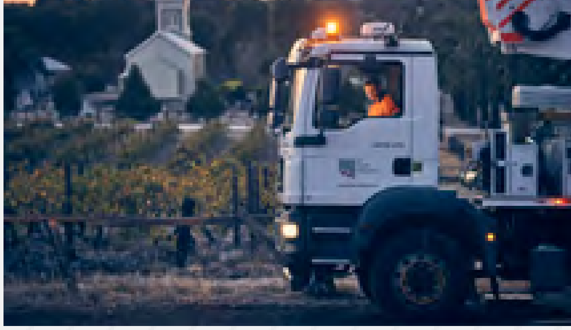
voices

CrowdStrike Customer Case Study



South Australian Utility Expands CrowdStrike Protections to Bolster Defence and Address Cybersecurity Skills Shortage

SA Power Networks is South Australia's sole electricity distributor. The electricity provider was an early adopter of the CrowdStrike Falcon® platform for endpoint detection and response (EDR), replacing a legacy Trend Micro antivirus solution that was not keeping pace with a rapidly evolving threat landscape.

Since then, the escalating threat of malicious cyber activity targeting Australia's critical infrastructure has heightened the risk for SA Power Networks. This has required the organisation to continuingly increase its preparedness, accelerate the adoption of cyber protections and enhance its own cyber resilience.

That's a significant challenge, especially considering the geographic scale of SA Power Networks' coverage area and the additional cybersecurity obligations it's required to meet as a regulated critical infrastructure organisation, explained Nathan Morelli, Head of Cyber Security and IT Resilience at SA Power Networks.

"We have almost a million customers throughout South Australia," Morelli said. "We have to provide network coverage across that entire operation and ensure the infrastructure is available and trustworthy for our teams. In a heightened threat environment, where we know that critical infrastructure is targeted and adversaries are constantly advancing their TTPs (tactics, techniques and procedures), we've got to consistently be better at what we do."

With a small in-house team responsible for cybersecurity, IT resilience and digital identity, SA Power Networks found it difficult to manage its own day-to-day business while keeping on top of advanced threats. The utility also struggled to recruit high-level cybersecurity resources during a significant skill shortage – not just in Australia but worldwide.

"We don't have the unlimited resources or time that the adversary does, and we don't get the rewards that they do. Whereas adversaries work on a model for making money, we've got a cost-based model. So we must have a focused effort, which is all about our threat-informed approach," said Morelli.

Securing a Distributed, Remote Environment

One of the biggest risks for SA Power Networks is its remote users. To help manage that risk, the Falcon platform protects nearly 3,000 laptops, desktops and servers running a mix of Windows, Mac and Unix clients. A key initial benefit for users in the switch from legacy AV was the reduction in CPU usage, which helped endpoints operate more efficiently in the field.

SA Power Networks Empowering South Australia

INDUSTRY

Utility

LOCATION/HQ

Adelaide, Australia

CHALLENGES

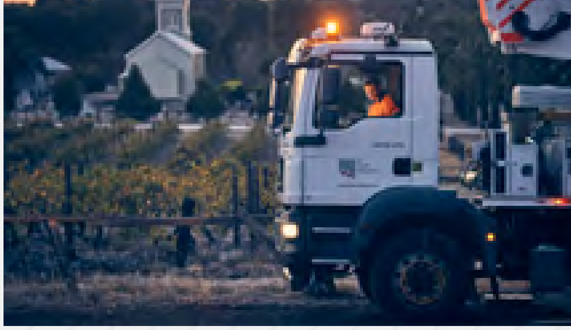
- Cybersecurity skills shortage makes it difficult and expensive to employ staff
- A large number of remote users creates a higher security risk
- Increasing cybersecurity regulations on critical infrastructure need to be met

SOLUTION

SA Power Networks expanded its use of CrowdStrike endpoint detection and response to CrowdStrike Falcon® Complete, thereby getting a fully-managed service from detection to remediation.

> "CrowdStrike understands our organisation and they understand what we're protecting. They have been such a good partner throughout that journey in terms of 'we want more, we want better, we want quicker."

Nathan Morelli
Head of Cyber Security and IT Resilience
SA Power Networks



Since that initial deployment of CrowdStrike EDR, SA Power Networks has found the minimal impact on system resources has enabled SA Power Networks to deploy a greater number of devices to field staff. Before, field devices were shared; now each worker has their own, increasing efficiencies and reducing security risks.

In 2019, SA Power Networks expanded its CrowdStrike usage with Falcon® Complete, a fully managed detection and response service across those devices, encompassing threat intelligence, threat hunting and incident response.

"We now have a partner in CrowdStrike that understands our organisation and what we're protecting. We're comfortable with CrowdStrike doing things that we're not comfortable with other providers doing because we trust them," said Morelli.

CrowdStrike now monitors all endpoints under management, taking action to counter any incoming threats or attacks. This includes isolating, investigating and triaging any suspicious activity to the point of remediation, and advising SA Power Networks on what needs to be fixed so it doesn't happen again.

The ultimate benefit for SA Power Networks is the comfort in knowing the devices under management are secure.

"We simply don't have incidents on our devices protected by CrowdStrike."

The partnership with CrowdStrike enables SA Power Networks to take a proactive approach to securing its environment. The security team runs an ongoing threat and attack simulation program, testing the organisation against its top threats. This way, potential problems can be found ahead of time, security controls can be checked and verified, and any high-risk issues can be addressed.

Development of Cybersecurity Skills and Capabilities

The CrowdStrike managed service has generated significant efficiencies and cost savings for SA Power Networks. "The overnight protection and support our team receives from CrowdStrike, plus knowing that CrowdStrike will respond quicker than anyone else, means we don't need a 24x7 SOC service and we only use overnight on-call for escalations in high-risk situations," said Morelli.

The partnership has also helped develop SA Power Networks' in-house cybersecurity resources and capabilities. With CrowdStrike providing the overall managed service, supported by security analysts and specialists as needed, SA Power Networks has been able to recruit more junior cybersecurity staff.

"Senior cybersecurity specialists are expensive and it's difficult to keep them. Now we can bring in recent graduates and less experienced analysts, and build them up so they understand our business and develop their cybersecurity skills along the way," explained Morelli.

The benefits of this approach are two-fold: while it gives SA Power Networks a lower cost base for its internal team and reduces risk to the organisation if it loses any staff, the focus on internal training and development is improving the overall cybersecurity industry and helping address the current skills shortage.

RESULTS

A proactive approach to cybersecurity

Fewer security staff required

Increased efficiencies by securing more devices in the field

ENDPOINTS

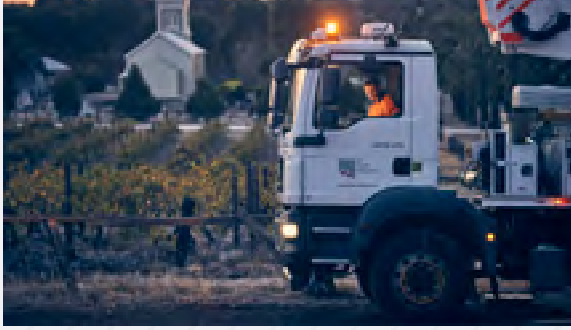
2,970

CROWDSTRIKE PRODUCTS

- Falcon® Complete managed endpoint 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® Cloud Security
- Falcon® Intelligence
- Falcon® Identity Threat Protection

voices

CrowdStrike Customer Case Study



The Power of a Hybrid Operating Model

A recent security incident when most of its security team was on leave brought the relationship with CrowdStrike into focus. Alerted by a notification that access credentials to one of its systems were for sale on the dark web, SA Power Networks invoked its incident response retainer with CrowdStrike. CrowdStrike analysts quickly determined it involved an external customer portal, not administrative credentials or privileged access, so the threat was minimal.

"While the impact was minimal, the advice we received from CrowdStrike drove a bunch of changes in how we manage customer identities," said Morelli.

More broadly, the incident showed the clear benefits of CrowdStrike's service model, which allows SA Power Networks to layer on additional services and integrate third-party products and solutions into its environment. It's also augmented by CrowdStrike's OverWatch threat hunting service. Although AI is a valuable asset in threat hunting, human experts hold indispensable expertise, intuition and adaptability, enabling them to detect even the most sophisticated attacks that deliberately seek to evade traditional security measures.

"The key advantage of CrowdStrike is its critical mass, where they see all the incidents and have the ability to bring in analysts from anywhere and everywhere. That helps them connect the dots and respond effectively"

The incident also accelerated SA Power Networks' deployment of Falcon® Identity Threat Protection, giving the organisation accurate, real-time prevention of identity-based attacks by combining advanced AI and behavioral analytics with policies tailored to cover its higher-risk processes.

"Most incidents start with identity, and CrowdStrike has been very good not just in reducing the impact of compromised credentials, but in identifying the potential risks and understanding the full chain of any identity-based attacks"

Prioritising and Automating Threat Intelligence

SA Power Networks is already using Falcon® Cloud Security to protect its cloud workloads. As they continue to expand their cloud infrastructure, SA Power Networks is investigating CrowdStrike's cloud-native application protection platform (CNAPP) as an end-to-end solution that protects their critical assets in the cloud and at the endpoint. SA Power Networks continues to see the use of cloud security as critical to their ability to serve customers. The utility is also increasing its use of CrowdStrike Falcon Intelligence.

"We are going to prioritise threat intelligence from CrowdStrike," concluded Morelli. "We need to know what's happened where, how we integrate that into our existing control set and how we determine if it's happened here. CrowdStrike will play a critical role in this work."

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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 prioritised observability of vulnerabilities.

June 2023. FR10295.

CROWDSTRIKE

we stop breaches