# CrowdStrike Helps the State of Arizona Protect Against Security Threats Using AWS

Cyber Command, a team created by the Arizona Departments of Homeland Security and Administration, engaged AWS Advanced Partner CrowdStrike to implement a multitenant solution that facilitates near-real-time responses to cyberthreats. Cyber Command protects devices used by the State of Arizona's employees. During the COVID-19 pandemic, many employees began working remotely, requiring Cyber Command to quickly set up secure remote-work capabilities. To improve cybersecurity, the team implemented CrowdStrike's Falcon Endpoint Protection Platform to monitor for malicious activity and unauthorized behavior. Cyber Command can now detect anomalies on devices and remediate them quickly.

Cyber Command, a team created by the Arizona Departments of Homeland Security and Administration, employs 12 cybersecurity personnel charged with protecting laptops, desktops, mobile phones, and tablets used by state employees. The Cyber Command team needed a multitenant endpoint detection and response solution that it could implement without cost overruns.

Cyber Command convened a multiagency committee of technology analysts, architects, engineers, and consultants to conduct a search. Looking to Amazon Web Services (AWS) for an answer, the committee identified several possible solutions on AWS Marketplace and chose AWS Advanced Partner CrowdStrike for its Falcon Endpoint Protection Platform security environment, including its Falcon OverWatch managed threat hunting solution. Falcon provided Cyber Command with 24/7 support for its security operations center, a single dashboard for monitoring and controlling the system, and near-real-time response to security threats.

### Setting Up Infrastructure to Manage Threats Against Remote Endpoints

During the COVID-19 pandemic, thousands of Arizona's state employees were working remotely, requiring Cyber Command's cybersecurity team to quickly set up secure remote-work capabilities for employee laptops, desktops, mobile phones, and tablets. The office began rolling out CrowdStrike's Falcon Endpoint Protection Platform security environment and Falcon OverWatch solution at the start of its fiscal year in July 2020, with just 4 months until its previous protection was set to expire. "Having dedicated support went a long way toward facilitating a smooth transition," says Tim Roemer, chief information security officer of the Arizona Department of Homeland Security.

CrowdStrike provides managed endpoint protection, threat hunting, and incident response services to several public sector customers, including customers in higher education, healthcare, and federal, state, and local governments. "We've tracked about 155 adversaries, and in doing that, we have learned the tools and techniques they use to breach environments," says Mary Farrelly, regional sales manager for CrowdStrike. "We incorporated that intelligence into our products." The cloud-native cybersecurity company has an aggressive performance standard in the event of an incident: 1 minute to detect, 10

Facilitates near-real-time response to cyberthreats

| | |
|---|---|
| **Company:** | CrowdStrike |
| **Website:** | crowdstrike.com |

## About CrowdStrike

CrowdStrike is a cloud-native cybersecurity company that tracks approximately 155 adversaries known to launch security threats worldwide on corporations and governments. CrowdStrike is an AWS Advanced Partner, an AWS Marketplace Seller, and an AWS Public Sector Partner.

## About the Arizona Department of Homeland Security

The Arizona Department of Homeland Security is an Arizona state government agency that administers and manages resources related to terrorism prevention and other critical hazards.

## Benefits

- Facilitates near-real-time response to cyberthreats
- Performs remediation quickly
- Proves successful against third-party penetration tests
- Provides 24/7 one-on-one support

## AWS Services Used

- Amazon S3
- Amazon GuardDuty
- Amazon EBS
- Amazon EMR

> “Consolidating vendors under CrowdStrike and procuring the solution through AWS Marketplace provided considerable savings and freed up funds for other security projects.”
>
> —Tim Roemer, chief information security officer of the Arizona Department of Homeland Security

minutes to triage and analyze, and 1 hour to fully resolve the problem.

CrowdStrike’s Falcon engine hunts for anomalous or novel attacker tradecraft to stop sophisticated threats. This modern endpoint protection includes full endpoint detection and response, which includes next-generation antivirus and identity protection as well as a 24/7 managed threat-hunting service. Falcon is powered by a lightweight agent that is rapidly deployed to endpoints, with no reboot required or user interface for end users. CrowdStrike hosts its Falcon environment using AWS services. For example, it uses Amazon Elastic Compute Cloud (Amazon EC2) for its secure, resizable compute capacity. And to gain high-performance block storage while using Amazon EC2 instances, CrowdStrike uses Amazon Elastic Block Store (Amazon EBS) for Apache Cassandra clusters.

During the deployment of the CrowdStrike Falcon solution, Cyber Command had access to CrowdStrike University, an on-demand portal with training programs on tasks required to implement, manage, develop, and use the solution. CrowdStrike also ran monthly technology acceptance model talks, provided one-on-one support to individual agencies, and helped the team’s security operations center respond to security threats. By the October 2020 deadline, CrowdStrike had successfully migrated 80 percent of Arizona’s state agencies.

### Coping with Statewide Security Events from Worldwide Threats

The Cyber Command team needed additional tools and support to bolster its small security operations team, which manages security for thousands of state employees. The team used CrowdStrike’s Falcon Spotlight enterprise visibility solution and its Falcon Discover information technology hygiene solution to monitor for account escalations and vulnerabilities related to recent supply chain security events. “Our managed detection-and-response system caught some odd behavior on a few machines,” says Roemer. “It turned out to be some very bad malware. We were able to quickly remediate before it could spread throughout the organization.”

Although cybersecurity incidents have been few, the solution has proven successful against third-party penetration tests and has successfully alerted the Cyber Command team to malicious activity. “Consolidating vendors under CrowdStrike and procuring the solution through AWS Marketplace provided considerable savings and freed up funds for other security projects,” says Roemer.

CrowdStrike pushes data from its sensors to Amazon Simple Storage Service (Amazon S3), a scalable object storage service. And CrowdStrike runs Apache Spark using Amazon EMR, which, by automating time-consuming tasks, makes it simple for CrowdStrike to set up, operate, and scale big data environments. The result is a fast engine that CrowdStrike uses to process hundreds of terabytes of event data and roll it up into higher-level behavioral descriptions on the hosts. To support its continuous monitoring of malicious activity and unauthorized behavior, CrowdStrike uses Amazon GuardDuty, which uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats to protect CrowdStrike’s AWS accounts, workloads, and data stored in Amazon S3. This capability has helped CrowdStrike provide visibility into homegrown applications that the Cyber Command administrators didn’t know existed, triggering alerts with insights into the data accessed by those applications. The 24/7 managed detection and response system also caught instances of malware. “Devices had been connected directly to a public internet provider,” says Roemer. “We wouldn’t have known about the threat without CrowdStrike.”

### Sharing New Capabilities with Other Governments

The Cyber Command team has begun collaborating with other state government agencies to share CrowdStrike best practices and to extend coverage to smaller communities, including county, local, and tribal governments. “It’s been great to have this new venue of collaboration,” says Roemer. “CrowdStrike brought us together, so we could start having those conversations.”

Cyber Command is investigating additional products and value that it can derive from CrowdStrike in the future. For example, Arizona is preparing for an election year in 2022 and for hosting Super Bowl LVII in Glendale in 2023, so the Cyber Command team is considering using Falcon X Recon for social media and dark web monitoring to get early warning of threats.

To learn more, visit https://aws.amazon.com/guardduty/.