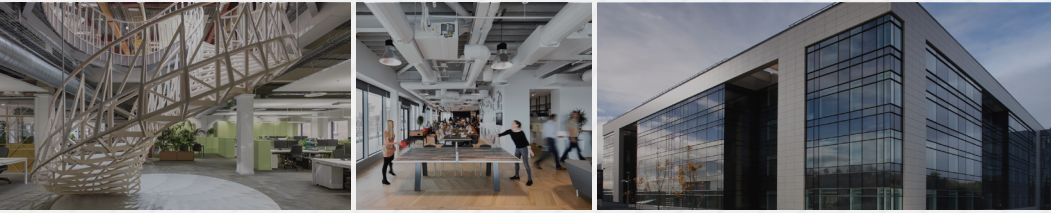




CrowdStrike Customer Case Study



CUNDALL

CrowdStrike Helps Engineering Consultancy Transform Protection and Reduce Time and Cost of Security Management

Gone are the days when Lou Lwin, CIO at engineering consultancy Cundall, worried he might get a cyberattack alert at 2 a.m. on a Saturday. He still might get an alert, but only to let him know CrowdStrike has already spotted and addressed an incident. "CrowdStrike gives me the comfort and satisfaction that active security protection is in place," said Lwin. "It has already dealt with the problem and that is quite a different concept than before."

Using CrowdStrike sets Cundall apart as one of the more advanced organizations in an industry that typically lags behind other sectors in IT and cybersecurity adoption.

Cundall is a global multi-disciplinary engineering and design consultancy offering a range of civil and structural engineering, building services, and specialty services such as acoustics and geotechnology, heating and ventilation. Cundall had already developed a strong security infrastructure with robust perimeter, email and web protection. However, endpoint security was one area that needed improvement. Tools such as antivirus and antimalware were doing an adequate job, but were time and resource heavy, while threats were getting more frequent and sophisticated.

Facing an Ever-Changing and Evolving Threat Landscape

"Back when the 'crown jewels' were being attacked, you had people manually handling detection and response, monitoring logs and providing a degree of protection," said Lwin. "Today, attacks are becoming more sophisticated and if they are machine-based attacks, there is no way an operator can keep up. The threat landscape is ever-changing. So, you need machine-based defenses and a partner that understands security is not 'one and done.' It is evolving all the time."

Cundall is involved in several critical infrastructure projects including airports, data centers, hospitals and financial institutions. "Due to the high-profile nature of our work, we handle a lot of sensitive and confidential information like building designs and plans," Lwin explained. "Consequently, safeguarding information and data protection are critical."

The company has over 1,000 staff worldwide, and many work in the field, which further complicates security management. When Cundall was researching an effective endpoint detection and response (EDR) solution, CrowdStrike was at the top of the list.

"CrowdStrike always does very well according to all the key market analyst groups because it delivers on its promises," Lwin said. "That is a point of great importance and certainly of concern to us. Does

INDUSTRY

Multi-Disciplinary Engineers

LOCATION/HQ

Newcastle, U.K.

CHALLENGES

- Protecting high-profile, sensitive construction projects
- Securing mobile staff globally
- Defending against sophisticated and ever-changing threat landscape

SOLUTION

Cundall, a global multi-disciplinary engineering and design consultancy, is using CrowdStrike Falcon Complete™ to improve endpoint security, enhance its business reputation and make security management more efficient and cost effective

"We were secure before but now with CrowdStrike, we are stopping things early on and getting good visibility into the nature of threats. The key factor is early detection, so we are not having to shut down and clean devices."

Lou Lwin
CIO
Cundall



CrowdStrike Customer Case Study



the solution actually work and deliver the protection you need? CrowdStrike is actively involved in — and very good at developing and changing — its counter measures to meet the threats.”

Other factors that drove the decision to select CrowdStrike were reputation, credibility and the fact that CrowdStrike can defeat high-profile cybersecurity incidents.

1,000 Endpoints Protected in One Week

Cundall uses CrowdStrike Falcon Complete™, a managed service that includes the experts, processes and technology needed to handle endpoint security. CrowdStrike has been deployed across the whole organization protecting over 1,000 endpoints, most of which are laptops. A portal enables Lwin and his team to get accurate and real-time reports on EDR performance. CrowdStrike reporting has been folded into the company’s security information and event management (SIEM) solution as a complementary toolset to other solutions. This enables Cundall to compare, track and monitor behavior and patterns that emerge across the IT environment.

The flexibility of Falcon Complete enabled the CrowdStrike solution to fit well within Cundall’s existing security infrastructure without much overlap. It also was extremely easy and quick to deploy, which was essential because of Cundall’s small IT team. (The company outsources its security operations center to another service provider.) “With CrowdStrike, rolling out sensors to endpoints was done almost without effort and only took a week,” said Lwin. “Once in place, any updates are pretty much transparent.”

Because the CrowdStrike solution places minimal overhead on devices, few end users have complained about laptops running slowly because of power-hungry background scanning. Cundall is growing and CrowdStrike’s ease-of-use and scalability makes it seamless to extend protection to new endpoints. “One of the wonderful differences about CrowdStrike is that end users simply do not know that the product is running on their devices and protecting them,” said Lwin. “I can remember when antivirus software could swamp a PC for hours and even crash it. Now, the overhead for users is nonexistent.”

Cundall is starting to move more services from its hybrid IT environment to the cloud. The company uses Microsoft software applications along with many design and engineering programs for special processes such as computational fluid dynamics, acoustics and sustainability analysis.

The deployment of CrowdStrike has brought several improvements to Cundall’s security management and protection, and CrowdStrike now forms a critical part of the company’s overall cyber defense. “Security absolutely has improved at Cundall because of CrowdStrike,” Lwin said. “We were secure before but now with CrowdStrike, we are stopping things early on and getting good visibility into the nature of threats. The key factor is early detection, so we are not having to shut down and clean devices.”

CrowdStrike: The EDR game changer

Cundall has also realized significant savings in managing its security since deploying CrowdStrike. “Using CrowdStrike to save time and money has been a game changer for Cundall,” said Lwin. “I have built up security teams in the past that were people-heavy. However, automated tools like CrowdStrike mean we no longer need people manually sifting through logs.”

RESULTS



Reduces security management time and cost



Enhances business reputation



Targets resources more accurately and cost-effectively

ENDPOINTS



CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)
- Falcon Discover™ IT hygiene
- Falcon Device Control™
- Falcon Firewall Management™
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management
- Falcon Intelligence automated threat intelligence



CrowdStrike Customer Case Study



One of the key advantages of CrowdStrike is the service and breadth of knowledge and experience that comes with its toolset. “It is not just having the CrowdStrike solution; it is everything behind the solution,” said Lwin. “This gives us the confidence that we have a whole army of resources protecting our business and our clients. CrowdStrike watches the global security landscape — not just one company — and gathers data from millions of endpoints to bring great insight to managing our overall security.”

Access to the CrowdStrike ecosystem and threat intelligence is another benefit for Cundall. The company is starting to use this and data from its own business to build a detailed and accurate picture of the company’s security environment. This enables Lwin to identify where security must be improved so resources can be targeted more accurately and cost effectively than before.

“Having the CrowdStrike Falcon Complete managed service wrapped around the CrowdStrike security ecosystem makes all the difference in the world,” Lwin said. “It is not just thrown over the fence to us. CrowdStrike helped set up and configure the solution and now maintains it.”

Apart from boosting Cundall’s security posture, CrowdStrike has also enhanced the company’s business reputation. “Our ambition is to be an organization that is very security conscious and puts it at the forefront of everything we do,” said Lwin. “CrowdStrike adds to our credibility and demonstrates how seriously we take security as something essential to protecting our organization and our clients’ interests. People see that and recognize that we are serious about our security stance. This increases repeat business and enhances confidence in new clients to work with Cundall.”

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 prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

© 2022 CrowdStrike, Inc. All rights reserved.