CrowdStrike Solutions

CROWDSTRIKE

FedRAMP

CROWDSTRIKE FALCON ON GOVCLOUD

Secure your public sector enterprise with a solution that provides unrivaled protection and optimal scalability.

DELIVERING MORE SECURE AND EFFICIENT SERVICES

The 2018 Verizon Data Breach Investigations Report (DBIR) showed that the public sector is one of the top three most exploited sectors in the United States, with more than 300 reported cyber breaches in 2017 alone. Highly resourceful adversaries — often nation-state sponsored or affiliated and equipped with an arsenal of advanced tactics, techniques, and procedures (TTPs) — continue to overwhelm security teams that are already pushed to the brink. As a result, bad actors continue to slip through agency infrastructure cracks, resulting in dwell times averaging well over a year.

To counter this trend, federal, state and local governments have increasingly mandated that public sector organizations modernize their IT infrastructure, as well as their overall approach to cybersecurity risk management. In their research article "Get Ready for the Inflection Point in U.S. Federal Government Cloud Adoption[1]", Gartner highlights that federal government CIOs are poised to make a major push into the commercial cloud in 2018 and beyond*. CrowdStrike believes that although this push will greatly enhance services, evolving this framework and protecting against modern threats remains a daunting task, and moving sensitive data to the cloud brings its own set of new risks.

KEY BENEFITS

Ready for public sector

Move to the cloud with confidence and trust

Unmatched in protection and visibility

Stops breaches and keep your data safe

Scalable and Efficient

A lightweight, unified solution that scales with you

[1] Source: Gartner, "Get Ready for the Inflection Point in U.S. Federal Government Cloud Adoption" by Rick Holgate and Neville Cannon. Published: January 19, 2016, Refreshed June 9, 2017.

DELIVERING ENDPOINT PROTECTION, FROM THE CLOUD, WITH US FEDERAL SPECIFIC TRUST STANDARDS

Moving critical capabilities such as security into the cloud requires careful consideration of a wide range of privacy and security assurances. Programs such as the Federal Risk Authorization and Management Program (FedRAMP) and DoD Cloud Computing Security Requirements have been developed in order to increase the confidence in the security of cloud solutions and accelerate their adoption.

Amazon Web Services (AWS) is one of the industry's most well known, broadly utilized providers of cloud-based infrastructure. AWS GovCloud (U.S.) (often simply referred to as "GovCloud") is an AWS Region designed to meet the requirements imposed by FedRAMP and other regulations. GovCloud has been validated to meet the requirements of the following regulations:

- Federal Risk and Authorization Management Program (FedRAMP) Impact Levels 2, 4 and 5
- Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG) Impact Levels 2, 4 and 5
- US International Traffic in Arms Regulations (ITAR)

GovCloud is broadly trusted by US government agencies at the federal, state and local levels, as well as contractors, educational institutions and other US customers that run sensitive workloads in the cloud.

CrowdStrike® partners with AWS to deliver next-gen endpoint protection from GovCloud: CrowdStrike Falcon® on GovCloud. CrowdStrike is the first and only endpoint protection platform delivered from AWS GovCloud (US) and also validated to meet or exceed the requirements laid out in the U.S. FedRAMP program at IL2/Moderate. CrowdStrike strongly supports the mission of civilian government, military and intelligence to deliver advanced services in a cost-effective manner, while maintaining the highest level of protection.

GovCloud is broadly trusted by US government agencies at the federal, state and local levels, as well as contractors, educational institutions and other US customers that run sensitive workloads in the cloud.

WHY CROWDSTRIKE

CrowdStrike Falcon provides a FedRAMP-authorized, cloud-delivered solution that safeguards your organization while satisfying your mission requirements. The threats the public sector faces are constantly evolving and you require a solution that proactively detects and prevents these events from occurring. CrowdStrike has built its solutions around the ability to detect and prevent breaches by even the most sophisticated adversaries. With a platform that seamlessly deploys and scales with your enterprise and a dedicated team of security professionals, CrowdStrike protects your enterprise with a solution designed to stop the breach and evolve with you.

LEARN HOW CROWDSTRIKE STOPS BREACHES

visit www.crowdstrike.com

Speak to a representative to learn more about how CrowdStrike can help you prepare for and defend against targeted attacks.

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: www.crowdstrike.com

01 READY FOR PUBLIC SECTOR

Challenge

Leveraging the cloud allows agencies to deliver more innovative services at a more agile pace. However, sensitive data must be handled with the greatest care and the cloud can put it at risk. Public sector enterprises require strong assurances that all proper security controls are in place and maintained in accordance with applicable regulations.

Solution

CrowdStrike Falcon on GovCloud provides cloud-delivered endpoint security, designed and operated to meet or exceed US federal assurance requirements.

CrowdStrike Falcon on GovCloud is FedRAMP authorized.

The first and only endpoint protection SaaS delivered from the trusted AWS GovCloud (U.S.).

The ideal solution for civilian and DoD applications at Impact Level: Moderate/IL2.

Benefit

CrowdStrike Falcon is built on the industry's most scalable, trusted platform to deliver endpoint security from the cloud that you can deploy with confidence.

02 PROTECTION AND VISIBILITY

Challenge

Public sector enterprises struggle to adequately protect their endpoints against increasingly sophisticated TTPs employed by adversaries.

Solution

CrowdStrike Falcon on GovCloud is designed with your security needs in mind and provides an arsenal to protect against all attack types:

CrowdStrike Falcon blocks known and unknown malware as well as malware-free threats.

Its continuous monitoring of the endpoint allows for rapid detection and response to malicious activity.

The IT hygiene module provides 360-degree visibility into managed and unmanaged assets, users and applications.

Benefit

CrowdStrike provides a single, powerful, unified solution that is focused on enabling public sector enterprises to improve visibility, stop breaches and keep data safe.

03 SCALABILITY AND EFFICIENCY

Challenge

As enterprises grow and become more distributed, an increasingly broad attack surface is provided for sophisticated adversaries targeting your data and IT infrastructures. The success of such attacks has been well-documented in recent years, showing the inherent vulnerabilities in conventional on-premises, network- and malware-centric defenses.

Solution

Crowdstrike protects your enterprise as you scale by deploying across all IT environments and operating systems:

With a lightweight agent that deploys in minutes, the CrowdStrike Falcon platform ensures comprehensive protection with immediate time-to-value.

Managed via the cloud, no on-premises infrastructure is required.

CrowdStrike Falcon deploys across all endpoint and data environments, including on-premises, virtual and cloud-based servers.

CrowdStrike Falcon streamlines your operational efficiency with a security solution that requires no new installs, reboots or scans.

Benefit

CrowdStrike provides an industry-leading solution that scales with your IT environment, providing comprehensive threat prevention and detection without impacting system performance.

FedRAMP

Federal Risk and Authorization Management Program

Developed to accelerate adoption of cloud-based solutions across the US government

Defines a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services

Lays out three Impact Levels (Low, Medium, High) with increasing requirements for security controls

www.fedramp.gov

DoD CC SRG

Department of Defense Cloud Computing Security Requirements Guide

Defines security controls and requirements necessary for using cloud-based solutions within the DoD

Defines six Impact Levels, with mappings to FedRAMP controls

https://iase.disa.mil/cloud_security/