proofpoint

CUSTOMER STORY

Bank Reduces Identity Security Vulnerabilities to Close to Zero with Proofpoint

The Challenge

- Identify potentially exploitable gaps between multilayered security controls
- Accelerate remediation wherever needed
- Preempt attackers

The Solution

Proofpoint Identity Threat Defense platform

- Proofpoint Spotlight
- Proofpoint Shadow

The Results

- Reduced domain administrator privileges from 350 to zero
- Identified and removed high-risk pathways to crown jewels
- Increased executive and board member confidence in organisational controls

The Company

This national bank is owned by a multinational financial services company and operates locations across the US. It provides a range of banking, credit card, lending and wealth management services. With billions of dollars under management, the bank is committed to keeping cybersecurity vulnerabilities as close to zero as possible.

The Challenge

The bank's cybersecurity team is responsible for more than 10,000 user endpoints, as well as securing engineering, operations and access processes. It had deployed multiple layers of security, including threat awareness and cyber risk management solutions, across its infrastructure. However, many security layers were siloed from each other. Only the bank's SIEM solution operated as a 'horizontal' layer across all controls, performing event collection and analysis. Yet, in spite of sophisticated defences, there was still ongoing evidence of relentless attacks, along with the sobering knowledge that no organisation is immune from potential compromise.

'I knew there would be some degree of vulnerability that we just have to live with,' said the CISO. 'Some assets are very difficult to patch without disruption, and cyber-hygiene perfection just isn't possible. We wanted visibility and protection across our network and all endpoints to identify gaps where our other controls might not be as effective.'

The Solution

The CISO learned about Proofpoint Identity Threat Defense through industry peers. He knew that several leading banks had adopted the platform, but he hadn't yet seen it in action.

'When I saw the Proofpoint platform, the logic behind it made a lot of sense,' said the CISO. 'It enabled us to see the network like an attacker sees it.'

Proofpoint Shadow is an agentless, intelligence-driven solution that effortlessly creates a dense web of deceptions at scale across the infrastructure. It deterministically accelerates threat detection by identifying threats based on attacker interaction with deceptions, not probabilistic analysis based on signatures or behaviours. Unlike other deception technologies that deploy agents or honeypots which can tip off or be exploited by the attacker, its agentless architecture prevents attacker discovery. The CISO and his team conducted a 60-day proof of concept (POC) with Proofpoint, putting the solution through its paces. They also used pen testers to try to bypass the solution—and they failed every time.

'Identity Threat Defense gives us a much higher level of confidence in our security controls. It has made the overall inherent quality of protection quantifiably better.'

Chief Information Security Officer

Proofpoint Spotlight also enabled the team to discover high-risk pathways that an attacker could use to move more quickly through the network toward crown jewels. It continuously identifies unused or extraneous access privileges, as well as improperly stored credentials that attackers can compromise and use to their benefit.

'Spotlight quickly identified our most exploitable gaps based on actual cyberattack patterns,' said the CISO. 'It gave us the proof and context we need to prioritise remediation and optimise other security controls if necessary.'

To maximise the solution's effectiveness, only a few people on the bank's security team even know that has been deployed. Identity Threat Defense alerts are treated as policy violations and sent to the SIEM. The bank has one analyst dedicated to reviewing 'policy violations' coming from the platform. The individuals who deployed the solution had no issues with false positives—any alert is a genuine indication of a lateral movement attempt by an unknown person in the network.

'The information captured by Proofpoint provides high-value, actionable insights that act as a powerful storytelling device.'

Chief Information Security Officer

The Results

Eliminating domain access

Immediately upon deployment, Spotlight revealed and amplified unknown hygiene gaps, such as misconfigurations and access control issues. The platform provides perpetual discovery and selective automation for easily discovering and removing high-risk pathways. Not only did Proofpoint identify overprivileged accounts, but it also displayed the real network pathways an attacker could take to reach the bank's crown jewels. With this visibility, the CISO's team gained the context needed for knowing exactly how seemingly innocent connections exposed the bank to lateral movement by attackers. That insight enabled them to remove unnecessary points of connectivity based on risk metrics and impact on business operations and workflows. In addition, the CISO worked with the IT team to strategically deprivilege and phase out access privileges across the infrastructure.

'We fine-tuned our policies and reduced domain administrator privileges from 350 to zero,' said the CISO. 'Break-the-glass access is only enabled for a limited period of time in an emergency.'

The ability to quickly and easily discover exploitable gaps gives the security team a preemptive advantage over attackers. When an employee leaves, they use the ex-employee's credentials to identify where credentials were used by the employee and close any gaps that might otherwise go undiscovered.

Winning—and keeping—board of director's confidence

Besides effectively detecting lateral movement and helping the team harden the environment, the Identity Threat Defense platform delivers high communication value. The Proofpoint solution's rich telemetry and reporting enabled the CISO to provide bank executives and board members with clear, visual understanding of how attackers operate, why lateral movements are so serious, and how the bank's defences protect the environment.

Although the bank's cybersecurity infrastructure was already strong, Proofpoint gave the CISO better control, visibility and communication power. The ability to see, remediate and demonstrate control effectiveness took the bank's security to the next level.

'Identity Threat Defense gives us a much higher level of confidence in our security controls,' said the CISO. 'It has made the overall inherent quality of protection quantifiably better.'

LEARN MORE

For more information, visit **proofpoint.com**.