MORPHISEC | Merrick Bank®

Case Study

Merrick Bank Closes Security Gaps, Improves Audit Scores

Morphisec Automated Moving Target Defense (AMTD) fortifies Microsoft Defender for Endpoint and Microsoft Defender Antivirus to prevent ransomware and ensure IO stability, efficiency and system uptime

Customer

Merrick Bank is an American financial institution specializing in credit card issuance, recreational lending and credit programs. The company holds $5.3 billion in assets and serves over 2.4 million cardholders, financing consumers and marine and RV dealers across the U.S.

The company's 350 employees operate out of its Utah-based headquarters and numerous nationwide branch locations. The business relies on a mix of on and off premises workstations, approximately 1,500 endpoints, 1,100 virtual desktop infrastructure (VDI), 1,000 servers and various cloud deployments.

Like all financial services companies that accept, transmit and store sensitive customer information and financial details, Merrick Bank is federally regulated and undergoes frequent assessments and security testing to ensure compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Attestation of Compliance is maintained through an annual audit and reporting process.

Industry

Finance - Bank - Credit Card Issuer

Headquarters

United States

Company size

- 395 Employees
- $650M+ in annual revenue
- $5.3B assets under management (AUM)

Challenges

- Gaps across security stack
- Inability to defend against in-memory attacks
- Risk of IO interruption, lost functionality, system downtime and lost revenue due to competing agent-based technologies
- Internal, federal and industry-based compliance and auditing requirements

Solution

- Morphisec AMTD Technology deployed on all endpoints, VDI, on and off premises servers, and cloud deployments in concert with Microsoft Defender for Endpoint and Microsoft Defender Antivirus

Results

- Improved ransomware and other cyberthreat protection against complex threats like fileless malware
- Endpoint IO stability, maintained system efficiency, functionality and uptime
- Simplified compliance processes and alignment to PCI and SEC regulatory requirements
- Improved security audit scores

Challenge

Financial organizations remain a top attack target and face a number of omnipresent and complex threats including phishing, credential theft and ransomware attacks. Richard Kirschner, the company's Manager of Infrastructure and Access Security, is responsible for endpoint and data loss prevention (DLP) control assurance at Merrick Bank and its parent company, Cardworks.

The organization's security initiatives are supported by an in-house Security Operations Center (SOC), fully staffed red team, and a third-party managed service provider (MSP) for 24/7 detection and response. The organization operates a culture of assumed breach; in addition to weekly purple team exercises the team maintains a rigorous internal security review and audit process, and a layered defense-in-depth strategy to safeguard its systems while maintaining regulatory compliance.

"When optimizing a layered defense-in-depth approach you can't protect what you don't know exists," said Richard. "Optimizing and augmenting our strategy is paramount to maintaining a robust security posture and regulatory compliance. Regular testing ensures we quickly identify and address security gaps."

When a third-party pen test uncovered gaps related to fileless malware, the team's testing partner suggested Morphisec Automated Moving Target Defense (AMTD) as a preventative layer on top of the organization's Microsoft Defender for Endpoint and Microsoft Defender Antivirus deployments.

"A layered defense environment can be challenging—competing agent-based technologies can cause friction on endpoints, risking input and output (IO) interruption, efficiency lags, lost functionality and potential lost revenue," said Richard.

A layered defense-in-depth approach is critical for security teams as they:

Manage Broader Attack Surfaces

The rise of remote work and digital transformation initiatives like DevOps have stretched attack surfaces past most security teams' ability to define them.

Defend Against More Evasive Threats

Threats that enter a network environment are getting harder to spot and are moving further from their initial point of access. A study by the University of Eurecom (FR) reviewing over 170,000 real-life malware samples revealed that the use of evasive and in-memory techniques capable of bypassing the protection provided by NGAV/EPP/EDRs accounts for over 40% Lateral movement is a feature in at least 25% of all cyber-attacks.

"Ensuring technologies work in concert is critical for security and operational uptime."

Solution

After thorough risk and impact assessments the team deployed Morphisec (AMTD) across company endpoints. According to Richard, deployment was simple: "Everything just worked, and the integration with Microsoft Defender immediately boosted Morphisec's value."

"Morphisec initially supported defense-in-depth initiatives and filling 'cracks in the wall' that no other solution could," said Richard. "Since deploying Morphisec five years ago we've realized even greater value with additional capabilities like built-in vulnerability assessments, ransomware protection, credential theft protection and VDI security."

Today the organization uses Morphisec AMTD to secure all resources including its on-premises and private cloud servers. "Servers are a tricky environment in agent security; it comes down to inputs, outputs and minimizing interruption," said Richard. "Set and forget is an important benefit- we can let Morphisec run without having to do maintenance. The product isn't intrusive and doesn't steal resources from other applications. With Morphisec, it does its job well and you'll never know it's there unless you want to know, in which case you can set up notifications."

Results

With Morphisec, the team has confidence that the organization is protected from complex and evasive threats. "We continue to have good outcomes related to external pen testing," said Richard. "Our red team attacks and challenges Morphisec on a daily basis, and Morphisec continues to outperform expectations."

The solution's internal and intangible value is a significant bonus: "Morphisec is instrumental to our internal and external auditing initiatives," said Richard. "Since we deployed Morphisec we've consistently improved audit scores, which simplifies compliance and gives our leadership greater peace of mind and confidence that we're protected across the spectrum."

Morphisec's seamless integration across the organization's security stack keeps IO on endpoints low at all times; processing, hard drive and memory IO remain stable, maintaining system efficiency, functionality and uptime.

"Morphisec is natively comfortable," said Richard. "From a product perspective, it's a solution that fits a layered approach. From a company perspective, the level of support we get from Morphisec's incident response and customer success teams on an ongoing basis is the icing on the cake. Our Morphisec experience is a partnership—it's been a truly successful collaboration."

Morphisec's breach prevention solution features a revolutionary, patented AMTD technology that Gartner calls 'the future of cyber'. It secures critical systems against the most advanced and disruptive cyber threats. More than 7,000 customers trust Morphisec with its AMTD, vulnerability visibility and risk-based prioritization technology to stop supply chain attacks, zero-day attacks, ransomware, fileless and in-memory attacks, and more, from endpoint to the cloud.

"A layered defense consisting of AMTD obstacles and deceptions significantly elevates an organization's security posture."

Gartner® Tech Innovators in Automated Moving Target Defense

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Cipla, Citizens Medical Center, and many more. Learn more at www.morphisec.com

To learn more, visit morphisec.com/demo