voices

CrowdStrike Customer Case Study

European Construction Supplier Repels Ransomware, Rebuilds Security Defenses

SIG, a leading European building solutions provider, had just started to deploy CrowdStrike across its France-based business, when in the early hours of a Friday morning a GandCrab ransomware attack struck over 600 devices. The company was forced to shut down its entire French operation, a part of the business that accounts for almost 30% of total revenues. Thankfully, two devices were protected because they had CrowdStrike installed, and this was key to ultimately defeating the attack.

SIG is a publicly traded supplier of specialist building products and solutions to commercial customers across the UK, France, Germany, Ireland, Poland and Benelux, and has 6,500 employees spread across 425 locations.

Several months before the ransomware incident, the SIG security team had begun an evaluation to determine if its existing cybersecurity culture and infrastructure were still appropriate to protect against the growing threat of attacks, especially for end users, which were seen as primary targets.

At the time, the company had multiple endpoint antivirus products in place. Carl Baron, CISO of SIG, said, "You name it, there was a strong possibility that we had it deployed." But many were proving to not be fully effective due to unnecessary administration challenges or efficacy of the product.

Toughening Up Endpoint Security

The evaluation resulted in a decision to reinforce the company's cybersecurity strategy, with a focus on endpoint protection. Initially, Baron's team considered improving endpoint security using its security operations center (SOC) but discounted this because of limited IT resources and adhering to a recent strategy to build strong vendor partnerships.

As the business has a lean IT organization — regional teams supported by a lean, centralized IT function — partnerships are seen as an essential component of the overall security posture. It is critical that any partner should be capable of augmenting the internal team at both group and local levels.

To choose an endpoint security vendor, the SIG team evaluated independent consultants' reports and recommendations, including research by Gartner and Forrester. The field was narrowed to three contenders, with CrowdStrike already informally earmarked as the favored choice. "We rejected two players because of their lack of response capability and limited breadth of security features, but specifically the immaturity of their services," said Baron. "In contrast, we chose CrowdStrike because of its proven managed service capability, its reputation and the quality of its response during the tender process."

INDUSTRY

Construction

LOCATION/HQ

Sheffield, UK

CHALLENGES

- Growing threat of attack and endpoint vulnerability
- Mix and match of variable quality antivirus systems
- Lean IT team and limited regional resources

SOLUTION

SIG, a leading supplier of building and construction products, has deployed CrowdStrike Falcon Complete™ managed detection and response (MDR) to protect thousands of dispersed endpoints in 425 locations across multiple European countries.

"We are a committed Falcon Complete customer but have benefited from our partnership with CrowdStrike far beyond the technology."

Carl Baron
CISO
SIG plc

voices

CrowdStrike Customer Case Study

Technology and product quality were part of the decision but the portfolio of additional capabilities that CrowdStrike offered — including Falcon Overwatch™ managed threat hunting, Falcon Discover™ IT hygiene and Falcon Device Control™ — proved to be key factors in the final selection.

CrowdStrike — a Critical Security Component

SIG selected CrowdStrike Falcon Complete™ managed detection and response (MDR) and first deployed it across the UK. The UK implementation was completed on schedule, but for a number of disparate reasons, the rollout to other countries was slower. "CrowdStrike is a critical component of our security posture, so we wanted to get it deployed and protecting us as quickly as we could," said Baron.

In France, CrowdStrike endpoint agents had only just been installed on a couple of devices when the organization was hit by the ransomware attack, resulting in over 600 of the country's systems being compromised.

"The two CrowdStrike-protected devices were key," said Baron. "They remained secure, detected the attack and alerted us to the situation. This enabled us to take action to prevent the ransomware from spreading more broadly."

Swiftly, SIG mobilized its global IT team and partners. Although Falcon Complete had already been purchased, the selection of additional CrowdStrike services was still being finalized. Nevertheless, CrowdStrike was contacted and immediately started helping SIG by triaging the incident and providing vital information on the GandCrab ransomware variant.

The SIG IT team set about rebuilding key infrastructure components — such as Microsoft Active Directory using Group Policy Objects (GPOs) and reimaging devices across branch locations in France — to return to normal business operations.

"The event enabled us to demonstrate to the rest of the business that we now had the ability to detect such a threat," said Baron. "It also highlighted the reason we were putting CrowdStrike at the forefront of our incident response plan. CrowdStrike had shown — in a very real-life situation, in a very tangible way — its ability to accurately identify attacks and stop them from spreading."

CrowdStrike Performs "an Amazing Feat"

The French ransomware incident was the catalyst to quickly complete deployment of CrowdStrike. However, an obscure in-house infrastructure issue stopped many of the country's systems from successfully receiving the necessary CrowdStrike Falcon® agent.

To resolve the situation, one of the company's IT team suggested testing just how good CrowdStrike is by getting it to resolve the issue. "Within 30 minutes, CrowdStrike had 450 of the 600 devices up and running and protected!" said Baron. "This was an amazing feat given that we had just spent 24 hours trying and failing to fix the problem."

RESULTS

Received critical incident support despite no formal agreement in place at the time

Two CrowdStrike-protected devices provided insights needed to secure 600 infected systems

Achieved an "amazing feat" securing 450 vulnerable endpoint devices in just 30 minutes

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)
- CrowdStrike Compromise Assessment
- CrowdStrike Incident Response (IR) detect, contain and recover

voices

CrowdStrike Customer Case Study

The ransomware attack in France reinforced the value of CrowdStrike and very quickly Falcon Complete was protecting every endpoint in the company. The threat also prompted SIG to utilize the CrowdStrike Services Compromise Assessment capability to investigate the "why, how and impact" of the GandCrab attack and to ensure measures were put in place to prevent the recurrence of any similar threats.

SIG also has signed up for the CrowdStrike® Incident Response (IR) Service. With the inherent flexibility of the contract, unused IR time can be applied to other CrowdStrike deliverables. These include a group-wide IR plan, developing ransomware playbooks to define process workflows, and creation of standard operating procedures when confronting an attack.

Exercises have been conducted to measure the effectiveness of the IR plan and ensure there is a good understanding across the business about risks and threats and how to deal with them. Data from CrowdStrike Falcon sensors is being integrated with its ServiceNow platform to improve IT resource management and create a vulnerability program and security scorecards.

"We are a committed Falcon Complete customer but have benefited from our partnership with CrowdStrike far beyond the technology," said Baron. "There has never been a point where we have asked CrowdStrike for something that it cannot do. CrowdStrike is a strong ally to SIG and a true extension to our team. Life would not be the same without the partnership."

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches