Morgan Sindall Uses AI Protection to Guard Against a Range of Threats

The Challenge: Protecting a Complex Value Chain

Construction and infrastructure group Morgan Sindall is constantly creating new ways to provide the best experience for their customers. With over £3bn in revenues, its collected businesses offer engineering and building services in projects geared towards UK demand for affordable housing, investment in infrastructure & construction, and the revival of inner-city areas.

Morgan Sindall's work on critical national infrastructure projects can involve sensitive data. Its constant quest to innovate for its customers also creates valuable intellectual property. It has a responsibility to keep this information safe.

It must do this while exchanging data with its subcontractors. "The engineering and construction industry is highly collaborative," explains Neil Binnie, the group's head of information security and compliance.

"There's a lot more information-sharing than you might find in other industries," he added. Binnie works with a team of internal professionals to protect the group's eight companies from cyber attacks.

Though every company-to-company data exchange interface is a potential attack vector for credential theft and malware implantation, Morgan Sindall's team must keep the data flowing while simultaneously minimising the attack surface, ensuring that any attack is spotted early and automatically remediated.

CHALLENGES

+ Legacy AV, on-prem management could not support a new remote workforce
+ The modern threat landscape overwhelmed older, legacy technology
+ Support of users independent of location was needed
+ Quick implementation to support a fast-moving business was key

Looking for a Smart Solution

Morgan Sindall's previous endpoint security used to have acceptable performance, but the security team began to see a decline in its effectiveness as the adversaries upped the sophistication of their tactics. Its legacy signature-based detection mechanisms were outstripped by a world that has moved on to far more nuanced attacks. Signature-centric products are also more difficult to keep up-to-date. The security team needed a smarter product that could spot emerging threats and suspicious behaviours while keeping system overhead and team effort to reasonable levels through AI and automation.

Binnie and his team needed visibility across multiple operating system platforms and versions to support the group's mixture of Windows and Linux machines. It also needed the

tool to watch for threats arriving via different channels, such as USB, Wi-Fi, and Bluetooth.

The company envisioned a solution where more happened in the cloud to support an increasingly mobile workforce. To support that, it wanted a cloud-based security solution that would help it adapt to a changing business environment.

"With the group moving towards a cloud-based strategy, it also made sense to move towards a cloud-based protection capability," Binnie recalls, adding that he couldn't wait too long to deploy a solution. "As a new guy coming in, I needed to move with speed. So having a 12-month deployment schedule was not going to work for me."

Fast Deployment Was Key

Fast deployment for the group's 6,600 users was, therefore, a key factor. Morgan Sindall took advantage of SentinelOne University's professional training courses so that the team could quickly become proficient in SentinelOne's simple, web-based interface.

"Our team finds the UI to be intuitive, clean, easy to access, and responsive," he says. "They're finding it very easy to understand what types of threats are happening in real time and how SentinelOne's automated responses are neutralising them."

Binnie and his team also enjoy a close dialogue with the SentinelOne team which gives them a sense of involvement in the product's future. "We've had really good support and access into engineering, and visibility of the product roadmap," he explains.

Since implementing SentinelOne's products, the group now enjoys greater peace of mind during out-of-hours periods of the day. Because the SentinelOne technology uses artificial intelligence (AI) to analyse software behaviour, it can adapt to changing threat conditions and, unlike their former legacy AV product, does not need daily updates.

Flexible Security in the Cloud

SentinelOne drastically reduces the amount of required maintenance while still maintaining high levels of effectiveness. This, combined with cloud-based operations, provided the group with maximum flexibility during the COVID-19 pandemic, Binnie added.

"With everybody home and not working from the office, SentinelOne gave us the confidence that our staff could continue to work safely and securely, regardless of their location," he says.

SentinelOne's end-to-end EDR capabilities also offer deep visibility into endpoint operations, enabling the security team to examine detailed events on a per-device basis. Furthermore, SentinelOne automatically connects the dots on all of these events using patented Storyline™ technology. This saves the group's security staff from tedious, error-prone attack reconstruction activities, freeing up valuable time for higher level thinking activities.

SentinelOne underpins what Binnie describes as a people-centric security strategy in which employees become partners in protecting against cybersecurity threats. "You can't put people-centric security in place without a really great technology baseline," he concludes.

SentinelOne's platform will provide even greater protection for Morgan Sindall as it implements the Singularity® Ranger network visibility and control component later this year. Ranger is a component of the same single agent, single console architecture and provides visibility to every device type, including potentially risky IoT devices. Ranger provides insight

SOLUTION

+ SentinelOne Complete Licenses for Endpoint Protection, Detection and Response
+ SentinelOne Ranger for network visibility, unknown device discovery, and control over suspicious devices
+ SentinelOne Training Credits to ensure maximum utilisation and efficient use

BENEFITS

+ Protection that autonomously identifies emerging threats with AI rather than relying on known signatures
+ Enterprise-grade EDR that's both comprehensive and easier to use, making it accessible to more novice analysts
+ Quality administrator training with SentinelOne University, reducing the time to administrator productivity
+ Cloud-based protection that enables the team to support employees wherever they are

into what's communicating with what, and the facility to isolate suspicious devices and provide a direct, 1-click protective response even if that network is in some remote part of the world.

SentinelOne's 5,500+ customers have invested in its platform because they see how modern endpoint security can be simultaneously easier to manage and have more consolidated features that lower overall risk. Customers also appreciate SentinelOne's focus on the customer experience because the partnership is important to both parties. As it continues to innovate across its construction and engineering ecosystem, Morgan Sindall can be sure that SentinelOne has its back.

> "Our team finds the UI to be intuitive, clean, easy to access, and responsive. They're finding it very easy to understand what types of threats are happening in real time and how SentinelOne's automated responses are neutralising them.
>
> **Neil Binnie**
> HEAD OF INFORMATION SECURITY AND COMPLIANCE

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?