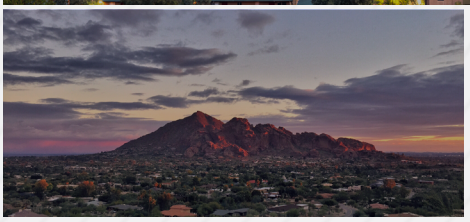
voices

CrowdStrike Customer Case Study



Fifth Largest City in the U.S. Deploys World-Class Endpoint Security and Services to Protect Diverse Infrastructure

When Shannon Lawson, CISO at the City of Phoenix, told senior city managers about the costs associated with ransomware attacks on Atlanta and Baltimore, it was the kickstart they needed to support a comprehensive review of the city's security posture.

The City of Phoenix is the municipal government for Phoenix, the fifth largest city in the U.S. It provides about 1,600,000 citizens with a wide range of public services including water, police, fire and housing, and employs 13,000 staff across diverse and often autonomous operational units.

The city's existing security infrastructure consisted of a mix of individual, mostly on-premises legacy components. "When evaluating the maturity of any new environment, I first look at web, email and password exposures, and especially how endpoints are being protected," shared the CISO. "I needed to determine if we had all the right pieces in place."

Focusing on validating the city's choice of endpoint protection, Lawson carried out a detailed review and comparisons across the endpoint detection and response (EDR) market. "I compared leading offerings with our incumbent endpoint protection product — using criteria that included ease of deployment, scope of supported systems, CPU power consumption, the overhead imposed on the endpoint, and how well both common and previously unseen threats were handled — and decided that we should do more in-depth testing of CrowdStrike," he said.

Choosing CrowdStrike was a No Brainer

Lawson conferred with several other public sector organizations that had deployed CrowdStrike. However, it was not until the city ran a trial that the real power of the CrowdStrike Falcon® platform and Falcon Complete™ managed detection and response (MDR) service became apparent.

Lawson likened his initial experience of evaluating CrowdStrike to the movie Aliens when the crew scans the spaceship and watches, mesmerized, as the alien gets closer and closer. "We set up CrowdStrike to monitor our environment and witnessed the launch of a keyboard attack targeting our externally-facing PeopleSoft servers," explained Lawson. "CrowdStrike immediately detected the threat attempt and before anything malicious could occur, we were able to shut down the servers. The CrowdStrike team then calmly walked us through the resolution process and helped ensure that the servers couldn't be compromised in this way again."

"Bam! Right off the bat, CrowdStrike delivered and then some. Choosing CrowdStrike was a no-brainer for us all," Lawson said. "Everyone was sold."

City of Phoenix

INDUSTRY

Public Sector — State and Local Government

LOCATION/HQ

Phoenix, Arizona

CHALLENGES

- Securing a large, diverse and complex municipal organization
- Facing an industry shortage of security professionals
- Keeping ahead of increasingly sophisticated attacks

SOLUTION

The City of Phoenix has deployed the CrowdStrike Falcon platform to help protect the staff and municipal operations of America's fifth largest city.

"As soon as it was installed, CrowdStrike immediately found crazy stuff taking place on these boxes. The other two products weren't detecting anything. Once we saw that, we knew we'd made the right decision."

Shannon Lawson
CISO
City of Phoenix

voices

CrowdStrike Customer Case Study

Rapid Deployment, Rapid Returns

The city deployed a broad selection of CrowdStrike products, using the Falcon platform to deliver widespread capabilities, including EDR, next-generation antivirus protection, IT hygiene and vulnerability management. To offset the industry-wide shortage of security expertise, especially in the public sector, Lawson implemented CrowdStrike Falcon Complete MDR and purchased a CrowdStrike Incident Response Retainer.

Starting with the pervasive information technology services (ITS) group, CrowdStrike was rolled out across the city's environment and immediately onboarded, in less than 24 hours, by the Falcon Complete team. "We were operational right off the bat," Lawson said. "Some vendors make products that are unnecessarily complicated and need a PhD to understand. Falcon is not one of these. Ramp-up time is minimal for something this sophisticated. It has a very intuitive interface that accelerates analyses and the amount of information it gives us is unreal. Really, it's that good!"

To maintain continuous protection, CrowdStrike was implemented on endpoints prior to the city's legacy security application being uninstalled. In some instances, a third, well-known endpoint security tool also had been running in parallel on the same device. "We had the perfect trifecta on some of these systems to do a meaningful three-way comparison," Lawson said.

"As soon as it was installed, CrowdStrike immediately found crazy stuff taking place on these boxes. The other two products weren't detecting anything. Once we saw that, we knew we'd made the right decision."

Accessing the Full Power of CrowdStrike

Close collaboration and operating as a single team with the Falcon Complete MDR team has been another appealing aspect of the CrowdStrike solution. "CrowdStrike is there for us 24 by 7 by 365 and gives more flexibility for my team to take time off as the company really has our back. It's like having a secondary SOC and indeed, many times functions as our primary operations center for endpoints," said Lawson. Through the city's Falcon Complete contract, Lawson has access to a large pool of highly trained security experts and continuous human threat hunting via Falcon OverWatch™, something that would be impossible for most public or private entities to achieve on their own.

The CrowdStrike Incident Response Retainer also has proven invaluable. "We've had the retainer in place since 2019. When the SolarWinds attack hit in late 2020, the first thing we did was to call the CrowdStrike Incident Response Team. Because we already had the contract in place, they were immediately able to assist in determining if we'd been compromised. Knowing that most of the world's CISOs and CSOs were scrambling to get help from their security vendors, it was just great to get priority treatment," said Lawson.

Another way CrowdStrike helped the city secure itself — and accommodate the sometimes convoluted public procurement processes — was agreeing to a flexible purchasing schedule aligned with the city's budgeting calendar.

RESULTS

Comprehensive protection across complex, distributed attack surface

Immediately operational

Rapid access to team of global security experts

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)
- Falcon Discover™ IT hygiene
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon Overwatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management
- CrowdStrike Incident Response and Proactive Services Retainer

voices

CrowdStrike Customer Case Study

The CrowdStrike solution also demonstrated its merits during the outbreak of COVID-19. "We instantly had people working all over the place, but because CrowdStrike only needs an internet connection to function, we were able to continue operating securely, even in the midst of the pandemic. We couldn't do that with a lot of our other tools," said Lawson.

CrowdStrike: A Great Decision

Lawson noted that some vendors focus too much on the bottom line rather than customer relationships, but not so with CrowdStrike. "I am a CISO for a very large city and have a lot to focus on. But CrowdStrike has been one of those vendors that really is a true partner," he explained.

"We have never been pressured, in any way, to buy additional products or services. The solutions work very well, there is great technical support and expertise, and the company has been with us every step of the way. I have nothing but good things to say!"