Sandfield strengthens IT security and automates monitoring with LogRhythm

The organisation

Established in 1989, Sandfield has grown to become a leading provider of software applications for operational businesses looking to differentiate themselves through the use of technology.

The company's services and product portfolio includes software and website development, application delivery, database administration, mobile app development, and integration services. Sandfield supports clients throughout New Zealand and around the world.

The challenge

As it has grown during the past few years, Sandfield has increasingly been taking on larger and more complex client projects. This has required an expansion of the company's cloud operations and an increase in processing and storage capacities.

Justin Knight, Head of IT Operations at Sandfield, said this growth had also led to the need for increased IT security measures to ensure client applications and data were fully protected from external threats. At the same time, the organisation benchmarked its protocols against an international standard to ensure their capabilities would be protected.

"About 18 months ago, we achieved our ISO ISO27001 certification," he said. "As a part of that, and to ensure we had all the required controls in place, we realised we needed better insight into and management of our security measures."

Initially, the company's IT team assessed whether this could be achieved using internal staffing and resources. However, it quickly became apparent that this would not be the most effective approach.

sandfield
Get an edge

ORGANIZATION
Sandfield

INDUSTRY
IT

COMPANY SIZE
110+

KEY IMPACTS

- Achieved higher visibility of all security logs and events
- Improved proposition for application delivery solutions
- In a recent month, distilled 191 million logs ingested into 37 alarms for manual investigation or remediation

The solution

After examining a range of alternatives in the IT security space, a decision was taken to engage the services of New Zealand managed services provider Advantage.

Advantage assessed Sandfield's specific requirements and recommended that the LogRhythm-based Security Information and Event Management (SIEM) platform be deployed. The project began in early 2021 with a proof-of-concept (PoC) before rolling it out to cover all critical systems.

"The first step for us was to enable LogRhythm to capture all our Windows and firewall logs," said Knight. "Since then, we have added logs from our AWS and Azure cloud environments as well as Google Workspaces."

Knight said the fact that Advantage already had a comprehensive knowledge of LogRhythm was invaluable as it allowed the new security framework to be up and running very quickly. "By using their team of experts, it meant our internal IT team did not have to fully understand the complexities of the platform before we could put it into action," he said.

Advantage also worked to include a stream of New Zealand-specific security data into the system, including Malware Free Networks from the New Zealand Government Security Bureau, to further improve protection. This data helps to identify localised threats that may have already been flagged by other organisations.

The benefits

With the LogRhythm SIEM platform now fully functional and receiving logs from a range of core systems, Knight said the biggest benefit has been "peace of mind".

Knight said the level and extent of protection enjoyed by the company would simply not have been possible to achieve without LogRhythm. As an example, in a recent month there were more than 191 million logs ingested by LogRhythm, of which 3.5 million were forwarded to a second stage for closer analysis by artificial intelligence tools.

"This then led to 67 alarms being triggered, of which just 37 needed to be investigated by the Advantage security operations team," he said. "That is an example of how effective LogRhythm is as spotting potential threats amid very large volumes of alerts. There would be no way to do that manually."

Knight said the LogRhythm infrastructure has already proven to be invaluable as it recently spotted a misconfiguration that could have led to issues if not rectified in a timely manner.

"We were then able to rectify that misconfiguration immediately whereas, prior to LogRhythm, it may have been days or even weeks before it was spotted," he said. "We are now much more comfortable that we have the level of visibility we require to ensure our systems and resources are secure at all times."

Steve Smith, Auckland Regional Manager, Advantage NZ, said the strong working relationship that now exists between the two companies would help to ensure the current high levels of security protection would be maintained.

"[With LogRhythm,] we are now much more comfortable that we have the level of visibility we require to ensure our systems and resources are secure at all times. We can be confident that any misconfigurations, breaches, or unauthorised access of our systems will be quickly picked up. "

Justin Knight, Head of IT Operations at Sandfield

"We now have a solid understanding of Sandfield's requirements and look forward to supporting them as a team with the winning combination of LogRhythm's technology and expert skills as they continue to grow in the future."

Steve Smith, Auckland Regional Manager, Advantage

About Sandfield

Sandfield delivers custom software solutions that give clients an edge. We love to partner with ambitious companies who want to get that competitive edge and find innovative ways to stand out from the crowd.

We build software on proven frameworks that we have already developed, to provide out-of-the-box certainty with all of the benefits of a custom-built system. You'll gain a competitive edge because your software will do exactly the job you need it to do today, with flexible foundations to adapt cost-effectively for tomorrow.

Sandfield's expertise spans several technologies and industries with dedicated offerings in supply hain, integration, financial management and custom software development.

About Advantage

Advantage has been around for a while; over 36 years in fact. We started out building hardware for the local New Zealand market back in the early eighties. Once the big brands moved in, we pivoted into hosted services, building a state-of-the-art Tier 3 datacentre providing cloud services and disaster recovery infrastructure.

As the landscape continued to change, and our customer base grew, there was a natural progression into the security space. Most of our customers were in the financial, legal, and medical industries where regulatory requirements necessitated a focus on protecting data and systems.

Our business has continued to evolve and today we provide Security Services that are fully supported by our 24x7 Security Operations Centre (SOC).

We have offices in Auckland, Palmerston North and Wellington, servicing customers throughout New Zealand and the Pacific region. Our customers are the focus of everything we do. We want to understand your business needs and through a partnership approach, tailor bespoke solutions to suit your requirements. We have a full suite of highly regarded security solutions available, that are backed up and supported by our highly experienced Advantage Team.

About LogRhythm

LogRhythm helps busy and lean security operations teams save the day — day after day. There's a lot riding on the shoulders of security professionals — the reputation and success of their company, the safety of citizens and organisations across the globe, the security of critical resources — the weight of protecting the world.

Together, LogRhythm and our customers are ready to defend. Learn more at logrhythm.com.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an everchanging threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.