CASE STUDY: FLEXI-VAN LEASING INC.

TO PROTECT AND MONITOR:
STRAIGHTFORWARD SERVICE FOR A SOLID SECURITY POSTURE

When James Mercer, Director of Information Technology, joined Flexi-Van in 2010, IT had been an under-resourced part of the business for some time. As would any experienced IT executive, Mercer developed a pragmatic get-well plan based on risk assessment. After completing core infrastructure improvements, Mercer and his team shifted their focus to security posture. While the intermodal transportation industry isn't regulated like healthcare or finance, security is still a primary concern for Flexi-Van.

After analyzing their current state and determining the requirements to obtain the right level of security confidence, the conclusion was obvious. The level of staffing required to establish and maintain the appropriate security coverage for datacenters and connections with customers, partners and employees nationwide was much higher than the budget allowed.

To find the right security solution, Mercer searched for a business partner that could deliver core security services, like intrusion detection and vulnerability scanning, as well as actionable intelligence around events, alerts, and incidents to help his team manage and prioritize its focus. He evaluated solutions from several providers and ultimately selected Alert Logic.

"We were looking for more than a security product, and only Alert Logic offered the fully managed service that we needed to protect our datacenters," said Mercer.

Today, Flexi-Van uses Alert Logic Professional for intrusion detection, scanning and log management.

FLEXI-VAN LEASING

ABOUT

Since 1955, Flexi-Van has provided the intermodal transportation industry with equipment to move freight via rail, ship and truck. Today, the company is one of the largest full-service chassis lessors in North America, with a fleet of more than 135,000 chassis and 3,200 generator sets for shipping items that require a controlled temperature.

SOLUTIONS

ALERT LOGIC® PROFESSIONAL

An integrated suite of intrusion detection, vulnerability scanning and log management for the cloud, on-premises, hosted, and hybrid infrastructures.

WORKING WITH ALERT LOGIC

Mercer describes getting started with Alert Logic as straightforward and fast. Within a few days of signing the contract, Alert Logic Professional threat detection and log management was configured and Mercer's team was trained via a few web-based sessions, giving them the foundation to start benefiting from the solutions.

Soon after deployment, the IT team at Flexi-Van started hearing from the Alert Logic Security Operations Center (SOC). Alert Logic solutions are fully managed, giving customers access to products that are backed by security analysts who staff a 24/7 SOC and constantly monitor customers' environments, analyze events and incidents, and alert customers when incidents occur, offering recommendations on remediation.

> ***"WE WERE LOOKING FOR MORE THAN A SECURITY PRODUCT, AND ONLY ALERT LOGIC OFFERED THE FULL MANAGED SERVICE NEEDED TO PROTECT OUR DATACENTERS."***
>
> **- James Mercer, Director of Information Technology**

"When we first deployed Alert Logic, we heard from the SOC frequently," said Mercer. "Because we had so many vulnerabilities, we were being attacked frequently. We would be notified by an analyst about an incident, and we'd either fix it immediately if we knew what to do, or we'd ask for remediation assistance, in which case the analyst would work with us until the issue was addressed."

MORE SECURITY. MORE AVAILABILITY.

One of the first big discoveries for Flexi-Van was with their Microsoft Remote Desktop Protocol (RDP) server. The Microsoft RDP environment was configured without following best practices, leaving it vulnerable to attacks from the outside. Prior to deploying Alert Logic Professional, the team didn't realize the system was being attacked; when the system would hang or grind to a halt, they'd assume it was because of a slow server situation and reboot. These reboots were expensive—the team was rebooting the system 3-4 times a month, losing 30-50 labor hours each time for financial systems and operational staff who needed access to the system for business purposes and IT staff who would spend time fixing the system.

Once Alert Logic was in place, the team realized that the system was hanging not because of a server issue, but because of frequent attacks. Using Alert Logic blocking policies against specific attacks was a good short-term solution and, for a long-term solution, knowing how they were being attacked enabled the team to reconfigure Microsoft RDP so it was inherently secure from external attacks.

Mercer notes that Alert Logic continues to work with Flexi-Van to address new attacks, in similar and new systems on an ongoing basis. For example, Flexi-Van is alerted when their IIS web servers experience Denial of Service (DoS) attacks, allowing the team to immediately change firewall rules.

ALERT LOGIC BENEFITS

In addition to the managed solution and access to security experts, there are several things that Mercer likes about working with Alert Logic.

- "It's all cloud-based." The logs, IDS data and scan results are all stored in the Alert Logic cloud. Flexi-Van doesn't need to worry about storage or disaster recovery—that's all managed by Alert Logic.
- "No initial long-term commitment." Mercer appreciated that he wasn't forced to sign an initial long-term contract. Flexi-Van started with an 8-month contract, which gave them time to complete a reasonable evaluation and determine that Alert Logic was the right business partner.
- "Available anywhere." The online dashboard lets anyone on the Flexi-Van IT team access Alert Logic from anywhere. If an incident happens when people are away from the office, they simply need a secure Internet connection to access security incident details.