



Auto Finance Company Expands Vulnerability Programme to Encompass Identity Risks With Proofpoint

The Challenge

- Incorporating identity risks into their vulnerability management programme
- Legacy applications can't be feasibly supported by their Privileged Access Management (PAM) solution
- Lack of continuous visibility into their privileged identity risks

The Solution

- Proofpoint Identity Threat Defense
- Proofpoint Spotlight

The Results

- New awareness of substantial identity risks
- Immediate improvement in risk posture
- Comprehensive vulnerability programme now addresses the No. 1 attack vector, identity

The Company

This company is a global provider of auto finance solutions, with over 9,000 employees and operations in North America, South America and Asia. Working with consumers and car dealers, they offer retail financing and lease programmes, as well as commercial lending products to dealers to help them finance and grow their businesses. They have roughly \$60 billion in assets.

The Challenge

This company has a large and diverse IT infrastructure and challenges with its longstanding legacy applications. Although they've implemented a Privileged Access Management (PAM) solution, it didn't protect many legacy applications—especially ones that were too costly to upgrade or were scheduled to be decommissioned. There were also service accounts and administrative accounts that couldn't be vaulted. The result was that the company couldn't fully control privileged credentials and identities or even have good visibility into potential identity risks. This was true for both IT administrators and regular users.

As their SVP of global cybersecurity strategy and operations says: 'If you have a large on-premises infrastructure, where you've been using Active Directory for years, there are decisions made long ago, the forgotten landscape, where vulnerabilities often exist. There's lots of technical debt. Also, cloud migration and M&A activity introduces complexity.'

The Solution

The company saw Proofpoint Identity Threat Defense as a major expansion of their comprehensive vulnerability management strategy. Traditionally, the company's approach to vulnerability management had been focused on CVEs and CWEs. But they were aware that identity configuration missteps were also creating many potential risks, so they had started tracking those as well—basically anything in their environment that caused cybersecurity risk, regardless of whether or not it had an associated CVE. Using the ISO 7-layer model as a guide, they reviewed their automated risk assessment approach to make sure it covered their entire IT environment—and identity risk management was the missing capability.

'The Proofpoint tool has opened up new insights. Without it, we knew we should look into these identity risks, but we just didn't have a way to do it.'

AVP IT Vulnerabilities

Driven by this realisation, the company implemented the Proofpoint solution for identity risk management at the start of 2021. Identity Threat Defense integrates with the company's Active Directory (AD) infrastructure, and it also scans each endpoint regularly to produce a repository of identity risk findings, which the company retrieves using the API. The IT security team reviews these findings and meets with the IT vulnerability remediation team regularly, where together they execute, and track risk-reducing changes to their environment. It's a collaborative effort, and as their AVP IT Vulnerabilities indicates: 'We do our best to work as a partner to IT.'

Associated with their vulnerability remediation efforts are SLAs that vary depending on the level of criticality, so that more critical items are highly prioritised.

The Results

Immediately after implementation, the company could see improvements in their risk posture. After using the product for more than a year, the company typically sees several new critical issues a week, and they resolve them quickly. 'It's generally people not thinking, not something malicious. Just someone making a mistake or being in too much of a hurry'.

Asked what they'd do without the Proofpoint solution, their team is somewhat stumped, given they don't know any other way to get the kind of identity insights, especially into endpoints, that the solution provides. Their AVP IT Vulnerabilities says, 'There's no way to see a password saved in PuTTY, for example'.

The SVP global cybersecurity strategy and operations adds, 'M&A is a great case—doing a scan before and after integration. With the solution, I can tell how clean their environment is and the amount of technical debt.'

‘M&A is a great case—doing a scan before and after integration. With Identity Threat Defense, I can tell how clean their environment is and the amount of technical debt.’

SVP global cybersecurity strategy and operations

When asked if he'd recommend Identity Threat Defense to others: ‘Based on the successes I've had and knowing our direction, I would recommend this to everybody from a vulnerability standpoint. Being able to visualise everything—both traditional vulnerabilities and identity vulnerabilities and misconfigurations—that's where this tool comes in.’

He adds ‘It only takes one identity vulnerability—just one—to bring your entire environment down. Any way I can shine another light on something like that adds value, particularly when you can see the risk and can reduce it over time. There are hundreds of thousands of doors that have now been locked—that's huge.’

LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trade mark of Proofpoint, Inc. in the United States and other countries. All other trade marks contained herein are property of their respective owners.