Payments Are Decreasing
4. The Expanding Risks of Ransom Payments
5. Collaboration Supports Resilience Against Ransomware
6. Budgets Rise for Security and Recovery, but More Is Needed



Law Enforcement Forces Threat Actors To Adapt

TREND# 1

2024 saw increased scrutiny of prominent cyber threat groups and better collaboration among governments, leading to multiple enforcement actions against ransomware attackers.

In February, the UK's National Crime Agency worked with Europol and the FBI to take down ransomware-as-a-service (RaaS) group LockBit, which worked with hundreds of affiliates globally.[1] In March, the RaaS group BlackCat (also known as ALPHV) — which had already been disrupted by the FBI in 2023[2] — abruptly went dark following their successful attack targeting Change Healthcare and a sizable ransom payment.[3] And Black Basta reportedly halted RaaS activities in early 2025, evidently due to operator burnout and internal conflict according to leaked internal chat logs.[4]

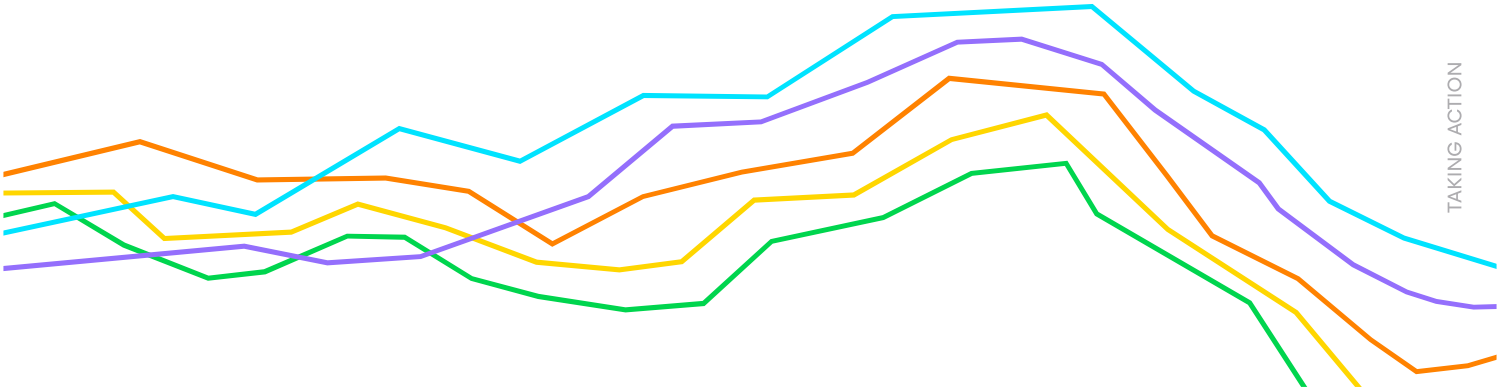
The elimination of those major ransomware groups is a welcome development, but it has prompted a new rising threat. **The number of smaller groups and "lone wolf" threat actors propagating attacks has increased.** Some of these attackers have shifted their aim to smaller entities to help reduce law enforcement scrutiny, focusing on organizations with fewer cyber defenses and targeting federal government agencies that may still use legacy systems and lax software update policies.

2024

RaaS group LockBit shut down by NCA, FBI, and Europol

2025

Black Basta reportedly halted RaaS activities

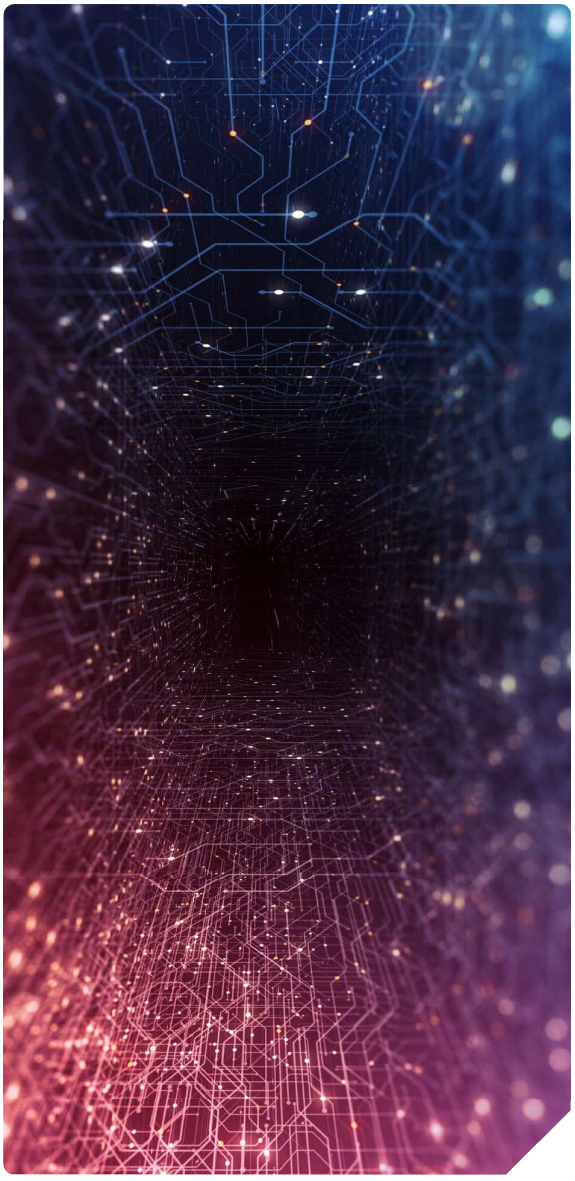


Data Exfiltration Attacks Grow

TREND# 2

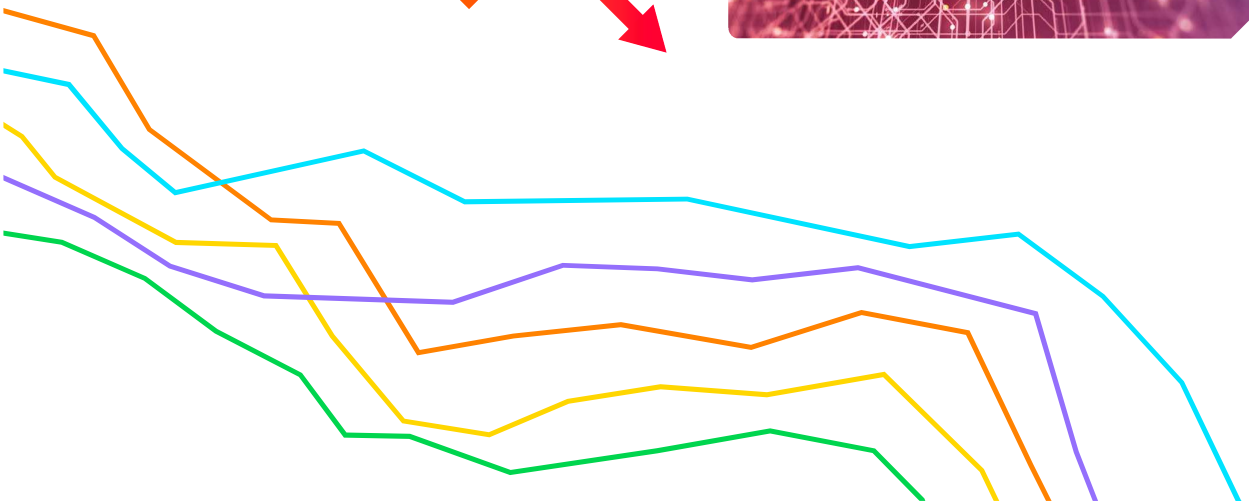
Shifting attack dynamics are another consequence of the adaptations by threat actors. Data exfiltration is commonly used along with data encryption, but Veeam tracked a rise in exfiltration-only cyber threats during 2024.[5] Unfortunately, **organizations with a weak cybersecurity posture and complex network architectures are particularly vulnerable to exfiltration and related threats.**

Data exfiltration uses what some would call a "smash and grab" approach that's common in ransomware incidents prior to encryption. These attacks often target vulnerabilities in poorly secured cloud-based applications and cloud infrastructure, such as unpatched software, misconfigured storage buckets, or inadequate identity and access management (IAM) policies. Another notable trend in line with "smash and grab" tactics is the **shorter dwell time during ransomware attacks, which can occur in just a few hours.**[6]



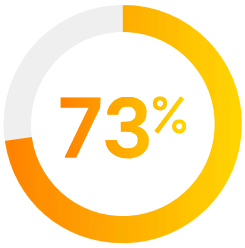
exfiltration-only threats increased

dwell time during attacks decreased

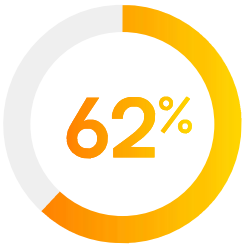


Ransomware Payments Are Decreasing

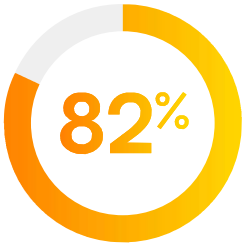
TREND# 3



of federal agencies paid a ransom



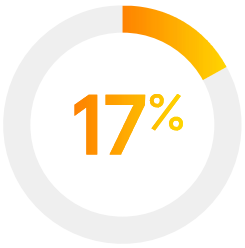
of non-federal entities paid a ransom



of organizations that paid a ransom paid less than the initial demand

of organizations paid less than half the initial demand

of organizations didn't pay a ransom and were able to recover their data

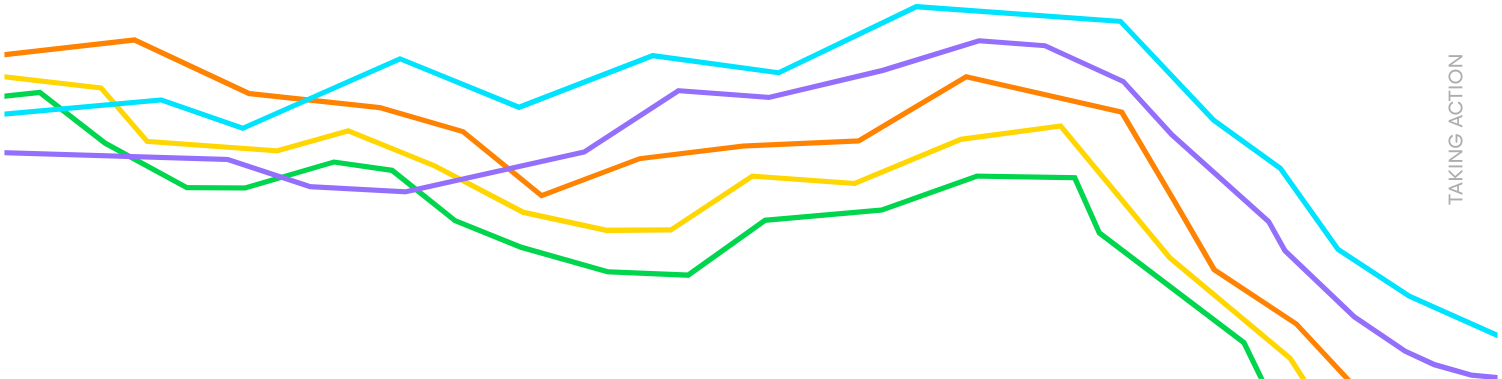


of U.S. federal organizations didn't pay a ransom and were able to recover their data

It's encouraging to see that the total value of ransomware payments decreased year over year during 2024.[7] Among all organizations surveyed that were affected by a ransomware attack, **73% of federal agencies paid a ransom compared to 62% of non-federal entities.** However, 82% of organizations that paid a ransom paid less than the initial demand, and 60% paid less than half.

This decline in ransom payments shows that organizations have made some progress toward cyber resilience, such as by developing incident response plans and using immutable backups in recovery.

Demonstrating the overarching value of cyber resilience, **25% of affected organizations didn't pay a ransom and were able to recover their data** anyway. However, that figure dropped to just 17% for U.S. federal organizations, which indicates the sector has significant room for improvement to support rapid recovery without paying cyber criminals for decryption keys.



The Expanding Risks of Ransom Payments

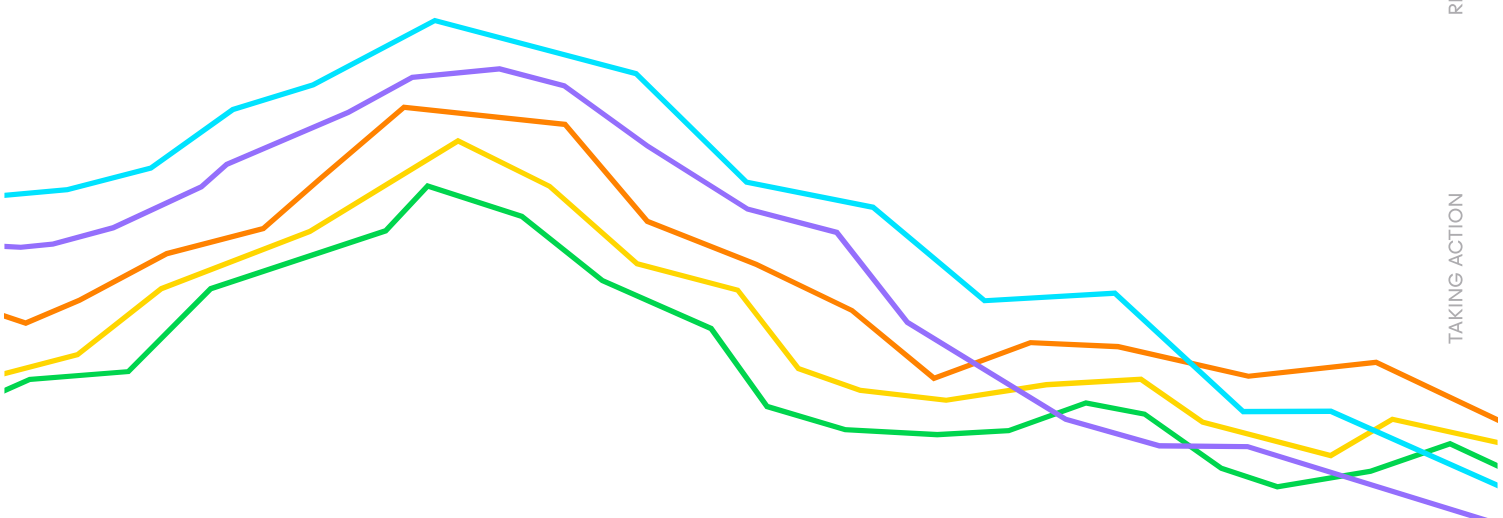
TREND# 4

Government entities face increased scrutiny and pressure against paying ransoms.

The FBI discourages organizations from paying threat actors,[8] and the U.S. Treasury Department advises there may be sanctions risks associated with payments made to entities blocked by the Office of Foreign Assets Control (OFAC).[9]

Of course, paying a threat actor doesn't guarantee decryption either — far from it. Among U.S. federal organizations, 15% of them paid a ransom and still were not able to recover their data, demonstrating the obvious pitfalls of working with attackers or relying on them for decryption keys.

of them payed a ransom and still were not able to recover their data



Collaboration Supports Resilience Against Ransomware

TREND# 5

Greater internal collaboration and good communication between IT and security teams leads to better resilience and outcomes.

However, 60% of U.S. federal organizations say significant improvement or a complete overhaul is needed to achieve this alignment. Just 12% said little improvement or no improvement is required.

Collaboration outside the organization is critical as well. Reporting ransomware and other cyberattacks to authorities strengthens collective defenses, enabling intelligence agencies, law enforcement, and technology partners to provide indicators of compromise and mitigation strategies to others in the ecosystem.

> "We are in a shared purpose of security, and we have to do that together. So, I don't think there's any way that we get to a future that is cyber secure without both the public and private entities, and their value propositions, coming together to find some solutions."

Sue Gordon

former Principal Deputy Director of National Intelligence

Watch the full interview with Sue Gordon and Veeam CISO Gil Vega.

60%

of U.S. federal organizations say significant improvement or a complete overhaul is needed to achieve alignment between security and IT

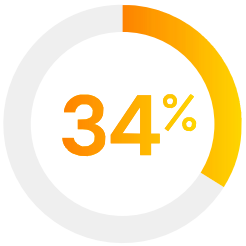
Budgets Rise for Security and Recovery, but More Is Needed

TREND# 6

While resilience against ransomware continues to improve in several areas, the expanding threat landscape demands increased budget to keep pace with evolving attack vectors. Overall, U.S. federal organizations tend to devote slightly more resources to security (34% on average) compared to recovery (30% on average).

Insufficient investments in either security or recovery weakens cyber resilience, but putting less focus on recovery can prove costly if and when an incident does occur. **U.S. federal organizations targeted by ransomware had an average of 40% of their backup repositories modified or deleted,** showing how precarious backups can be without robust protection measures.

On the plus side, **99% of U.S. federal respondents reported having increased budgets for recovery in 2025 compared to 2024, and 98% have increased budget for prevention,** indicating a growing priority to boost cyber resilience across the sector. Given the dynamic nature of U.S. federal agencies in 2025, plans may shift, but federal agencies should consider the potential for higher costs that can stem from decreasing investments in ransomware prevention and recovery solutions.



average federal agency budget devoted to security

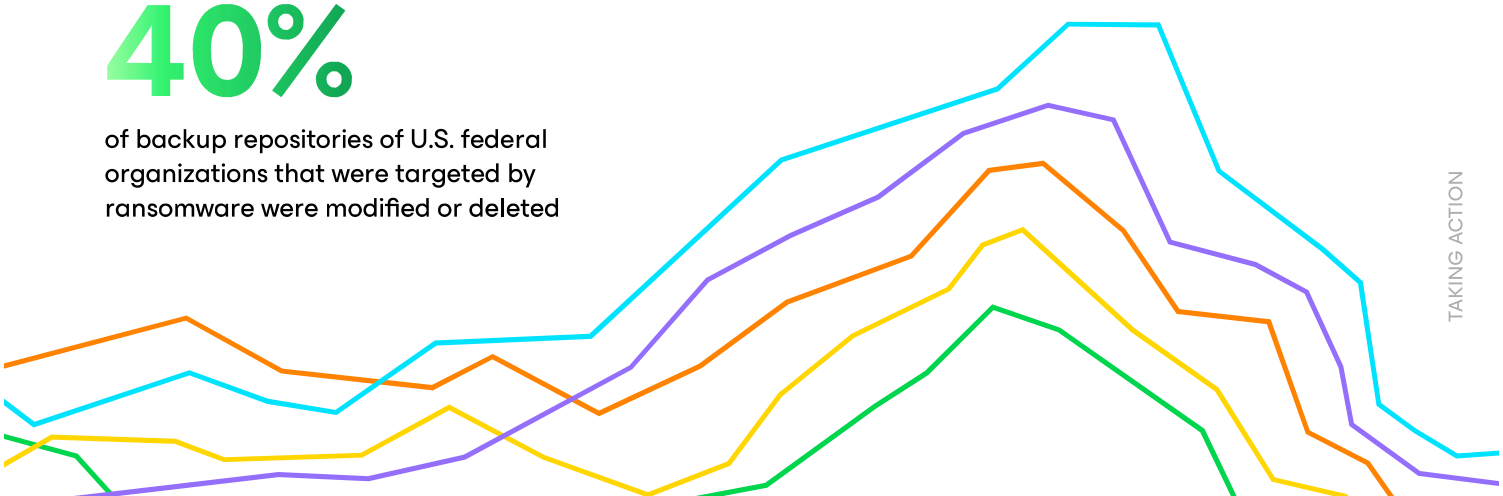
average federal agency budget devoted to recovery

of federal agencies have increased budget for recovery in 2025

of federal agencies have increased budget for prevention in 2025

40%

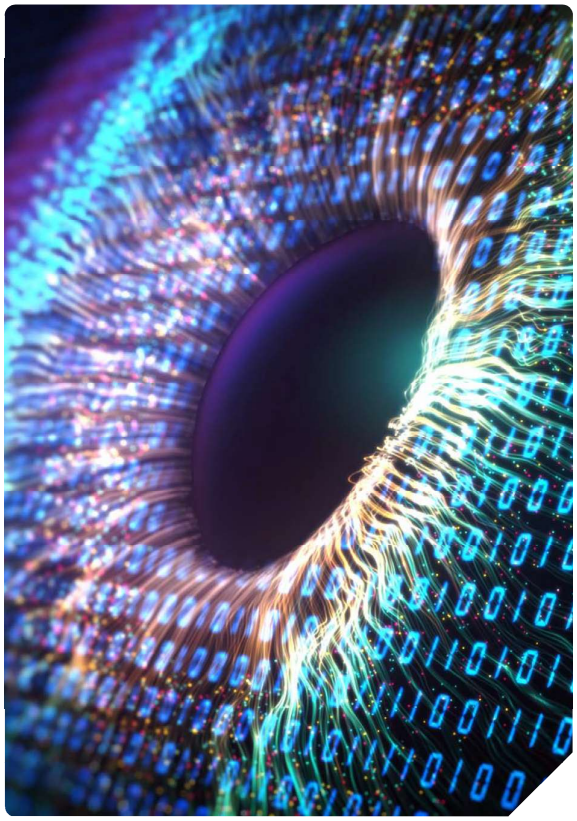
of backup repositories of U.S. federal organizations that were targeted by ransomware were modified or deleted



Ransomware Federal Agency Impact - 2024

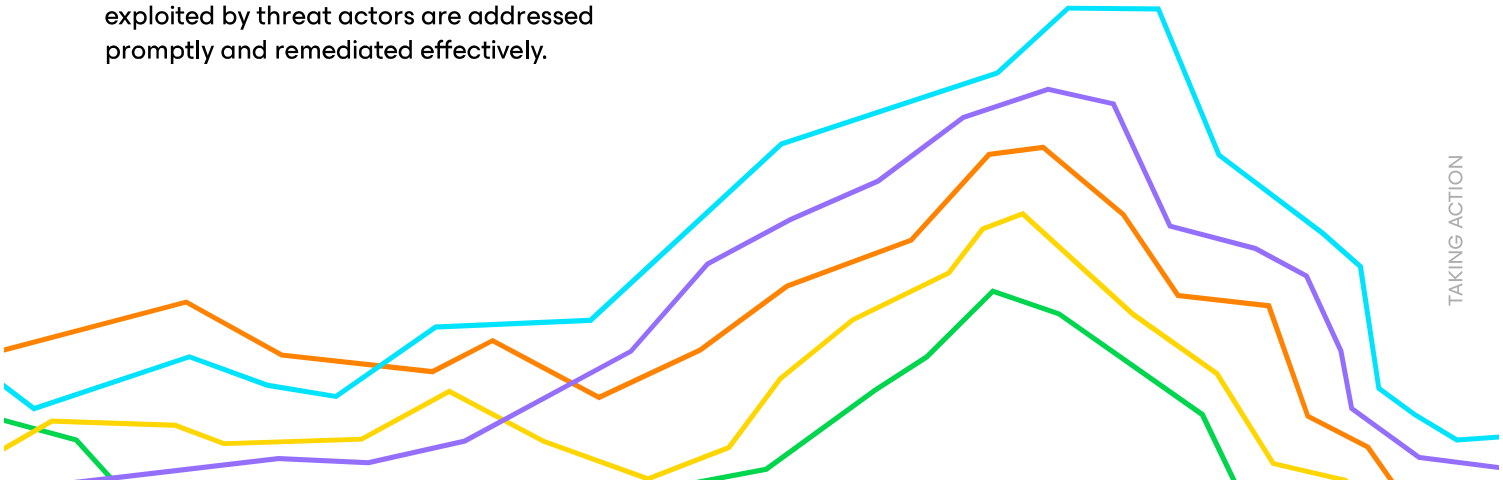
Due to the sensitive nature of their daily operations and the highly valuable data they process, federal agencies offer a promising target for threat actors looking to encrypt and/or exfiltrate data. They may also need to address legal and regulatory considerations while facing resource constraints.

Federal organizations have made progress in strengthening cyber defenses, but strict requirements, outdated systems, and scrutiny from constituents and lawmakers often delay the implementation of new security controls, leading to unintended vulnerabilities.



The survey responses highlight three clear focus areas for improving federal ransomware resilience, each with unique challenges and methods.

First, federal agencies must improve their overall cyber resilience. Second, there is a need to develop pre-defined strategies, such as comprehensive ransomware playbooks, to help reduce ransomware risks and minimize the impacts of attacks. Third, they should implement data protection best practices to address vulnerabilities, ensuring any gaps exploited by threat actors are addressed promptly and remediated effectively.



Improving Federal Cybersecurity and Recovery Preparedness

U.S. federal organizations serve as repositories for top-secret information and the most intimate data of hundreds of millions of citizens, so any attack can be devastating. According to this year's ransomware survey, 43% of federal agencies that experienced a ransomware attack resulting in encryption or exfiltration were attacked only once in the past 12 months.

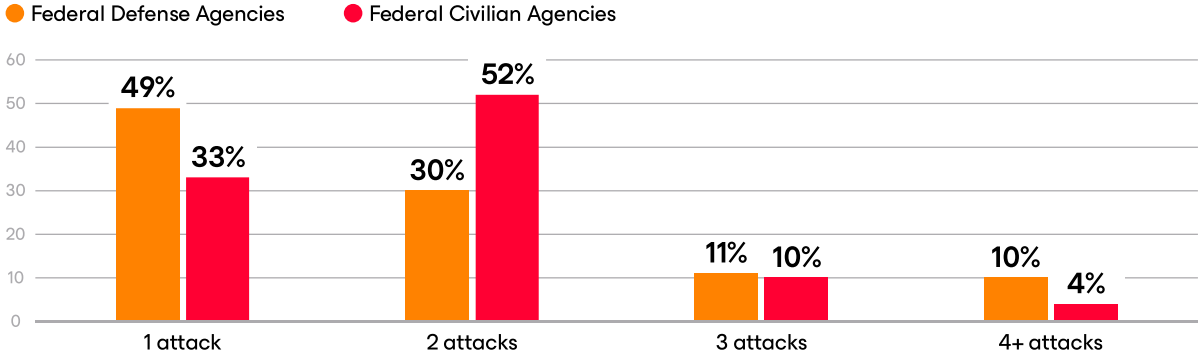
This figure was higher for defense agencies (49%) than for civilian agencies (33%), suggesting threat actors were more likely to repeatedly target agencies they judged to have relatively weaker defenses. However, **defense agencies were 150% more likely than civilian agencies to experience four or more attacks, indicating the persistence of sophisticated threats often aimed at defense organizations.**

This reflects both the highly sensitive and valuable nature of defense organizations' data, as well as the fact that defense organizations are generally more prepared for cyberattacks, resulting in many threat actors being discouraged from attacking again after their first attempt.

When attacks do happen, they can be especially costly for federal agencies, with **35% reporting increased insurance or due diligence costs as one of the biggest impacts of an attack.** But the impact of a ransomware attack on federal agencies is not only financial. Ransomware attacks can pose an outsize risk to federal agencies because of the critical work they conduct. In fact, **26% of defense respondents and 19% of civilian respondents noted the ransomware attack disrupted their mission or even posed a threat to national security.**

Federal organizations make a high-stakes gamble when they don't address inadequate cyber resilience, and the results can have significant real-world consequences.

How many ransomware attacks resulting in encryption or exfiltration has your organization experienced in the last 12 months?



Federal Agencies Overestimate Their Preparedness

Thirty-nine percent of federal entities rated themselves as "completely prepared" before an attack took place, with just 1% acknowledging they weren't prepared. **The number of federal organizations reporting that they were only somewhat prepared for an attack rose by 40% post-attack, and those reporting they were completely prepared declined by 28%.**

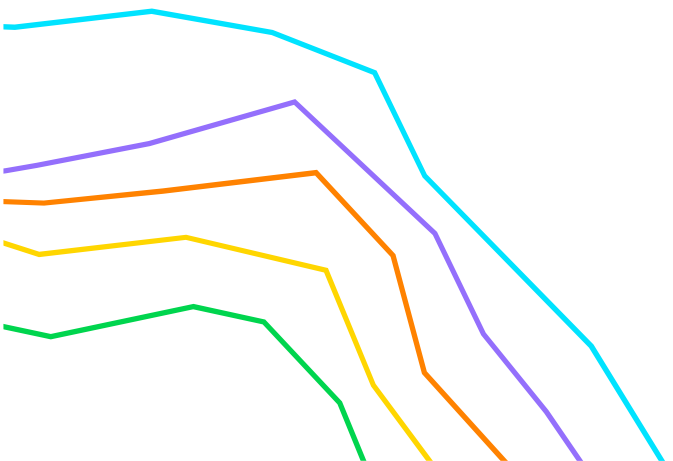
Nevertheless, **federal organizations were still 76% more likely to rate themselves as completely prepared post-attack (30%) than non-federal organizations (17%).**

30%

of federal organizations rated themselves as completely prepared post-attack

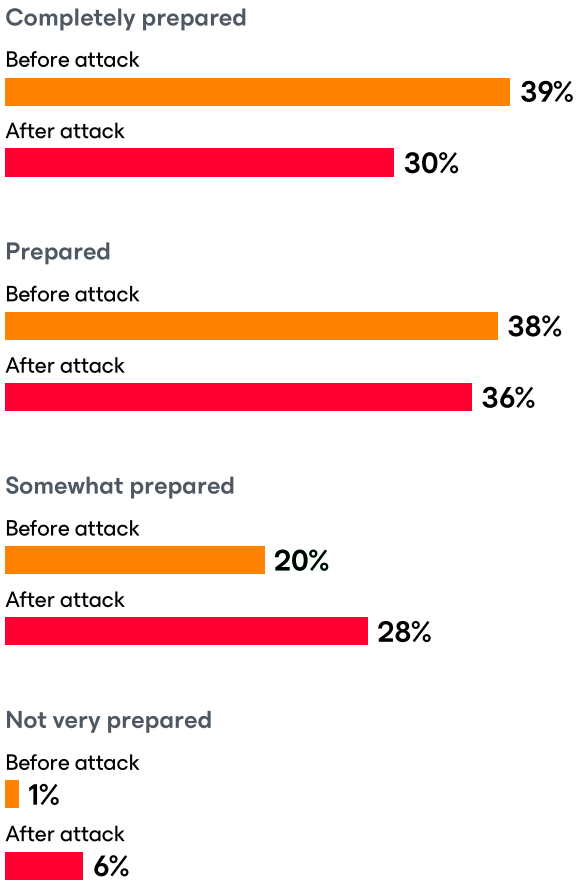
17%

of non-federal organizations rated themselves as completely prepared post-attack



Federal organizations also had different priorities in their ransomware playbooks than other organizations surveyed. For example, **federal organizations were less likely to have backup copies of data, a pre-defined chain of command for attack response, or alignment with broader disaster recovery plans.** On the plus side, 35% of federal agencies had outlined processes for engaging with law enforcement authorities compared to just 27% for non-federal organizations.

Thinking back to your most recent significant ransomware attack, how prepared did you think you were pre- and post-attack?



Misalignment of Cybersecurity and Recovery Teams

In September 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released guidance to support "Collaborative operational cybersecurity." One of the priorities was defensible architecture, setting the goal to design cyber infrastructure with an understanding that security incidents will happen, and that resilience is essential. Achieving that and related priorities requires alignment and collaboration among internal teams, but there's still plenty of room for improvement in that area.

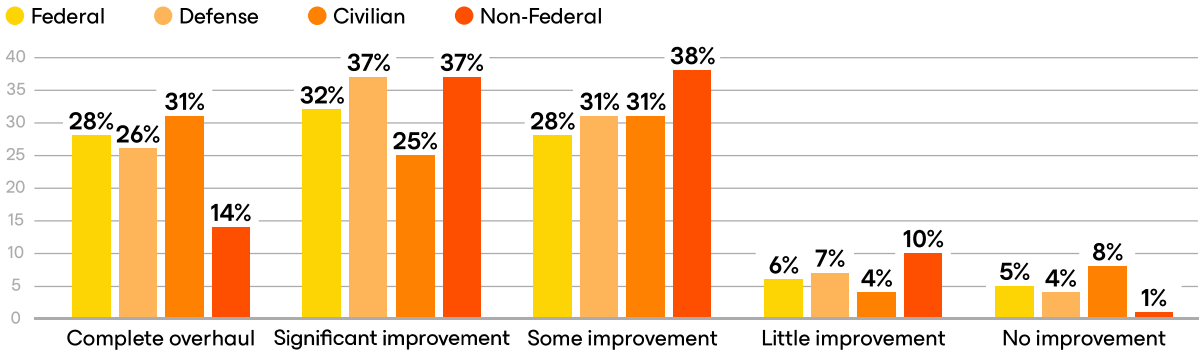
Federal respondents were twice as likely as non-federal organizations to respond that a complete overhaul was needed to fully align IT operations and backup teams with cybersecurity teams. This misalignment between recovery (typically handled by IT operations and backup teams) and cybersecurity functions was even more pronounced in federal civilian agencies, where 31% indicated a complete overhaul was needed.

The free-form responses to the survey also highlighted the importance of internal alignment, consistent communication, and strong collaboration. One person noted that "Responding to a ransomware attack requires a coordinated effort across departments," and another said "Swift communication and coordination are key to minimizing the damage during recovery." One respondent admitted they wish they had "Implemented better communication across teams."

Related to this misalignment, **federal agencies were 57% more likely than other organizations to have most or all backups modified or deleted,** and they recovered a lower percentage of server functionality following an attack. These outcomes emphasize the critical need to strengthen the strategic alignment between security and recovery teams.

To support that strategic alignment, it's critical to ensure data protection software can communicate bi-directionally with both the SIEM (security information and event management) and SOAR (security orchestration, automation, and response) software tools. SIEM collects and analyzes security data to detect potential threats, while SOAR helps automate and respond to those threats. Enabling communication among these key software tools helps integrate the people, process, and technology elements across teams, which supports better threat detection, incident response, and recovery.

How much improvement is needed to fully align your organization's IT operations backup teams with your cybersecurity teams?

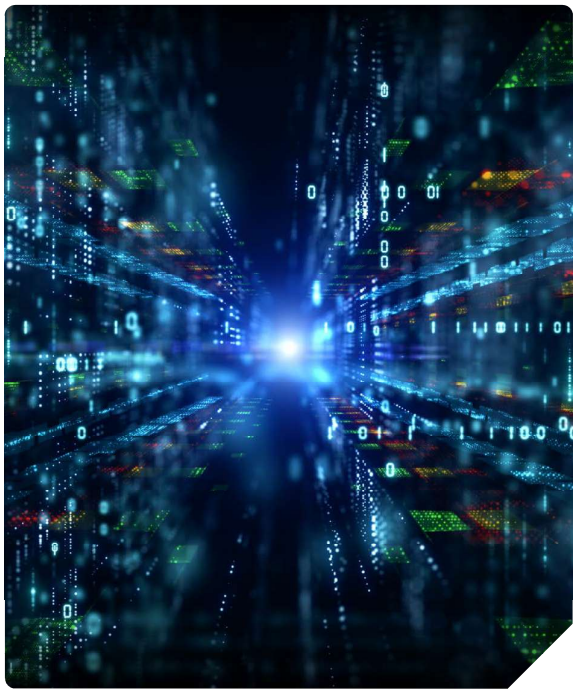


Federal Organizations Need Clearer Strategies for Dealing With Ransomware Attacks

While the FBI advises against making ransom payments and many federal agencies have policies against paying them, survey responses show a pattern of agencies paying ransomware actors.

Too many federal organizations surrender to threat actor's demands. In the federal defense sector, respondents stated they were likely to pay a ransom due to the threats made by ransomware groups, highlighting the high-pressure tactics these groups employ. Threat actors know federal defense entities must maintain national security, and they leverage threats against these missions to extort ransoms wherever they can.

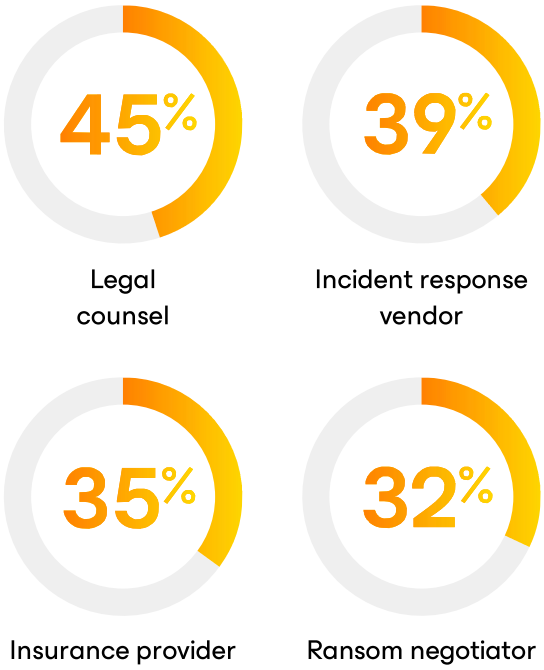
On the other hand, civilian agencies were more likely to pay to stop being targeted. **This defensive tactic of paying ransoms proved ineffective,** as it in fact encourages threat actors to target the organization again and incentivizes other cyber criminals to target that organization.



Additionally, threat actors may not provide all the encrypted data after a ransom is paid. They may also resort to a double-extortion strategy for remaining encrypted data, or threaten to leak exfiltrated data, unless a further payment is made. Triple-extortion demands can also be made by threat actors weeks or even months later, along with the potential for other types of attacks and threats made to employees, customers, and others to coerce another payment. **Paying a ransom is no substitute for an effective cyber resilience strategy.** Once an organization shows that it's willing to pay, threat actors will use a range of tactics to try and extract the maximum possible sum.

Engage Third-Party Support When Dealing With an Attack

When faced with a ransomware attack, federal agencies often engaged outside help to communicate with threat actors, and they did so more often than other organizations:

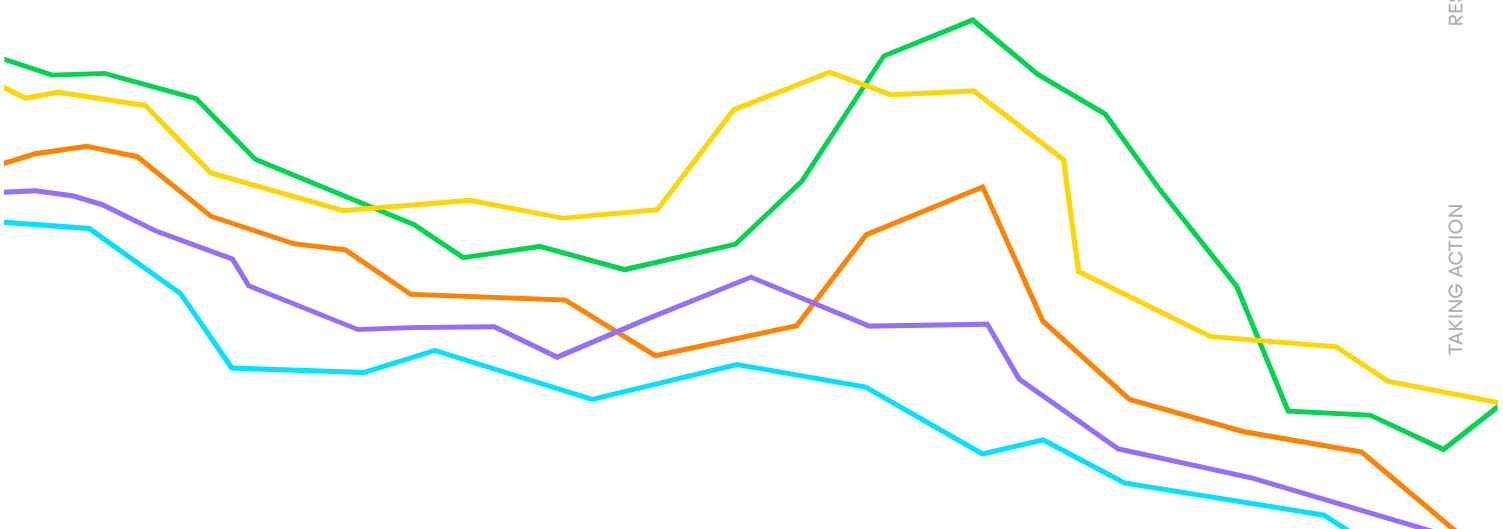


Engagement with experienced third parties can have a positive impact on incident response, particularly for entities that lack mature cyber resilience. However, **the best way to accelerate recovery is strengthening organizational resilience against cyber threats before an attack occurs.**

Proactively developing and updating a ransomware playbook with multiple key elements serves as an important tactic for boosting preparedness. It's especially important for government entities, which may face internal resource constraints and complex decision trees. Unfortunately, **just 25% of federal organizations had third-party specialist arrangements in their playbooks.** Implementing a ransomware playbook helps establish a clear chain of command for incident response and clarifies when and how to use third-party support.

25%

of federal organizations had third-party specialist arrangements in their playbooks



Data Recovery and Restoration

Cyber resilience stems from robust preparedness in both security and recovery measures. **Federal agencies were 27% more likely than non-federal organizations to use a decryption tool from the threat actor, and they were 28% less likely to restore data from backups or replicas.** That divergence points to the insufficient recovery options that force organizations to rely on untrustworthy threat actors rather than secure backups to restore critical data.

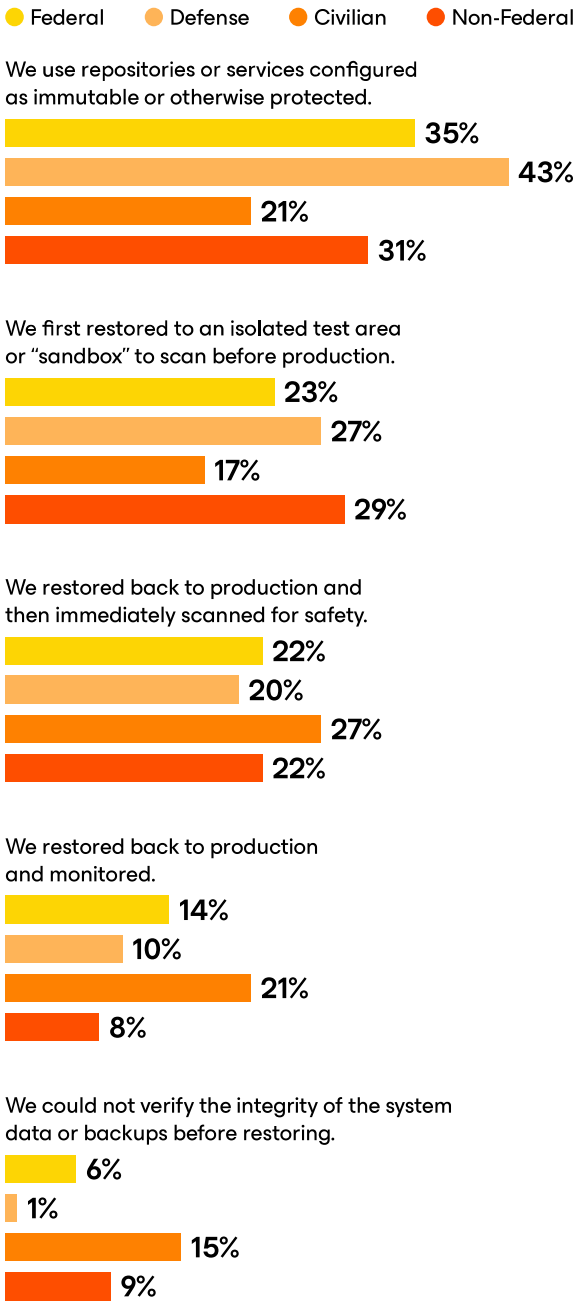
Federal entities also used less secure measures overall than non-federal organizations to check for malware before restoring system data to production, but there was a notable divergence among federal entities using that method. Defense agencies were more than twice as likely as civilian agencies to use immutable repositories, underscoring a critical gap in recovery planning and remediation measures among civilian agencies.

Worse still, 15% of federal civilian agencies reported not being able to verify the integrity of system data before restoring — compared to just 1% of defense agencies — underscoring the need for a change in their backup strategies.

IT and security leaders must ensure that data and backups are scanned and free of malware before restoring to production, or else they risk a range of consequences, including: reinfection, lateral movement, persistence mechanisms, delayed detonation, sustained business interruption, compliance violations, and more.

When asked about which key things they wish their organization had done differently before the attack, hindsight was clear: Federal defense agencies were twice as likely as civilian agencies to say they would have implemented immutable storage for backups. That suggests an awareness gap about the critical importance of using immutable configurations for backups, especially considering that threat actors successfully modified or deleted at least some backup repositories in 66% of ransomware attacks.

How did the organization ensure system data or backups were free from malware prior to restoration?

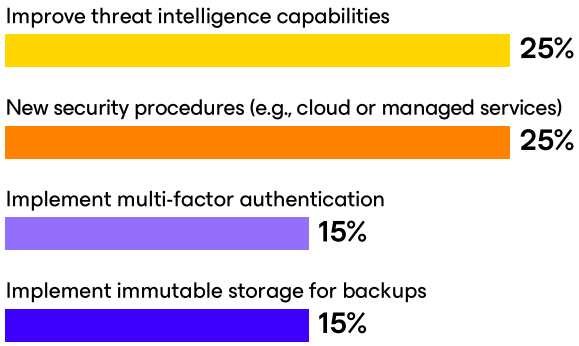


Post-Attack Improvements: Not Implemented Often Enough

After an attack happens, every organization must thoroughly evaluate what went wrong with their cybersecurity defenses, outline what could have been done differently to prevent the attack, and put in place an improved incident response plan for dealing with ransomware attacks when they happen. Unfortunately, too few federal organizations clearly followed these steps in the aftermath of being attacked in 2024, leaving them vulnerable to future attacks.

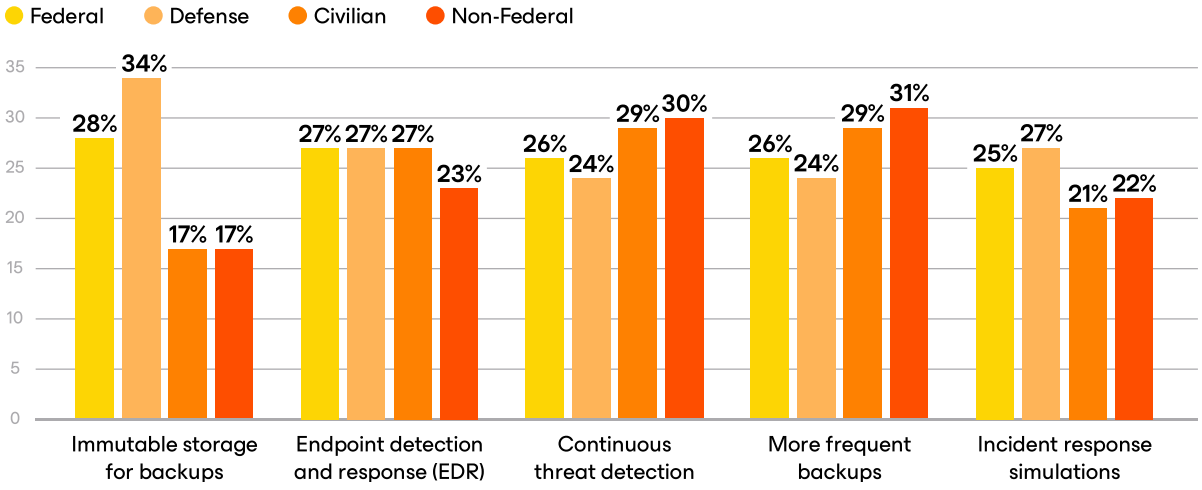
Not having these measures in place before the attack points to inadequate preparedness and cyber resilience, but it also reflects the operational challenges government agencies must navigate. Public organizations face longer approval processes for changes due to strict regulatory compliance burdens and tend to rely on legacy IT systems, which may hamper the use of some best practices for cybersecurity.

Only 26% of federal organizations showed a lower propensity than other surveyed organizations to increase budgets for security and backup. They were also less likely to take the following measures:



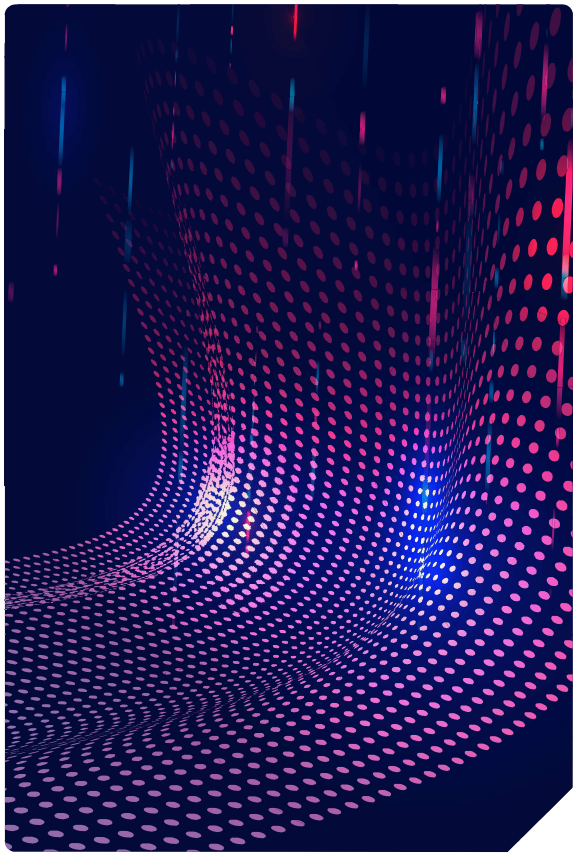
One positive trend is the greater likelihood of civilian agencies to **adopt zero trust** principles in response to an attack (35%) than either defense agencies (21%) or non-federal organizations (23%). Even if internal considerations add complexity among federal entities, more organizations should consider implementing zero trust in the near future to improve resilience.

How did the organization ensure system data or backups were free from malware prior to restoration?



Veeam's Kubernetes Data Protection Strategy for Federal Organizations

Federal organizations face a challenging mix of growing ransomware threats and strict compliance requirements which may impede defenses. Veeam's Kubernetes-native backup solutions help to protect mission-critical applications, while ensuring recovery of vital data, through a combination of:



- Immutable backups
- Automated policy-based protection
- Zero-trust security model
- Multi-cloud flexibility
- Instant recovery and disaster preparedness

Read more about Veeam's modern data protection for mission-critical applications for government.

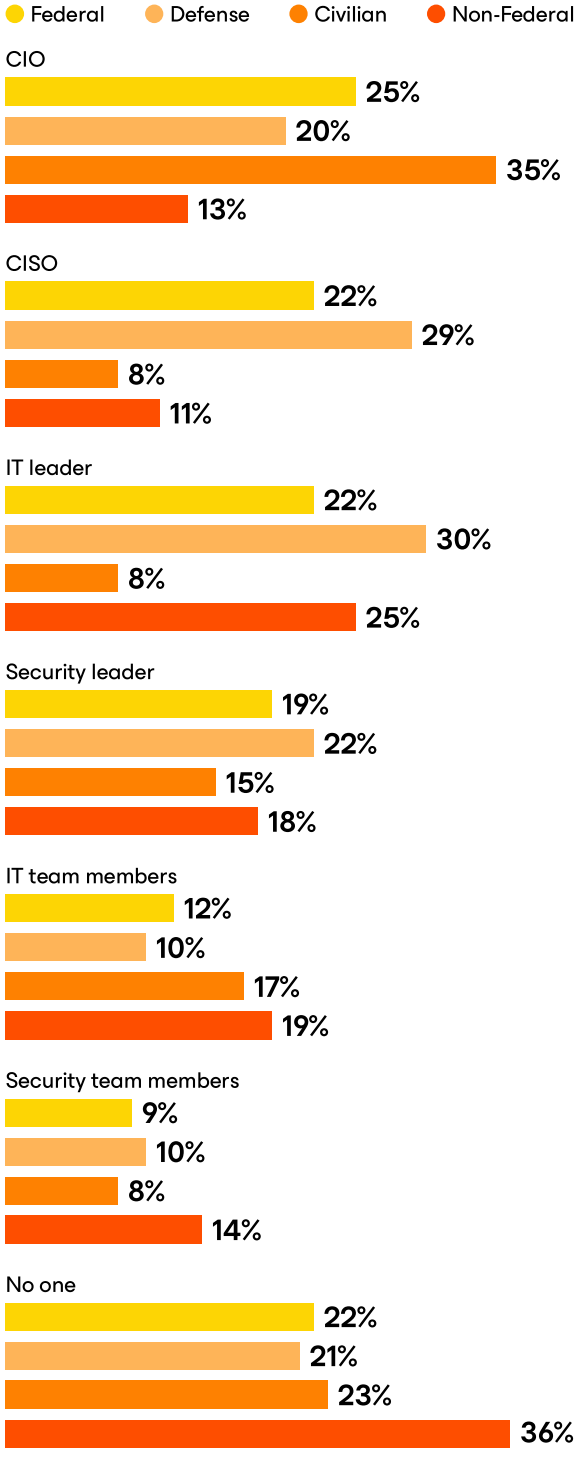
Leadership Accountability and Organizational Fallout

Given the critical nature of federal organizations' work — often involving highly sensitive data, national security concerns, and essential services for constituents — the workforce repercussions of a damaging ransomware attack tend to be more severe.

In order to fulfill their responsibility to constituents, facilitate mission delivery, and support continued stakeholder trust, federal agencies should take steps to shift from reactive security to proactive cyber resilience strategies. By following the steps outlined in the final section, federal organizations can reduce risk and improve recovery outcomes before a ransomware attack takes place.

of CIOs in federal civilian organizations were terminated or reassigned as a result of a ransomware attack

Roles terminated or reassigned as a result of a ransomware attack



Turning Insight Into Action

How Federal Organizations Can Move Toward Proactive Cyber Resilience

The cyber threat landscape is shifting, but ransomware is here to stay. To keep up with rapidly evolving threats and reduce risk, **federal organizations must take steps toward proactive cyber resilience strategies. The steps needed to improve cyber resilience are clear:**

6 Steps to Improve Cyber Resilience

1. Federal agencies should **enhance collaboration of IT operations and backup teams** with cybersecurity teams to improve threat prevention and recovery.

2. Agencies must **invest more in immutable backups and network segmentation,** which can protect critical data from modification or deletion and limit lateral attack movement.

   - Consider using the 3-2-1 backup rule: maintain three copies of your data; use two different types of media for storage; and keep at least one copy off-site.

3. **Expand incident response training,** including joint exercises, to improve detection and recovery speed.

4. **Increase the use of proactive security measures,** such as multifactor authentication (MFA), identity and access management, and cloud/managed services to minimize attack success.

5. **Leverage AI-driven security tools** for faster threat response and to maximize the impact of limited cybersecurity budgets.

6. **Engage with government-led cybersecurity initiatives** by encouraging reporting and information sharing to strengthen collective defenses.

When an attack does take place, ensure the organization focuses on collaboration and communication to support a rapid response. Having **pre-determined and well-rehearsed strategies** with a clear chain of command as part of the ransomware attack playbook significantly helps **provide a roadmap for recovery.**

In the aftermath of an attack, federal organizations should review the threat, address root causes, identify any gaps, and take the necessary steps to continue building ransomware resilience practices that better protect the missions and constituents they serve.

Proven strategies exist for ransomware defense and recovery. Don't wait for a cyberattack to happen — take the necessary steps to reduce risk and fortify your agency's resilience today.

Contact Veeam to learn more about how their experience and security solutions for federal entities can enhance your cybersecurity posture and help accelerate recovery.

Methodology

This year's ransomware report surveyed 130 U.S. federal government organizations, composed of 82 defense agencies and 48 civilian agencies that had experienced at least one ransomware attack resulting in encryption or exfiltration in the past 12 months. They were part of the 900 survey respondents that experienced as least one such ransomware attack, spanning multiple industries and regions, with roles including CISOs or executives with similar responsibilities, as well as security professionals and backup administrators.

1 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

2 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

3 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

4 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

5 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

6 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

7 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

8 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

9 https://ofac.treasury.gov/media/912981/download?inline

veeam Insights