merlin cyber

CYBERARK INFOSEC GLOBAL FEDERAL veeam

SOLUTION BRIEF


# Protecting Against Ransomware with a Comprehensive Cybersecurity Strategy for Detection and Prevention

The cybersecurity threat landscape is evolving faster than ever, and government agencies are at the forefront of defending the nation's critical systems and infrastructure. Ransomware and other forms of malware pose an especially major threat to federal agencies and their mission-critical systems, data, endpoints, and infrastructure. As threat actor's tactics, techniques, and procedures (TTPs) become more sophisticated, it is an arms race between these cyber adversaries and the federal government implementing cybersecurity best practices, enforcing actionable strategies, and leveraging innovative solutions to secure the attack surface and ensure national security.

## Common Ransomware TTPs

**Phishing & Social Engineering**
Attacks stemming from a user clicking on a malicious attachment or link.

**Exploitation of Unpatched Vulnerabilities**
Outdated software is exploited as a threat vector for cybercriminals to gain unauthorized system access and execute ransomware.

**Privilege Escalation**
Threat actors seek local or domain administrative privileges to enter systems undetected.

**Lateral Movement**
Once threat actors infiltrate, ransomware is executed across the network to infect multiple systems.

**"Living Off the Land"**
Attackers use legitimate tools (e.g., PowerShell) to evade conventional detection mechanisms.

**Fileless Attacks**
Injecting malicious code directly into memory, bypassing file-based detection mechanisms.

**Disabling Security Controls**
Attackers disable or tamper with EDR or Anti-Virus solutions once they attain administrative-level access.

**Data Exfiltration & Encryption**
Attackers pressure victims to pay ransom through double extortion attacks that exfiltrate data first, delete backups, and then encrypt files.

Considering that ransomware is one of the most common and severe attack vectors utilized by the cybercriminal world of nation-state and other organized threat actor groups, it is paramount for federal agencies to benchmark processes for a comprehensive and cohesive cybersecurity strategy. Specifically, these processes must be aligned with Zero Trust principles and centered around an actionable and repeatable cybersecurity lifecycle of detection, protection, response, and recovery. By implementing a robust cybersecurity strategy built around a Zero Trust framework and innovative software solutions, federal agencies can identify, evaluate, and respond to security threats with a proactive approach and automated security controls.

## Current Gaps in Federal Cybersecurity Strategies

To effectively combat cybercriminals and their constantly evolving TTPs, federal agencies require a holistic strategy built on innovative solutions to automate key cybersecurity processes. Unfortunately, many agencies currently lack each necessary piece of the puzzle for a comprehensive cybersecurity lifecycle and best practices. Without effective procedures and solutions in place to adequately address cybersecurity protection, detection, response, and recovery, agencies continue to struggle operationalizing Zero Trust and mission-critical data remains at a heightened risk of exploit.

Many agencies focus their security controls on addressing cybersecurity processes like vulnerability management and threat detection & response. For example, Endpoint Detection and Response (EDR) solutions are commonly utilized in federal environments to automate threat detection and response processes. Although these capabilities are essential to maintain cybersecurity posture, they alone are not enough to adequately prevent ransomware and other sophisticated threats. EDR and vulnerability management solutions fail to completely satisfy protection and recovery from Ransomware attacks. Specific limitations include:

- **Reactive Remediation and Prevention Gaps**: EDR solutions frequently detect and respond to security threats after they have already executed on endpoint threat vectors. This leaves a window open during which ransomware can move laterally or encrypt systems before detection and remediation is possible.
- **High Alert Volumes and Noise**: Countless number of alerts, false positives, and lower severity events contribute to noise that can overwhelm security teams and increase the risk of overlooking alerts on critical threats.
- **Privilege Escalation and Cryptographic Security Blind Spots**: EDR solutions do not inherently manage user privileges, secure human and machine identities, or detect threats related to cryptographic vulnerabilities. Cybercriminals frequently exploit excessive privileges or unmanaged identities and cryptographic algorithms to execute and spread ransomware.
- **Susceptible to Evasion Techniques**: Cybercriminal groups employ “living off the land” tactics using tools like PowerShell or other fileless attacks, which can evade EDR detection and result in costly system compromise.

**This reality emphasizes the need for federal agencies to implement EDR solutions for continuous monitoring and effective threat detection & response, endpoint privilege management (EPM) solutions for granular control over identity security and privileged access management, cryptographic security solutions to identify and remediate vulnerable algorithms, and data resiliency solutions for fail-safe backups and ransomware recovery.**

## Ransomware Protection

Many federal agencies currently have EDR solutions in place for continuous monitoring and threat detection & response capabilities. These solutions assist with detection and response activities; however, agencies also require solutions to address ransomware protection and prevention. This means agencies must also adopt solutions for cryptographic vulnerability management, identity security, and privilege management. Integrating the above capabilities with existing EDR tools enables agencies to achieve comprehensive ransomware protection. Solutions such as CyberArk and InfoSec Global Federal strengthen existing EDR capabilities to close privilege-based and cryptographic security gaps to proactively protect against ransomware exploitation:

CYBERARK®

### Endpoint Privilege Manager (EPM)

**Least Privilege**
- Remove local admin rights.
- Enforce least privilege.
- Step-up authentication.

**Threat Protection**
- Defend against ransomware
- Stop credential theft

**Integrations**
- Out-of-the-box policies and integrations
- Endpoint and network security solutions
- Identity products
- SIEMS
- Help desk platforms

**Improved Visibility**
- Policy audit

**Robust Cryptographic Agility and Security**

- InfoSec Global Federal's AgileSec Analytics comprehensively scans all cryptographic objects across the agency to identify weak, foreign, or malicious algorithms that may serve as threat vectors for ransomware attacks.

**Enforces Least Privilege and Zero Trust Principles**

- CyberArk EPM automatically removes local administrative rights from endpoints without disrupting user productivity.
- Restricts what actions users and applications can perform, reducing the risk of ransomware execution and spread.

**Enables Just-in-Time Privilege Elevation**

- CyberArk EPM grants elevated privileges only when necessary and under strict policy-based controls.
- Reduces the attack surface by preventing exploitation of always-on administrative rights.

**Application Control & Allowlisting**

- CyberArk EPM automatically blocks unauthorized or malicious applications from running.
- Granular application control ensures ransomware binaries or scripts are unable to execute, even if other security solutions are bypassed.

**Automated Policy Creation & Management**

- CyberArk EPM intelligently learns application behaviors and creates dynamic policies to allow, restrict, or elevate privileges – reducing manual and redundant efforts.
- Security policies remain current and aligned with dynamic business and user requirements.

**Reduced Exposure to Zero-Day Attacks**

- CyberArk EPM controls privileges and restricts unknown executables to reduce the potential damage of zero-day ransomware attacks.
- Threat actors cannot escalate privileges or disable security tools on endpoints with EPM in place.

## Ransomware Protection and Recovery for Mission-Critical Data

Now that federal agencies have fortified their cybersecurity lifecycle with ransomware protection, detection, and response controls, a vital final layer of security is implementing a solution for reliable backups and recovery. Adopting a robust ransomware recovery solution completes a comprehensive cybersecurity lifecycle that is aligned with best-practices and Zero Trust principles. Considering that cybercriminal TTPs will continuously evolve to exploit emerging vulnerabilities, it is paramount for agencies to have a fail-safe mechanism to secure and restore mission-critical data in the case of compromise. Veeam ensures robust data resiliency and comprehensive ransomware eviction and recovery:

**Automated and Secure Backups**
Veeam automatically stores backups in tamper-proof/air-gapped repositories to prevent threat actors from modifying or deleting sensitive data.

**Comprehensive Ransomware Eviction**
Veeam automatically scans backup files for ransomware and other malware-related threats to prevent the reintroduction of infected or compromised data during system restoration.

**Granular Restoration Control**
Veeam can restore entire systems or machines, specific applications, or individual data files for fine-grained control over ransomware recovery.

**Rapid Recovery to Reduce Downtime**
Veeam restores mission-critical systems in a comprehensive and efficient manner to minimize financial and operational impact of ransomware-related downtime.

**Validate Secure System State**

Veeam ensures backups are secure and ransomware-free before reintroduction to production environments with immutable backup storage, automated verification, and sandbox testing.

**Zero-Trust Data Security**

Veeam's Security and Compliance Analyzer ensures data backups are aligned with Zero Trust principles, regulatory compliance requirements, and security best-practices.

**Cloud and On-Premises Flexibility**

Secure data and systems hosted across on-premises and complex, hybrid or multi-cloud environments. Backups can also be stored on-premises or in the cloud.

## Cyber Resilience Relies on Planning

**Identify**

What data can you not afford to lose?

**Protect**

How do you backup your mission critical data?

**Detect**

Can you detect data loss and corruption?

**Respond**

Can you restore fast and accurately?

**Recover**

Are your disaster plans tested and current?

## Operationalize Zero Trust and Prevent Ransomware with Merlin Cyber

A multi-layered security approach ensures that federal agencies have the necessary controls implemented for effective ransomware protection, detection, response, and recovery. Integrating identity security and privilege management with EDR, backup & recovery, and cryptographic security solutions ensures mission-critical data is protected from ransomware and national security is maintained. Adopting the aforementioned cybersecurity processes and solutions not only enables agencies to achieve a robust cybersecurity lifecycle but also modernize and align their cybersecurity posture with Zero Trust principles.

**About Merlin Cyber**

Merlin Cyber is the go-to-market and Zero Trust Modernization affiliate of Merlin Group, a network of companies that invests in, enables, and scales technology companies with disruptive cyber solutions. Through Merlin Cyber, the U.S. Government can access innovative, public sector-ready cybersecurity solutions that are designed to meet government requirements and mission priorities. Merlin does this by selectively partnering with best-in-class cybersecurity brands, investing in visionary emerging technologies, and enabling the U.S. Government to successfully keep ahead of today's critical threats, accelerate Zero Trust modernization initiatives, and defend our nation.

Learn more at:
**merlincyber.com**

Contact:
**info@merlincyber.com**