GUARDSIGHT

Cedar City, Utah

Cybersecurity

GuardSight.com

sales@GuardSight.com

CASE STUDY

GUARDSIGHT HELPS AFEX DOUBLE THREAT DETECTION RATE

Experienced cybersecurity as-a-service provider enables financial services company to improve cybersecurity posture and boost team morale

The Background

When it comes to cyber attacks, financial services companies fall in two camps, according to a PwC 2018 report. Those that come under fire. And those that will.

So it's no surprise that AFEX, a mid-sized financial services company with a global customer base, wanted to be battle ready. But it faced challenges. It had only a small team of junior security analysts, and they lacked the support, both in knowledge and expertise, to manage IT security operations efficiently.

"We needed a backstop, someone we could rely on to help us implement the right tools and processes to improve our cybersecurity posture", said the AFEX Information Security Director.

To carry out its mission, AFEX turned to GuardSight, an established provider of cybersecurity threat detection and response services.

The Solution

Cybersecurity Assessment

AFEX first asked GuardSight to perform an assessment of the financial firm's cybersecurity vulnerabilities.

Over the next two to three weeks, the GuardSight team worked closely with AFEX analysts to evaluate the firm's software and hardware for weaknesses as well as technical flaws that could potentially be exploited by cyber attackers.

The assessment revealed vulnerabilities in the firm's customer-facing web applications, some of them critical. As a result, GuardSight offered remediation solutions that AFEX could deploy to fix the problem. However, a retest performed by GuardSight following the remediation showed the vulnerabilities were still present.

By then, AFEX had made its own assessment:
- GuardSight's capabilities would help AFEX improve its cybersecurity posture.
- GuardSight's culture of discipline and commitment to the work could have a positive impact on AFEX's young analysts.

At that point, AFEX decided to hire GuardSight as a managed security services provider (MSSP) to support AFEX's internal security operations (SecOps).

> *"We needed a backstop, someone we could rely on to help us implement the right tools and processes to improve our cybersecurity postures."* — AFEX Information Security Director

Cybersecurity Operations (SecOps)

The GuardSight team took a methodical, systematic approach when implementing SecOps for AFEX.

The Solution Cont'd

1 HANDLER ON DUTY (HOD)

GuardSight designated a **24/7 HOD** from the GuardSight team to manage, escalate and coordinate responses to incoming alert data. The HOD was on the scene almost immediately to ensure no cyber threat went undetected.

2 TOOLS and SYSTEMS

GuardSight deployed an arsenal of tools and systems, which it refers to as cyber weapons, to help AFEX more effectively monitor, prioritize, and respond to cyber threats. These tools complemented AFEX's existing tools and were put in place **within 72 hours.** These weapons included endpoint detection and response systems, intrusion prevention systems, web application firewalls, central logging systems, security information, and event management systems.

3 THREAT DETECTION

With the necessary security established, GuardSight collaborated with the AFEX team to proactively hunt down and isolate threats. **Machine learning** played a significant role by helping to prevent and detect unique attacks. For more severe attacks, GuardSight deployed a **quick reaction force** of senior analysts to investigate and manage containment.

4 TESTING

Throughout the process, GuardSight continuously tested all cyber weapons — both AFEX's and its own — for functionality, availability, performance, and integrity.

5 KPIs

GuardSight gauged the implementation's success by tracking key performance indicators and key risk indicators, such as the number of security alerts according to intent and severity, daily averages, and response times. The two teams used this information to **guide security enhancements and reduce risk.**

6 INDUSTRY STANDARDS and BEST PRACTICES

GuardSight used the Cybersecurity Capability Maturity Model and Cybersecurity Framework to **measure** AFEX's **cybersecurity maturity and readiness.**

GUARDSIGHT

The Results

Doubled Threat Detection Rate

GuardSight increased AFEX's ability to detect threats by keeping an eye out, bringing in new tools, and augmenting the company's existing tools.

Tools don't work on their own, however. GuardSight helped AFEX manage and prioritize threats through a choreography of processes. This enabled AFEX to separate the signal from the noise, so the firm could determine which threats were important and respond more quickly than before.

GuardSight's own responsiveness and availability had an impact as well. GuardSight's ability to act fast has enabled AFEX to contain critical threats.

Improved Team Morale

GuardSight's knowledge and experience had a positive impact on the whole AFEX team.

AFEX has benefited from GuardSight's expertise, too. It regularly bounces ideas off the GuardSight team and gets recommendations on tools that GuardSight uses with enterprise clients.

"I have good analysts, but they don't have the years in the trenches that the GuardSight team has," the Information Security Director said. "GuardSight fostered a culture of commitment and passion for cyber. My staff has learned a great deal from working with GuardSight's senior analysts, and they now have more confidence."

"GuardSight gave us the tools, the processes, and access to knowledge and expertise to help us succeed. We are a much stronger and more capable team, and we have fortified our defenses."

— AFEX Information Security Director

2X
THREAT DETECTION RATE

↑
BOOSTED TEAM CONFIDENCE

A Successful Partnership

GuardSight continues to serve AFEX as an MSSP, and the two parties have a great working relationship.

"AFEX has vastly improved its threat detection rates and its ability to investigate alerts related to threats. They also understand that ultimately, this is warfare, and the enemy never gives up. They can't ever let their guard down," said John McGloughlin, GuardSight CEO.

GUARDSIGHT

SIGN UP FOR MORE INSIGHTS
https://www.guardsight.com/resources/blog/