USM Anywhere: a Swiss Army knife in the battle for survival against pervasive threats

Customer Challenge

In 2018, Cyber Audit Team (CAT), an Australian information security services provider, was just getting their managed services portfolio off the ground. They needed a solution to power their Managed Detection and Response (MDR) offering. Initially, with a small security operations team, CAT did not have the time or resources to undergo a complicated or costly implementation, but they didn't want to skimp on functionality or performance. CAT's clients are mostly small to mid-sized businesses, and many of them do not have an internal IT department, let alone IT security expertise in-house. But they still require essential cybersecurity services to protect their networks, brands, and reputations.

Solution: USM Anywhere provides enterprise-level security for small and medium-business (SMB) clients

CAT selected USM Anywhere from AT&T Cybersecurity as the platform for their MDR services. USM Anywhere provides the centralized security monitoring, analysis, threat detection, and log management CAT needed, all in a single cloud-based solution. Fast and easy to deploy, USM Anywhere is also highly scalable—which means it has kept pace with CAT's needs as their business expanded.

USM Anywhere's enhanced approach to security monitoring lets CAT provide their clients with timely analysis of cybersecurity threats, using a solution that is more flexible and effective than traditional Security Information and Event Management (SIEM) technology.

Evolving needs in a complex environment

As businesses move from closed perimeter networks to cloud-based applications and remote working, cybersecurity threats have increased exponentially. The complexity of the environment means that information security services must be able to detect threats in the cloud, in microservices, and in home office networks. And it's no longer just the large corporations that need to protect their digital environments; all business that use web applications are high on cyber attackers' target lists.

SMB's are the core of CAT's business, but it can be a challenge to explain to senior executives why they need to care about protecting their networks and information. Good governance and compliance with data security and privacy regulations are a component, but beyond that, cyberattacks are a major business risk and prove costly. As Alex Blinko, CAT's Chief Operating Officer (COO), explains, "If their business is disrupted from a ransomware attack, or they lose customer data from a privacy breach, it's their brand and their reputation that takes the hit."

Blinko is seeing companies come to CAT for MDR services for a variety of reasons, from proving they are safe to their global partners, to reducing supply chain risk, to creating an ongoing security culture and awareness program.

The "Swiss Army knife" of security services

CAT uses USM Anywhere as the core of its MDR services, to help protect clients' digital estates from threats in the cloud, on-premise and at the endpoint. Blinko describes USM Anywhere as their modern day, digital "Swiss Army knife", referring to its wide-ranging capabilities. The platform has everything that's needed for effective security monitoring: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, and continuous threat intelligence.

One of the major benefits of USM Anywhere is that CAT didn't need to hire a much larger team to manage the platform. Blinko explains, "We can effectively have a smaller security operations team. With other tools we would need threat intelligence staff and analysts writing correlation rules for Indicators of Compromise (IoCs) and we would probably not be able to do that cost effectively."

Access to a global community of experts

As Cyber Audit Team's business has matured, threat intelligence is becoming a topic of conversation more and more with their customers, and the threat intelligence from AT&T Alien Labs really sets USM Anywhere apart.

AT&T Alien Labs is the threat intelligence unit of AT&T Cybersecurity. It includes a global team of threat researchers and data scientists who, combined with proprietary technology in analytics and machine learning, analyze one of the largest and most diverse collections of threat data in the world. This dedicated team spends countless hours researching and analyzing the different types of attacks, emerging threats, vulnerabilities, and exploits—so CAT has the latest intelligence at their fingertips. The threat intelligence from Alien Labs is continuously fed into USM Anywhere in the form of correlation rules and other high-order detections. This up-to-the-moment vigilance helps defend customers from the latest threats.

Additionally, USM Anywhere receives threat intelligence from the AT&T Alien Labs Open Threat Exchange® (OTX™). OTX™ is the one of the largest crowd-sourced threat intelligence communities in the world, providing security insights that are powered by a global community of threat researchers—more than 145,000 IT and security professionals in 140 countries.

Alien Labs and OTX combine to provide CAT with an invaluable resource by identifying threats and providing correlation rules. As Blinko says, "Because the correlation rules are written for us, not only do we get the benefit of the streamlined process—the customer gets the benefit. We can get early detection on something that's in the wild, and two days later or even sometimes hours later there's a rule written, so we can take that signature or behavior and ensure our customers get the immediate benefit of being protected. It makes our job much easier."

Enhanced protection through integration with third-party providers

CAT also takes advantage of AlienApps, USM Anywhere's highly extensible platform that provides integrations with third-party security and productivity tools to extend their security orchestration capabilities. "We integrate into a lot of third-party tools using AlienApps," Blinko says. "We've got clients using Barracuda, Carbon Black, email filters, Cisco Umbrella, and multiple different types of firewall interfaces."

AlienApps allows CAT to visualize external data with USM Anywhere's rich graphical dashboards and push actions to third-party security tools, such as firewalls, based on threat data.

A strong relationship to support future growth

Blinko says that thanks to AT&T Cybersecurity's channel partner model they have built a strong relationship with good support. "We're very comfortable and confident with the partnership and the management platform," he says. "That's important because if we were not confident it would make us second-guess taking on more complex and larger clients."

With AT&T Cybersecurity as a partner, Cyber Audit Team has a platform with the maturity and expertise to meet the challenge of providing sophisticated threat intelligence in an ever-changing landscape.

About Cyber Audit Team

Cyber Audit Team was founded in 2017 as an independent provider of information security and cybersecurity specialist services, partnering with organizations to protect their brand, value, reputation, and digital assets against internal and external threats in the rapidly-evolving threat landscape. Based in Brisbane, Australia, their customers come from a wide variety of sectors including financial services, healthcare, not-for-profits, e-commerce/retail, construction, professional services, and government. While they work with businesses and organizations of all sizes, their focus is on ensuring that small to medium-sized businesses can access the same cybersecurity mechanisms, controls, and protection that large multinationals enjoy, by making them practical, affordable, and sustainable.

Contact us to learn more, or speak with your sales representative.

About AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.