Case Study

FIJI NATIONAL UNIVERSITY

Thanks to COVID, the shift to remote work and learning has been vastly accelerated. But as workers and students move beyond the protection of hardened IT networks, they walk among hidden dangers, their computer devices presenting a softer target to cybercriminals intent on tiptoeing undetected into IT networks.

Tiko Domonakibau, Director of ICT at Fiji National University (FNU), worried about the university's security posture. Aware of the industry arms race that high profile (and often thinly resourced) organisations like his were forced to enter, he hatched a plan to repel more frequent and highly coordinated attacks in a race the university couldn't afford to lose.

Client: Fiji National University (FNU)

Industry: Tertiary education

Environment: 10,000+ user network with blend of networked and DIY devices

Chillisoft solution: SOC-aaS delivered by Advantage; powered by Chillisoft's best-of-breed cybersecurity technology 'stack', including vendors LogRhythm, ESET, Radware, Cofense, Tripwire, and Forcepoint. Supported by VT Solutions

Highlights: Zero-trust security posture; 'need to know' alerts and remediation ease the load on FNU's small security team; end-to-end visibility supporting real-time threat detection and remediation

While email and firewall protection secured the university's IT network entry and exit points, Domonakibau moved to step up network defences, using synchronised best-of-breed solutions to put a single window on threats, incidents, and how they were triaged. And rather than wrestling security applications and monitoring required to do the job themselves, FNU opted for a SOC service or, in the vernacular, SOC-aaS.

Enter Chillisoft and FNU IT partner VT Solutions

Reviewing FNU's cybersecurity posture, Chillisoft and Fiji-based IT provider VT Solutions identified risks attached to manual updates and patching demanded by FNU's point solutions. While the situation could be improved, the fallibility of manual intervention fuelled the broader ambition for a more cohesive approach to security management.

CHILLISOFT | Advantage TAILORED TECHNOLOGY SOLUTIONS | VT Solutions www.vt-solutions.com

Case Study

FIJI NATIONAL UNIVERSITY

Chillisoft's security assessment formed the basis of a tender, which was contested by 10 submitters – and eventually awarded to Chillisoft, with partner VT Solution, and Advantage – a New Zealand-based security specialist and provider of SOC-aaS.

"A compromised endpoint very quickly becomes a compromised network and domain," Domonakibau said. "Speed of remediation is critical, which is why a SOC service is so important. We can't have eyes everywhere – we simply need experts to detect problems and show us what needs to be done."

More protection, less technology – why smart organisations are switching to security-aaS

Shailesh Sharma, founder and owner of corporate ICT provider VT Solutions – a long time provider of services to FNU and, for this project, the team charged with delivering and installing the physical components of the new solution – said best-of-breed technology was an inescapable feature of effective cybersecurity. "But clients shouldn't have to wrestle all the moving parts," he said. "The university didn't want products, because they invite a host of complexity and additional responsibilities small security teams simply aren't up to managing. SOC-aaS was the only viable alternative." he said.

A services-based model also prevents security from becoming unwieldly. "With core security technology and Advantage's expert tracking and diagnosis remaining behind the 'curtain', FNU simply acts on supplied information to direct its team to make the correct fixes," Brad Pearpoint, Managing Director of Advantage, said. "We simply find the issues that FNU should focus on and do that 24/7/365. It's less noise for FNU and plays into the hands of a specialist provider with the horsepower to provide this type of vigilance at scale."

CHILLISOFT | Advantage TAILORED TECHNOLOGY SOLUTIONS | VT Solutions www.vt-solutions.com

Case Study

FIJI NATIONAL UNIVERSITY

Chillisoft's security technology stack protecting FNU

Advantage is an independent company using a diverse portfolio of security software. The following vendors, distributed and supported by Chillisoft, are the engine room for the SOC-aaS supporting FNU.

- LogRhythm - NextGen SIEM/SOAR
- ESET - Endpoint Detection & Response (EDR/EPP)
- Radware - Load balancers and Web Application Firewall
- Cofense - Simulated phishing and security awareness training
- Tripwire IP360 - Vulnerability Management
- Forcepoint - Next Generation Firewalls

Zero trust pays

A 'zero trust' IT environment means that no one is trusted by default from inside or outside the network, requiring users to be authenticated, authorised, and continuously validated before they can access applications and data. The approach leverages advanced technologies to continuously scrutinise in real-time a host of user attributes, such as user identity, logins, endpoint hardware, and applications. FNU's new security mechanism upholds this posture, demonstrating a significant advance over its more traditional "trust but verify" network security.

While strategic in its intent, SOC-aaS also delivers so-called small improvements to those working at the security coalface. "The last thing we need to be doing is running around applying security patches," Domonakibau said. "The key theme for the university is visibility. Now we can see alerts, identify vulnerabilities, and act before damage is done. Not knowing is a grave risk – so to operate with the insight we have now is a huge weight off my shoulders."

A change in Fiji's COVID-free status at the time of writing this case study brings the value of the university's upgraded security screen into stark relief. As lecturers and students confined themselves to their homes and the country's leaders considered a nation-wide lockdown, Domonakibau and his team breathed a sigh of relief, knowing that the thousands of users accessing its network were unlikely to unleash a wave of malware and potential criminality that FNU was ill equipped to detect and destroy.