SUCCESS STORY

Proficio protects global customers with advanced cyber threat detection and response tools from Elastic Security

Region
United States

Industry
Software & Technology

Solution
Elastic Security

Increased SOC efficiency by 50%

- Proficio has increased data analyst productivity and improved the efficiency of its SOCs by 50% while using Elastic Security.

34% reduction in investigation time

- The Elastic AI Assistant for Security includes features like expert-level alert summaries and prewritten remediation steps, which have enabled Proficio to reduce the time required for investigations by 34%.

Achieved 60% business growth

- Elastic's scalability enables Proficio to meet the rising demands of its customer base without sacrificing effectiveness or analyst wellbeing.

Managed security services provider uses Elastic AI and automation tools to elevate cybersecurity, reduce response times, and deliver greater value to customers

Founded in 2010, Proficio is an award-winning managed security services provider (MSSP), delivering 24/7 security monitoring and managed detection and response (MDR) capabilities to customers around the world. The company is known for its advanced cybersecurity services that protect hundreds of organizations across many industries, including healthcare, financial services, and retail.

Proficio's team of security experts works from security operations centers (SOCs) in San Diego, Singapore, and Barcelona to monitor security events and hunt for targeted attacks. This continuous operation enables Proficio and its customers to stay ahead of cybercriminals who increasingly target vulnerabilities in cloud infrastructures and remote working networks.

A non-stop battle against cyber threats

Brad Taylor, CEO and cofounder of Proficio, sums up the company's mission: "Today, it's a constant battle against cybercrime, and we have to win every time. We must detect every attack on our customers before there's a compromise or breach that interferes with their operations."

Recognizing the challenge of monitoring vast data volumes and quickly identifying high-fidelity threats, Proficio turned to Elastic's AI-driven security analytics. Elastic AI Assistant and Elastic Attack Discovery have revolutionized Proficio's cybersecurity operations, enhancing threat detection and response capabilities while reducing the workload on analysts.
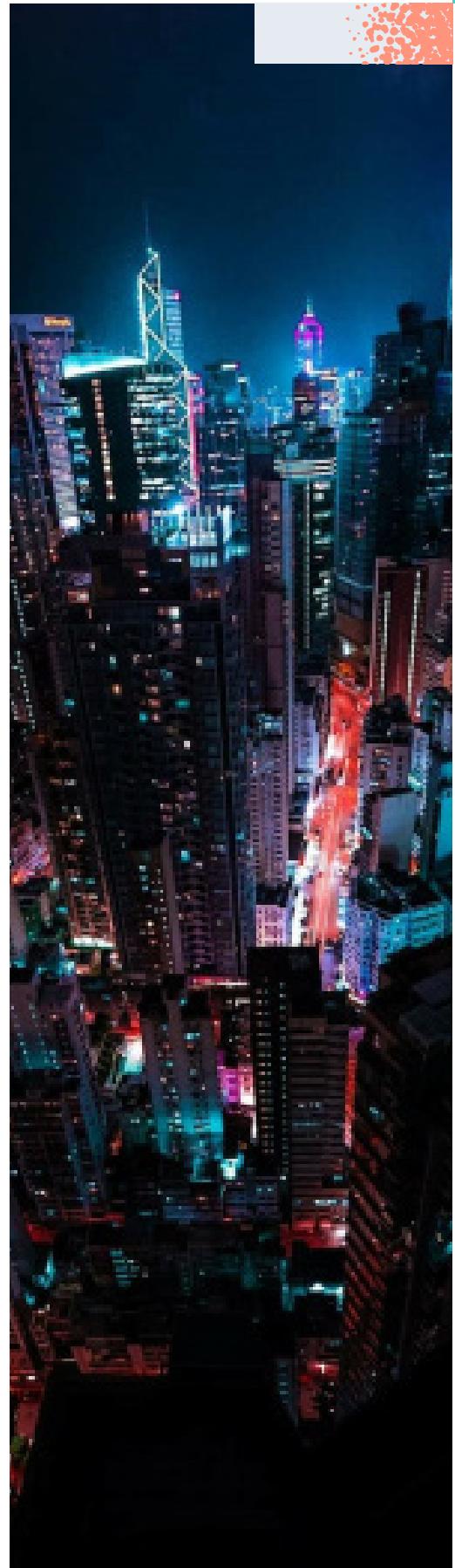
Boosting threat visibility with AI

Proficio has leveraged Elastic AI Assistant and Elastic Attack Discovery, running on AWS, to automate the detection of anomalies and identify malicious activities within data streams efficiently. "At first, integrating Elastic's AI capabilities was a significant shift from our traditional methods," said Taylor. "However, the AI-based insights have been pivotal in elevating our cybersecurity threat detection and response."

Elastic Security has significantly reduced the time spent on investigations by 34%, thanks to AI-enabled summaries and remediation steps. This shift has led to cost efficiency, with projected savings of around $1 million over three years.

Accelerating detection and response

One key area where Elastic Security has boosted Proficio's performance is threat visibility. Elastic enables data integration from various sources, enhancing visibility and discovery for security analysts and leaders alike. The team benefits from multi-variable threat detections and rules across many suspicious indicators using multiple log sources.

"Elastic Security really shines compared to other SIEMs if you need to build content for multiple vendor devices in a specific category across hundreds of customers," said Taylor.
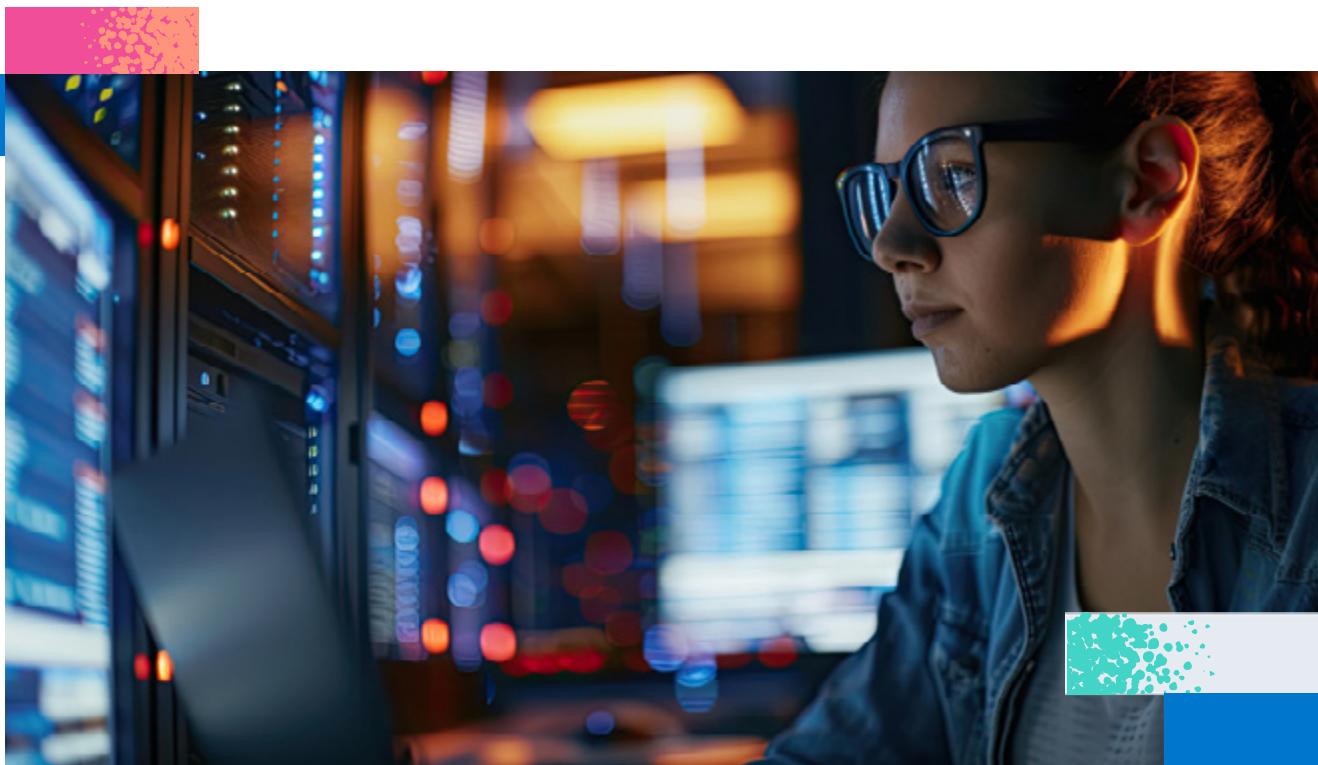
elastic

Embracing AI for proactive security

Taylor recalled a pivotal moment: "During an analysis session, an alert for a possible breach emerged. The enrichment and correlation provided by Elastic allowed us to leap into action immediately, transitioning from a reactive to a more proactive security stance."

Elastic AI Assistant streamlines onboarding and provides critical insights, significantly reducing false positives and alert fatigue for analysts. This integration has enabled Proficio to cut its mean detection time by 75%, reporting detection times of under 15 minutes and response times of under 4 minutes.

Continuous innovation with Elastic Security

Looking forward, Proficio aims to leverage Elastic's AI and machine learning (ML) advancements on AWS to build automated alert workflows, bolstering its capabilities to preempt cyber threats. Elastic AI Assistant and Attack Discovery allow teams to interact with alerts for immediate remediation guidance.

"Our journey is far from over," Taylor reflected. "We are eager to explore further integrations to augment our analysts' efforts. While we remain conscious of regulatory guidelines, we are poised to capitalize on these AI advancements, ensuring Proficio can maintain a fortified barrier against cyber adversaries."

Elastic Security's advancements underscore the transformative potential of innovative solutions in enhancing cybersecurity operations. As Elastic continues to evolve its Search AI Platform, organizations like Proficio can look forward to even greater protection and resiliency for critical infrastructures.

Embracing the future

Proficio's partnership with Elastic Security showcases the importance of embracing cutting-edge technologies to optimize threat detection and response. Elastic's AI-driven tools provide Proficio with unparalleled visibility, efficiency, and scalability, ensuring it remains at the forefront of cybersecurity innovation.

Address complex threats with Elastic Security, built on the Elastic Search AI Platform, to streamline SecOps.

Start now

elastic