CROWDSTRIKE CASE STUDY

WYOMING DEPARTMENT OF ENTERPRISE TECHNOLOGY SERVICES

STATE OF WYOMING TRUSTS CROWDSTRIKE TO HELP SUPPORT ECONOMIC DEVELOPMENT, PROTECT CITIZENS AND STAFF FROM CYBER THREATS

In January 2011, while early in his first term, Wyoming Gov. Matt Mead prioritized expanding the state's economy to include a high-technology sector. About a year later, the state legislature established the Wyoming Department of Enterprise Technology Services (ETS), to build the infrastructure to support the executive mandate and to provide cybersecurity and IT services to numerous state agencies.

"We built out high speed networks that are second to none in the country," explained State of Wyoming Chief Information Officer Tony Young, who also directs ETS. "Our responsibilities include supporting, maintaining and servicing the executive branch and, on occasion, some judicial and legislative branch offices of state government."

Altogether, ETS watches over about 10,000 end users, along with the hardware, software, network services and systems that span agencies from the Department of Agriculture to the Department of Transportation.

By extension, Young said, the department protects Wyoming's citizens and their data from cybercriminals, malicious hackers, rogue states and activists. "While we don't house a lot of data at (ETS), many of our state agencies do, and we have to protect and preserve all of that data," he said. "Because of that we are always concerned with how we approach cybersecurity."

While aspects of providing cybersecurity to a government entity are similar to doing so for a business — "Our network is no different than any other

Quick Facts:

AGENCY OVERVIEW

The Wyoming Department of Enterprise Technology Services (ETS) is tasked with building the state's infrastructure to support the governor's economic development mandate, while providing cybersecurity and IT services to numerous state agencies.

MISSION

"To establish and refine a coordinated enterprise information services and technology structure, which increases the ability of state agencies to deliver quality, cost-effective services to the citizens of Wyoming."

Website: ets.wyo.gov

The Story:

CHALLENGE

The State of Wyoming Department of Enterprise Technology Services (ETS) was established in January 2012 with a clear and guiding mandate from the governor — to help support economic development and to protect citizens and staff from cyber threats. ETS built a foundational statewide, high-speed network and now watches over about 10,000 end users, services and systems that span numerous state agencies. Like any business, its network is under constant attack; unlike any business, it must safeguard the economy and citizenry of an entire state, all the while complying with many diverse requirements. As a result, ETS requires a cutting-edge cybersecurity solution that can adapt with the evolving threat landscape and provide get-it-right-the-first-time protection and support.

TASK

ETS needed to replace a legacy antivirus solution that was missing detections, impeding the ability of end users to do their jobs, and not providing crucial 24/7 protection. In addition, ETS staff were finding it labor intensive to track network in that it is under constant attack," Young said — there are facets that are unique.

By safeguarding the state's public agencies, ETS is by extension "protecting every citizen in the state of Wyoming," said Senior Security Engineer Jason Strohbehn. "The level of care has to go up accordingly, which means I can't fumble through and work on something for two or three days and hope I get it right. I have to have the tools and I have to have the support to get it right the first time."

The State of Wyoming's network is also very diverse, Strohbehn said. "We have a lot of different compliance requirements, for everything from education and its FERPA requirements to healthcare and its HIPAA requirements," he said. "We have to be able to defend to the proper standard to protect those agencies."

To those ends, ETS staff began looking for a cybersecurity solution to replace its traditional antivirus solution, which was found to be failing in critical areas. "The legacy antivirus solution wasn't cutting it," Strohbehn explained. "We couldn't continue to use old techniques to defend against new attacks. Not to mention we were missing a lot of detections, it was very labor-intensive to go in and fix things, and it was process-heavy."

The legacy solution fell short in it's ability to stop new and emerging cyberattack methods, said ETS IT Administrator Sean Moore. "Malicious hackers are more sophisticated now than they were in the days of single-signature malware," he said. "They're creating malware that can adapt, and we need solutions in place that can adapt with it."

Moore challenged his teams to find a replacement that was both effective and innovative, with the ability to defeat even the most sophisticated attacks targeting the state's systems and citizens. "They came back with a host of different solutions," he said. "But only the CrowdStrike® Falcon® platform really stuck out."

CLOUD-NATIVE ARCHITECTURE: FAST DEPLOYMENT, LIGHTWEIGHT AGENT

CrowdStrike Falcon Platform Lets End Users Work Safely and Without Interruption

Installing the Falcon platform across the department's network was "very simple," according to Tim Walsh, supervisor of the department's security and firewall team. "We didn't get any feedback from any customer saying they had problems," he said.

Once the Falcon platform was installed and running, its lightweight agent and cloud-based engine offered seamless and virtually invisible protection. The differences between Falcon and the state's previous endpoint protection product became readily apparent.

"Our legacy AV could bog down a machine and cause problems, but not CrowdStrike," Walsh explained. "Our end users don't know it's there, even though behind the scenes, there's a lot going on."

Wednesdays at noon was a particularly trying time for Wyoming state employees. That was when ETS scheduled the weekly security scans and signature updates

down and mitigate what attacks the legacy AV was able to alert them to. Finally, the legacy solution was unable to stop new and emerging cyberattack methods.

WHY THE STATE OF WYOMING CHOSE CROWDSTRIKE

Both to maintain its cutting-edge reputation and, most importantly, fulfill its guiding mandate, ETS needed to replace a legacy cybersecurity solution with one that is effective, innovative and able to adapt to sophisticated attacks as they continue to evolve. Further, ETS leadership wanted to find a vendor it could rely upon as a partner in the battle against global cybercrime.

After evaluating several cybersecurity solutions, ETS chose the CrowdStrike® Falcon® platform. Not only was the Falcon platform easily deployed without impacting users, its lightweight agent and cloud-based engine offers seamless and virtually invisible protection every hour of every day. Productivity increased not only for end users who no longer had to endure CPU-intensive scans, but also for ETS staff who can now identify an attack almost instantaneously and mitigate it faster than ever before, thanks to the heightened real-time forensic visibility into processes the Falcon platform provides. Job satisfaction increased as well, with ETS staff able to be more proactive and less reactive and capable of ensuring end users were protected no matter where they were working from. In addition, the ETS team was able to bolster its effectiveness by engaging with the Falcon OverWatch™ managed hunting service, which ETS staffers likened to "having a 24/7 security operations center" without having to hire an entire new team.

required by the legacy AV solution that the Falcon platform replaced. Moore said the process was so arduous that some end users would submit help tickets asking "How do I turn this thing off?"

"At that time, everybody's computer would slow to a crawl," Strohbehn said. "With CrowdStrike, we're not pushing these CPU-intensive scans, and we're also not facing large signature updates. The Falcon platform is the least intrusive solution we found, and, coincidentally, it gives us the very best protection."

NEXT-GEN PROTECTION AGAINST ADVANCED THREATS

CrowdStrike Replaces Legacy Antivirus Solution

The legacy AV solution ETS previously used was also resource-intensive in terms of the time and effort staff spent finding a threat and then performing forensics on it. The Falcon platform has changed that, Moore said. "Using CrowdStrike's tools, we can identify an attack almost instantaneously," he said. "We can then find out which user is affected, where that user is, and then deploy tech people to isolate that machine, clean it, wipe it, re-image it, and return it to the user far, far faster than we've ever been able to do in the past."

Strohbehn praised the heightened real-time forensic visibility into processes the Falcon platform provides. "It lets us get down into the very heart of what's going on during a potential attack," he said. "Rather than just look at a signature and keep it or discard it, we can look and see what an attack is doing and determine if it is even real before we deploy a technician or apply additional resources to it."

Strohbehn is also pleased with CrowdStrike's ability to protect against everything from traditional malware to today's stealthy scripted attacks, as well as the ability to let his team be more proactive and less reactive. By being alerted to threats before they strike, ETS can take preemptive action, rather than getting alerts after events have already occurred. Now ETS can do more than wait until an attack strikes its user's systems, and just "pray that they're okay," he said. "It's been a huge difference for us."

Another big difference the Falcon platform provides, Strohbehn said, is the ability to protect end users wherever they are. "Whether you're at home, whether you're in your office, even if you're overseas, it doesn't matter to us where your state-issued computer is sitting — CrowdStrike is protecting it," he said.

PROACTIVE MANAGED THREAT HUNTING

CrowdStrike Falcon OverWatch™ Team: "Like Having a 24/7 Security Operations Center"

For ETS staff, one of CrowdStrike's most significant selling points was its Falcon OverWatch™ managed hunting service.

The constant presence of the OverWatch team is "like having a 24/7 security operations center," Director Young said. "For us to replicate that would require the hiring of six to ten full-time employees," he explained, noting the practical and fiscal challenges of fielding such a team of highly trained forensic experts.

"The OverWatch team has our back," Strohbehn said. "When we get an after-hours email alert from CrowdStrike, we know something needs our immediate attention." He added that the OverWatch team will "jump right in" and help if something is happening within the state network or with processes that Strohbehn hasn't encountered before.

That level of service has an added benefit, Strohbehn said. "Rather than having three, four or five guys dedicated to one task, it can be me and the OverWatch team dedicated to hunting for a specific threat in the network." Walsh added that having access to the Overwatch service makes his relatively small security team seem bigger, because his team can focus their efforts elsewhere. "Now my security analysts can do the other parts of their job," he said. "They're not just sitting there having to watch and catch things in the network."

"The Overwatch team really gives me comfort as an IT administrator," Moore said. "When I go to bed at night, I know I have the folks at CrowdStrike watching over our network, ready to contact us if something comes up and give our folks the tool set they need."

UNPARALLELED CUSTOMER SERVICE AND PROACTIVE PROTECTION

CrowdStrike Provides "Game-Changing, Hand-In-Glove" Cybersecurity

The Falcon platform not only delivers an advanced level of protection to ETS and the agencies it serves, it has changed the way the organization does business.

"Now we can actually take the time to go hunt through the network proactively, something we never had the ability to do before," Strohbehn said. "We can look for indicators of attack before they become indicators of compromise. It's a much more satisfying job than waiting for the bell to ring and having everybody run out to find out what's wrong."

In other words, Strohbehn said, the visibility the Falcon platform provides empowers the department to do our job to the best of our abilities.

"If we can see it, we can protect against it," he said. "That's where CrowdStrike fits in. It's a hand-in-glove sort of thing."

That "hand-in-glove" aspect gets at what Director Young believes is a strategic partnership between the State of Wyoming and CrowdStrike.

"I consider our vendors now as partners," Young said "That is, should we fail, they fail. Knowing that we have CrowdStrike in this battle with us gives us the strength and the courage and, frankly, the support that is needed to combat cyber threats on a global level, not just isolated as one state."

The partnership also supports what ETS staffers refer to as Director Young's "customer service mantra," which recognizes that if end users are happy with the platforms they're using or happy because they feel protected in the work they're doing, they're going to be happy with ETS.

Combined with the Falcon platform's ability to work in the background seamlessly and around-the-clock, the CrowdStrike solution is "the game-changer for cybersecurity," Moore said.

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The lightweight Falcon agent deploys in minutes to deliver actionable intelligence and real-time protection from Day One. The Falcon platform seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by a 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. The Falcon platform protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack-based (IOA) threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, the Falcon platform instantly correlates more than 70 billion security events from across the globe to immediately prevent and detect threats.

To learn more about how CrowdStrike can help protect your organization, contact us today at sales@crowdstrike.com or visit www.crowdstrike.com/seedemo to request a demo.

CROWDSTRIKE

sales@crowdstrike.com | (888) 512-8906
www.crowdstrike.com