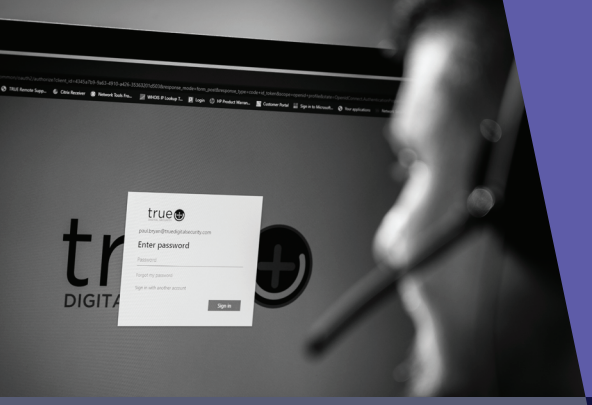
CASE STUDY

true DIGITAL SECURITY

True Digital Security Gains New Level of Visibility With Open XDR

Launching its Security Operations Center in 2012, True Digital Security is the trusted name in managed security services from the heart of America. The company is proud to be 100 percent U.S.-based, and has a history of protecting clients in the finance, healthcare, technology and energy sectors with full regulatory compliance. It has operations in Florida, New York, and Oklahoma.

STELLAR CYBER®



"I needed a partner who would treat us like a company they want to grow with, not like just a number. I wanted people who would work hand-in-hand with us, were eager to please, and excited about what they're doing, who were responsive. I found that with Stellar Cyber."

BEFORE

Scattered Security
several security platforms used to solve a problem

High Cost
cobbled together solutions were expensive

Limited Capabilities
other SIEM options didn't offer flexibility

WITH STELLAR CYBER

Open XDR
deploys as software in the cloud, edge or via a turnkey appliance

Scalable
scales easily from small to large customer accounts

Streamlined
easy to spot real threats

Pre-Integrated
core capabilities out of the box ensures the platform is accurate

Responsive
automated security coverage

"With Stellar Cyber's multi-tenancy, I can monetize every log that comes in. The way Stellar Cyber pools data ingestion, it gives me the flexibility to adjust our rates if a client's logs are sending more data than we agreed on."

STELLAR CYBER®

Finding a Responsive Partner

True Digital Security had been using an AlienVault SIEM as a key part of its security infrastructure for four years, but after AlienVault was acquired by AT&T, the SIEM provider became less responsive. "After the acquisition, the support started diminishing," said Scott Williamson, Vice President of Information Services at True Digital Security. "As a startup, they were eager to help with issues and even wrote scene directives for the SIEM and gave them to us for free, but gradually they became less and less interested in a relatively small firm like ours. It began taking up to a week to get a response to an issue, and in one instance, it took 45 days."

"I needed a partner who would treat us like a company they want to grow with, not like just a number," Williamson added. "I wanted people who would work hand-in-hand with us, were eager to please, and excited about what they're doing, who were responsive. I found that with Stellar Cyber. I talked with Joe Morin [CEO of MSSP CyFlare], and he confirmed that Stellar Cyber was just as responsive after the sale as they were during the POC."

Another key aspect of the decision to move to Stellar Cyber's Open XDR platform was that it integrated well with True Digital Security's other security tools, like SentinelOne's EDR and Siemplify's SOAR. "That was the beginning of the end of manually correlating data from multiple tools," said Williamson. These integrations allow Stellar Cyber's AI-driven analytical engine to not only analyze data from third-party tools, but to issue responsive directives through appropriate security platforms.

> Stellar Cyber gives us the power, flexibility, and visibility to form very close client relationships by serving those clients with fast, accurate detections and responses to security incidents, and by showing them exactly what they're getting."

AI and Machine Learning Deliver Instant Responses

True Digital Security differentiates itself by building close relationships with its customers and by executing quickly on issues it finds. With the Stellar Cyber platform, the company actually wins new customers through lightning-fast responses to new breaches.

"We use Stellar Cyber to give us instant telemetry about what's going on in networks," said Williamson. "Sometimes, we hear from non-customers when they have a breach, and we can jump in and find out the cause and fix it. That's a compelling way to establish a new customer relationship."

Stellar Cyber's machine learning technology becomes more accurate over time by learning each client's network behavior and applying that knowledge to events as they occur. "A few days ago, we got an alert about someone executing a script with a file type they had never executed on that server before. Because it was an anomaly, the Stellar Cyber platform alerted on that and executed actions on that server to block the malware," said Logan DeWitt. "We were proactive in blocking the incident rather than seeing it and having to write a rule to block it in the future. Besides, how would you write a static alert to know when a user logged into a machine they'd never logged into, or logged in at a weird time? You can't, but Stellar Cyber automatically catches things like that."

Greater Visibility, Happier Clients

Stellar Cyber's dashboards are also very helpful in providing visibility into what's going on across the security infrastructure. In fact, True Digital Security has built a client portal called TrueSpeed that shows each client exactly what they're getting and how the MSSP has helped keep them safe. "We offer more than just SOC services – we have MDR, XDR, and SIEM, but we also have GRC, vulnerability management, pen testing, and managed IT services," said Williamson. "Our portal offers a single pane of glass that our stakeholders can go into and see where they are, where they've been, and what they're getting for their money."

The Stellar Cyber platform also helps True Digital Security focus on profitability. "With Stellar Cyber's multi-tenancy, I can monetize every log that comes in," says Williamson. "The way Stellar Cyber pools data ingestion, it gives me the flexibility to adjust our rates if a client's logs are sending more data than we agreed on."

The bottom line for True Digital Security is that moving to the Stellar Cyber platform has made its analysts more productive and its customers happier while enhancing revenues. Says Williamson, "Stellar Cyber gives us the power, flexibility, and visibility to form very close client relationships by serving those clients with fast, accurate detections and responses to security incidents, and by showing them exactly what they're getting."

> **"We offer more than just SOC services – we have MDR, XDR, and SIEM, but we also have GRC, vulnerability management, pen testing, and managed IT services," said Williamson. "Our portal offers a single pane of glass that our stakeholders can go into and see where they are, where they've been, and what they're getting for their money."**