FedRAMP

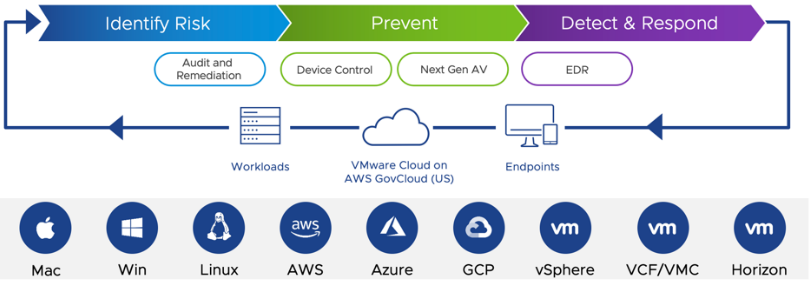
VMware Carbon Black Cloud on AWS GovCloud (US)

Modern endpoint security and advanced workload protection for the public sector

The United States government faces increasingly advanced cyberattacks that target sound infrastructure to inflict damage. These sophisticated hacking methods use advanced tactics and pose a tremendous risk to sensitive data and state secrets. As a result, public agencies are facing a mandate for federally compliant, cloud-delivered security solutions to protect critical assets and stay one step ahead of adversaries.

With VMware Carbon Black Cloud on AWS GovCloud (US), public sector customers can meet such demands and deploy modern endpoint security and advanced workload protection required to face today's complex attacks. The platform enables government agencies to prevent, detect, and respond to threats on endpoints and service workloads from a single console for improved visibility and simplified operations.

Adhering to the rigorous requirements of the Federal Risk and Authorization Management Program (FedRAMP), Carbon Black achieved FedRAMP High authorization through the Joint Authorization Board (JAB). In partnership with VMware Government Services (VGS), the platform was vetted by the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA) and cleared for use on a government-wide scale. VMware Carbon Black Cloud is a streamlined solution for federal, state, and local agencies to utilize and modernize their IT infrastructure.



BENEFITS

- FedRAMP High JAB Authorization
- Vetted by Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA)
- Direct access and integration with AWS GovCloud (US)
- Meet Continuous Diagnostics and Mitigation (CDM) requirements
- Secure data with US federal specific trust standards
- Third party verified so key vulnerabilities are not ignored
- Cost-effective solution with no hardware investment
- Continuously monitored to maintain government standards

RESOURCES

- VMware Cloud Trust Center
- VMware Carbon Black Cloud with VMware Government Services (VGS) on FedRAMP marketplace
- VMware Carbon Black Cloud FedRAMP High authorization on the VMware Security Blog

vmware | aws

Key Capabilities

VMware Carbon Black Cloud™ on AWS GovCloud (US) is optimized to protect highly sensitive government data against would-be attackers. The platform delivers enhanced endpoint telemetry and threat intelligence to public sector customers in their adoption of zero trust security strategy.

Secure highly sensitive government data

To ensure that cloud systems used by government agencies have adequate safeguards in place, they are required to modernize their IT infrastructure. With the FedRAMP High authorization, VMware Carbon Black Cloud gives you the ability to secure highly sensitive government data with to meet security and compliance requirements needed for federal agencies.

Protect against ransomware

Stay up-to-date and protect your data against ransomware with rapid cloud releases. Proactively identify risk and investigate events to reduce the attack surface by setting specific ransomware polices or utilizing default mode ransomware protection.

Enhance your Zero Trust security strategy

With advance analytics, the platform securely collects and visualizes comprehensive information about endpoint and workload data, giving you increased visibility for a stronger Zero-Trust strategy.

Utilize complete endpoint and workload protection

Built on Carbon Black Cloud in partnership with AWS GovCloud (US), provides you with advanced threat hunting and incident response functionality from the same agent and console as our NGAV, EDR, and real-time query solutions, allowing your team to consolidate multiple point products with a converged platform