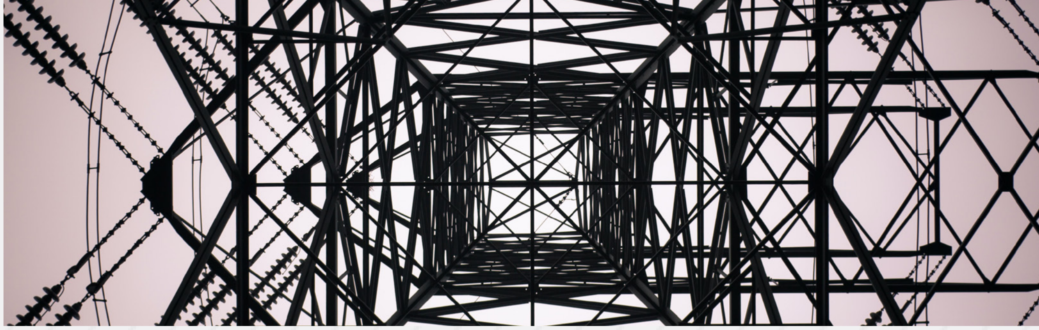
CrowdStrike Customer Case Study



Jemena
bringing energy to life

Australian Utility Provider Partners With CrowdStrike to Transform Cybersecurity Defense and Critical Infrastructure Protection

Australian energy utility Jemena owns and operates a diverse portfolio of energy-related assets, supplying millions of households and businesses with essential gas and electricity services. The company is also spearheading a number of high-profile green energy initiatives — all of which makes it an enticing target for cyberattacks.

Australia is on the cusp of introducing new cybersecurity regulations to ensure the country's critical infrastructure is protected. In response to these upcoming regulations and the growing threat of cyberattacks, Jemena appointed Dave Worthington as CISO to strengthen its security posture.

Lack of Cohesion and Integration Drives Risk

Worthington soon realized that protection in certain areas of the business could be enhanced. Several security products and services had been acquired over time by different business units, resulting in a lack of cohesion and visibility. There was an awareness of security-related incidents, but no clear and timely understanding of exactly what occurred or the level of risk associated.

One of Worthington's first actions was to conduct a red team exercise using ethical hackers to test the scope and resilience of existing security measures. "The red team clearly demonstrated that what we had in place at the time was not fully effective," he said.

The company's security team began looking for a better solution. After an extensive market review, it selected a series of CrowdStrike Falcon® platform solutions. "It was very evident that CrowdStrike was the clear winner out of all the options we evaluated," said Worthington.

Jemena was surprised by the ease and simplicity of deploying CrowdStrike. "Traditionally, we would implement a new product on a small number of clients as the first step in a 6-12-month rollout plan," Worthington said. "But CrowdStrike was deployed to every endpoint in the business in just three days."

Actionable Alerts, Lowered Overhead

INDUSTRY

Utility

LOCATION/HQ

MELBOURNE, AUSTRALIA

CHALLENGES

- Preparing for new cybersecurity regulations in Australia
- Concern over effectiveness of its existing endpoint security solution
- Protecting its AWS cloud and identity attack surfaces

SOLUTION

Jemena uses CrowdStrike Falcon® Complete for 24/7 managed endpoint detection and response, in addition to a host of CrowdStrike Falcon® platform modules to protect cloud and identity attack surfaces.

Another challenge with Jemena's suite of legacy security products was the complexity of the information provided. "It was like drinking from a firehose and having it make little sense," Worthington said. "In comparison, CrowdStrike is simple and easy to use. We don't have to spend a lot of time analyzing the information ... we immediately know what's going on."

Another area where CrowdStrike stands apart, according to Worthington, is the nominal impact of the CrowdStrike sensor on computer performance. Initially, there was resistance within Jemena to using new software because its prior legacy antivirus application bogged down processing. When users were told CrowdStrike would improve rather than impede performance, there was skepticism. However, the ensuing 30% drop in resource consumption won a lot of trust among users.

"CrowdStrike reversed the drain on resources that had previously been a big issue for us," Worthington said. "Being able to implement a better product while simultaneously improving performance is almost unheard of, so it was fantastic to be able to deliver this to our users."

Incident Response Times Slashed from Days to Minutes

Jemena chose CrowdStrike Falcon® Complete, a 24/7 managed detection and response service. The CrowdStrike team immediately detected previously unnoticed vulnerabilities and elevated visibility across the entire infrastructure. Although Jemena has only experienced a few serious threats, CrowdStrike constantly monitors activity to deliver a much deeper and more accurate view than it ever had.

"With CrowdStrike, there is a massive difference in the levels of visibility and clarity we can obtain," Worthington said.

The enhanced protection from CrowdStrike has enabled Jemena to cancel an existing managed security service provider (MSSP) contract, resulting in savings of about 70% annually. Additionally, coverage from the MSSP never approached the continual 24/7 monitoring provided by CrowdStrike. Incident response times have been slashed from days with the MSSP to as few as five minutes with CrowdStrike.

"It could take our MSSP multiple days to identify the presence of a threat, which often had become a big deal by that point. Going to Falcon Complete makes us considerably more effective ... life is significantly easier now," Worthington said.

CrowdStrike is further contributing to cost reductions and improved productivity for the energy provider through the quality of its alerts. Previously, support team members were constantly getting notifications that ultimately turned out to be harmless. That changed with CrowdStrike.

Expanding to the Cloud

Recently, Jemena expanded its CrowdStrike protections to the cloud. The utility is migrating its data center assets to the AWS cloud to benefit from the speed and simplicity. So far, it's migrated nearly 1,000 data center servers to EC2 instances and is already running hundreds of containers, with plans to steadily increase its container footprint.

Worthington emphasized that while Jemena experiments with containers, securing these containerized environments remains a priority.

"On the container side of things, we've got a bunch of different workloads with different needs and platforms — all of which needs to be secured," said Worthington. "Falcon Cloud Security gives us container runtime protection to secure all of it while we feel out where we're going."

Another key reason Jemena chose CrowdStrike for cloud security was because it could continue using the same agent and command console as its existing Falcon platform modules. The integrated Falcon platform

RESULTS

- 70% savings and enhanced capabilities
- Incident response times slashed from days to minutes
- Solution deployed to all endpoints in just three days

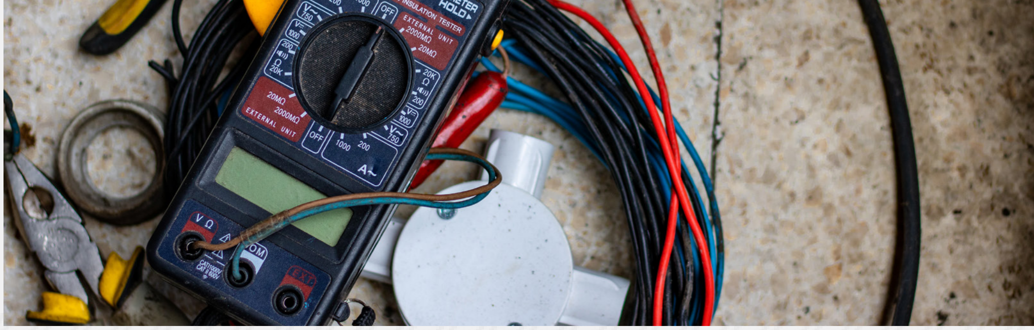
ENDPOINTS

3,800

CROWDSTRIKE PRODUCTS

- CrowdStrike Falcon® Complete managed detection and response (MDR)
- CrowdStrike Falcon® Cloud Security
- CrowdStrike Falcon® Identity Threat Protection identity-based attack detection
- CrowdStrike Falcon® Discover IT hygiene
- CrowdStrike Falcon® Insight XDR endpoint detection and response (EDR)
- CrowdStrike® Falcon OverWatch™ managed threat hunting
- CrowdStrike Falcon® Prevent next-generation antivirus
- CrowdStrike Falcon® Intelligence automated threat intelligence

> "CrowdStrike was deployed to every endpoint in the business in just three days."
>
> **Dave Worthington**
> CISO, Jemena



approach and deployment automation are specifically designed to make it simple and transparent for IT teams to deploy and operate at scale.

“Falcon Cloud Security has made securing our cloud deployments pretty seamless. Most of our teams don’t even know it’s there. It’s just there and it works,” said Worthington.

Focus on Identity

Looking forward, identity protection is a key priority for Worthington and his team. Identity-related attacks are rising sharply, and moving to the cloud heightens the team’s concern. Jemena has successfully used CrowdStrike Falcon® Identity Threat Protection for a number of years and will continue to trust it to defend against identity-related threats.

“A big thing when you move to the cloud is that identity is now one of your key protections. That was a big part of the puzzle we had to solve before moving to the cloud,” concluded Worthington. “Our CrowdStrike identity product hooks in well with Falcon Cloud Security. I have full confidence CrowdStrike will continue to innovate and keep us ahead of adversaries.”

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start Free Trial

Learn more **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches