voices

CrowdStrike Customer Case Study

OKLAHOMA

State of Oklahoma Deploys CrowdStrike to Defend Thousands of Endpoints Against Daily Threats

If there is any doubt about the impact of cybersecurity, the words of Jerry Moore, chief information officer for the state of Oklahoma, are a poignant reminder. "Security breaches disrupt our ability to deliver critical services to citizens," he said. "An example I use is a child protection caseworker in the field whose computer is attacked and they cannot perform their responsibilities. It's imperative that every caseworker is always able to respond quickly and at the moment of need."

The online threats facing public organizations like the State of Oklahoma are acute and getting worse. "Security is more important in the public sector because the scope and scale of what we do for citizens make us a high-profile target," said Moore. "The situation is further complicated by the volume of attacks and the size of our attack surface; every user, citizen and household is a potential entry point."

The state is charged with bringing a modern digital experience to its four million citizens and ensuring services are delivered in the most efficient and effective way. It has a duty to protect assets by using data to make informed decisions and raise the cybersecurity capabilities of the whole state, not just government agencies.

Complex Attack Surface is a Prime Target for Attacks

To do this, Oklahoma has consolidated what were once siloed departments into a single, state-wide IT operation covering 77 counties, a network of 10,000 servers and 1,200 applications. The program now encompasses approximately 128 agencies such as wildlife, driver licenses, child welfare, environmental quality and health, as well as all centralized government services. As a result, the state is responsible for a total of 120,000 endpoints which, astonishingly, are hit by 61 million attacks every day!

COVID-19 exacerbated the problem because, overnight, 98% of state employees became remote workers. "We used to have 30,000 employees using state assets behind a 'castle wall' on secure networks," said Matt Singleton, chief information security officer for the state of Oklahoma. "COVID-19 removed that wall."

Stonger Together

To respond, the state set up the Oklahoma information sharing and analysis center (OK-ISAC) to shift its strategy from a castle-and-moat approach to a Zero Trust cybersecurity model. A key part of the strategy was to make security a community responsibility. "Before OK-ISAC, we had a few organizations that had threat intelligence expertise, but it was very siloed," said Singleton.

INDUSTRY

Local Government

LOCATION/HQ

Oklahoma, State of Oklahoma

CHALLENGES

- Defend complex attack surface for 128 external agencies against onslaught of daily threats
- Mitigate increasing threat from thousands of staff working remotely because of COVID-19
- Protect state services and bring a modern digital experience to 4 million citizens

SOLUTION

The State of Oklahoma has rolled out a portfolio of CrowdStrike solutions to help build a security ecosystem that extends protection beyond state operations to embrace the whole region and even into people's homes.

"We deployed a set of solutions that included CrowdStrike to give us the ability to really dig deeply into behaviors and traffic flows to understand exactly what is happening on the network."

Matt Singleton
Chief Information Security Officer
State of Oklahoma

voices

CrowdStrike Customer Case Study

OK-ISAC plays a significant role in ensuring that the state and its citizens are continuously educated and well-prepared to conduct day-to-day online activities in a safe and secure manner. "People are buying into the notion that cybersecurity is a community effort," said Singleton. The center reaches across a diverse number of sectors to provide cybersecurity support and foster information sharing among members: participants range from K-12 schools to private corporations and law enforcement.

Singleton added, "OK-ISAC is just one example of how we forge partnerships to benefit all of Oklahoma."

CrowdStrike — the Bleeding Edge of Cybersecurity

A portfolio of CrowdStrike solutions forms an essential part of the Zero Trust cybersecurity strategy to protect 35,000 of the state's total endpoints. CrowdStrike dovetails with a range of other security tools for defense, protection, offense and investigation. "The State of Oklahoma was dealing with increasingly hostile and frequent attacks, especially when we went from office to home-working," said Moore. "When we evaluated different endpoint protection technologies, one of the core differentiators of CrowdStrike was the crowdsourced model, delivering protection to end users quickly, seamlessly and with minimal disruption."

Another key advantage of CrowdStrike is how it supports remote working. "It was important, especially during COVID-19, that we considered the best way to secure the diverse environments of each staff member," said Moore. "A key component of this approach was to make CrowdStrike available for home use."

Over an 18-month period, the state used CrowdStrike in conjunction with other security tools to complete 38 separate cybersecurity initiatives, including new cloud proxy servers, a new VPN and replacing endpoint detection, antivirus and network intrusion systems. "This has put us at the bleeding edge of cybersecurity in terms of our capabilities and technologies," said Singleton. "We deployed a set of solutions that included CrowdStrike to give us the ability to really dig deeply into behaviors and traffic flows to understand exactly what is happening on the network."

As an example, there was an anomaly occurring on a system that held a large amount of citizen data. CrowdStrike fired off an alert to say something unusual had been detected and automatically contained the issue before any harm was done. "This showed how important it is to have tools with deep capabilities, like CrowdStrike, that can effectively stop even the most aggressive attacks," said Singleton. "This is a really big deal for us."

Widespread Enhancements to Security

As part of its community-based security ethos, the state is keen to extend protection to the entire population and is running several statewide communication and social media campaigns to raise awareness. "It is a 'high tide raises all boats' scenario," said Moore. "The more people we can get to understand their role in protecting themselves, their community and the systems that they interact with, the better we are across the board."

The rollout of CrowdStrike was straightforward and provided a template for enterprise-wide cybersecurity deployment, with 111 state agencies now under unified and centralized endpoint control. "We have seen a dramatic improvement in security management," said Singleton. "Efficiency has

RESULTS

Increased security team efficiency by 60%

5-year cost benefits estimated to be $5.7M

Expected ROI of 300%

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Device Control™ cloud-delivered device control
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon Prevent™ next-generation antivirus
- Falcon Prevent™ for Home Use
- CrowdStrike Threat Graph® breach prevention data and analytics

voices

CrowdStrike Customer Case Study

increased by 60% and we expect to see an ROI of almost 300%. With CrowdStrike, we can rapidly identify bad things happening, contain the threat and, in less than a minute, have everything under control and users back at work." Before, the average time to react was two days.

The state estimates that with the efficiency gains and smarter processes, it will realize cost benefits of $5.7 million over five years.

CrowdStrike has been central to community-based security.

"One thing I absolutely love about CrowdStrike is being at the heart of a cybersecurity ecosystem," said Singleton. "As things happen on endpoints or servers anywhere in the world, CrowdStrike is generating its own threat intel and passing that on to other platforms. CrowdStrike is a force multiplier that saves valuable resources."

In addition, Oklahoma gathers threat intelligence and shares it with partners across the state. Coupled with the success of CrowdStrike, the state has ignited interest from multiple organizations, including other government entities, to participate in the OK-ISAC.

High-value CrowdStrike Partnership

One of the critical parts of improving security has been partnerships with industry experts and none more so than CrowdStrike. "CrowdStrike is a critical partner to the state of Oklahoma," said Singleton. "We have enjoyed the CrowdStrike relationship and it continues to get better as our team becomes more familiar with the platform and its capabilities. The value that CrowdStrike provides to the state is growing and we are doing things that we could not even consider before. CrowdStrike is our primary tool for hunting down threats."

Since implementing CrowdStrike, the state's cybersecurity team is uncovering threats that were not previously detected. "We're aware of a lot more threats targeting our environment, but we're now equipped to mitigate those risks," said Singleton.

Singleton concluded by advising those yet to discover the value of endpoint security, "Everyone is aware of cybersecurity challenges. One of the main ways to combat this is an endpoint detection and response solution that is smart enough to spot threats in real time — not one based on dated, incomplete definitions. Having CrowdStrike is the proactive way to help prevent attacks from being successful."