Secureworks®

Bristow & Sutor Evolves Security Maturity with Managed Detection and Response

Debt resolution company gains rapid access to security expertise with Secureworks Taegis.

Challenge

The evolution of Bristow & Sutor's overall security strategy has been an ongoing process. Chief Technology Officer Paul Lillico arrived at the company in 2018, and his first step was to implement a defensive security approach he summarized as "effectively making the walls as tall as possible." The goal was to prevent as many threats as possible.

As the company's security strategy evolved, Bristow & Sutor designed its approach with the assumption that a threat actor could penetrate its defenses. The company could no longer rely on just stopping threats at the perimeter.

"That shift in approach forced us to strengthen our playbooks" Lillico said. "That to me was a transition we needed. We needed more data, we needed the ability to monitor telemetry 24/7, and we needed additional skill sets to support us in the event of an attack."

BRISTOW & SUTOR

Name: Bristow & Sutor

Industry: Debt Resolution

Country: England

Employees: 500+

CHALLENGES

- Need for a proactive approach to cybersecurity
- Desire for better visibility and access to more data
- Team lacked capacity to fully perform investigation and response

SOLUTION

Bristow & Sutor selected MDR from Secureworks to take advantage of:

- Managed threat detection and response available 24/7
- Immediate access and support from security experts
- Visibility into the threat landscape and intelligence

BENEFITS

- Improved security maturity, lowering organizational risk
- More holistic detection, investigation and response to avoid costs related to breach
- Extending capabilities of a small internal team with low TCO

Solution

Secureworks managed detection and response (MDR) solution, Taegis™ ManagedXDR, delivers superior detection and unmatched response via the open and transparent Taegis security platform. Taegis continuously gathers and interprets telemetry from proprietary and third-party sources throughout a customer's environment, including endpoint, network, cloud, identity, OT, email, and business applications.

MDR from Secureworks offered Bristow & Sutor team the 24/7 threat monitoring they needed to avoid costs related to a breach. In addition to providing them a security operations center (SOC), Secureworks also gave the team the ability to engage SOC analysts within 90 seconds, access to full-service incident response capabilities, one year of raw telemetry storage, impactful threat intelligence, and proactive monthly threat hunting. Taegis is a transparent platform: SOC analysts and customers share the same interface for collaboration, and customers can see all actions taken by Secureworks. Having expert security resources in the SOC available around the clock was a big differentiator for Bristow & Sutor during their decision-making process.

"We chose Secureworks because of their SOC," said Head of ICT Ian Lusardi. "The most attractive thing was having access to a much larger team."

Added Systems Administrator Rhys Bartley: "It feels like you have a much bigger team. You have access to a 24/7 SOC, and it's like messaging a colleague on your own team. It's really valuable."

Benefits

Having Secureworks operate as Bristow & Sutor's 24/7 SOC filled a critical gap in the organization's overall security strategy. The team can instantly tap into vast security expertise instead of trying to hire, train, and retain a large team of internal resources, saving significant costs relative to building their own team. Secureworks surrounds MDR customers with a variety of security experts that go beyond the security operations team in the SOC, including experienced threat hunters who perform monthly threat hunts, threat researchers who provide deep insights into the threat landscape, incident responders to help with readiness and emergency response, and support from a Customer Success Manager and a Threat Engagement Manager.

> **We get access to a plethora of expertise, and that makes a big difference as it helps raise our own expertise and improve our cyber defense program.**

Paul Lillico,
Chief Technology Officer,
Bristow & Sutor

"That extending of our team is really important for us," Lillico said. "We're doing more with less, being smarter, and those are big strategic goals of ours. We'd probably need a team of 50 people to analyze the traffic in our environment. We are an ambitious, fast growing business and partnering with Secureworks was really about accessing expertise and capacity, to meet the needs of our clients. Secureworks provides a strong security offering that has reduced our risk, at a cost significantly less than building on our own."

The Taegis platform contains a wealth of information the Bristow & Sutor team finds valuable, from threat landscape analysis from Secureworks Counter Threat Unit™ research team to the level of detail included in threat investigations and threat hunting findings. Taegis contains 700,000 curated threat indicators, 2,000 curated countermeasures, and dozens of advanced detectors to deliver superior threat detection, prioritizing those that present the most real threats.

"The threat research that Secureworks offers is highly valuable to us," Bartley said. "We have calls with the Secureworks threat hunter, and they share how threat intelligence is used in investigations and how we can better use that information in our own internal operations."

Bristow & Sutor sought a solution that could help their security program evolve, one that would provide a powerful combination of advanced analytics and human intelligence to keep the company ahead of cyber threats. The Secureworks MDR solution delivers a level of monitoring and expertise that Lillico said has significantly helped reduce the risk of cyberattack at his organization.

"It's the fact that Secureworks helps our team," Lillico said. "We connect and learn from a wide array of security experts. The SOC analysts investigating events. The quarterly security posture reviews with the Threat Engagement Manager are good quality. We have constant opportunity to address security concerns. I don't think I could have ever said that about our other cybersecurity providers. We get access to a plethora of expertise, and that makes a big difference as it helps raise our own expertise and improve our cyber defense program."

> **"It feels like you have a much bigger team. You have access to a 24/7 SOC, and it's like messaging a colleague on your own team. It's really valuable.**
>
> **Rhys Bartley,**
> Systems Administrator, Bristow & Sutor

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com