MORPHISEC

CASE STUDY

Global Hedge Fund Protects Endpoints and Bloomberg Terminals from Ransomware and Other Advanced Attacks

Morphisec Automated Moving Target Defense (AMTD) helps firm avert critical system downtime and eliminate false positives

Customer

Morphisec's customer is a leading US-based hedge fund with a portfolio of approximately $5B in assets under management. As a quantitative fund ("quant shop"), workstations outnumber employees 10:1. The firm's team relies on complex systems to drive statistical techniques, mathematical modeling, and automated algorithms.

Global operations run 24/7, leveraging worldwide data lines and source providers across domestic servers and three US-based data centers. Financial services platforms (multiple versions of Bloomberg Terminals) support the firm's critical stock and option trades and provides access to an email client, real-time market data, newsfeeds, and messaging and collaboration services.

INDUSTRY

Finance – Hedge Fund

HEADQUARTERS

United States

COMPANY SIZE

- Leading US-based hedge fund
- $5B assets under management (AUM)

CHALLENGES

- Security gaps to protect Endpoints and Bloomberg Terminals from evasive attacks
- Reduce system downtime due to EPP incompatibility with the trading systems
- Reduce high volumes of false positives

SOLUTION

- Morphisec AMTD Technology deployed on all workstations, trading terminals and servers

RESULTS

- Eliminated system downtime, saving reputational damage and lost revenue of up to $10 million per year
- Reduced false positives by 99 percent
- Prevention of evasive attacks – hundreds of browser-based attacks, and multiple severe cyber attacks
- Full trading system compatibility with negligible performance impact (Sub-10MB agent, 0.5% CPU*)
- Easy to deploy, operate and update

** As tested per standard configuration, actual results may vary according to specific usage*

Challenge

The firm's Chief Information Security Officer (CISO) and six-person team manage an internal Security Operations Center (SOC) and multiple security tools for data inventorying, data loss prevention, endpoint security, and event mitigation. The team is tasked with protecting the firm from cyber-attacks, including the protection of their trading systems, prevention of data loss, and protecting the firm's reputation. Critically, the team ensures that their cybersecurity solutions support operational continuity, do not impact performance, and enable meeting customer SLAs.

While sourcing in-memory detection tools the team discovered that most are not compatible with trading software. Previously the company had used Determina by VMware, which was discontinued. Financial trading platforms like Bloomberg Terminals frequently issue configuration changes, with signature and software updates that can trigger false positives in EPP and EDR solutions. In response, these solutions automatically isolate and disable trading software for alert investigation and remediation. Teams must then reinstall and reactive the software, which can take a quarter of a working day.

Financial trading platforms are critical to trader performance—system downtime takes traders offline and can cost the firm from $1.2 million to over $10 million per year, depending on market volatility during downtime due to trading disruptions. Downtime creates data integrity issues within the trading platforms, creating multi-day disruptions, and lead to potential missed customer SLA and reputational damage.

In addition to generating false positives, signature and behavioral-based endpoint protection solutions annually missed between 1-2 workstation events per quarter, creating multiple major undetected events per year. Manual event intervention and incident remediation required extensive team time and attention.

By their nature, financial platforms are highly performance sensitive and cannot allocate the system resources required to deploy the full protection coverage of traditional endpoint security solutions. The consistent and timely delivery of updates and patches to the firm's operation-critical financial software is a key concern that had to be addressed when selecting endpoint security solutions.

System uptime and connectivity to trading terminals like Bloomberg, Eikon (by Refinitiv), Factset, and others are paramount for business operations, however, these platforms present additional challenges to hedge fund security teams and are a single point of failure which can dramatically impact business.

In this case, the firm's Bloomberg Terminals are accessed through dedicated private line infrastructure that effectively bypasses the firm's firewall or gateway solutions, thereby increasing risk.

Bloomberg Terminals, and similar platforms, are used by financial analysts, large institutional investors, and portfolio managers. The systems are delivered with unique hardware and software bundles for trading activities, real-time market data feeds, investing analytics, and instant messaging services. The terminals are costly and business-critical assets that are highly sensitive to downtime and must be protected against cyber threats.

Solution

The firm's CISO chose Morphisec and its **Automated Moving Target Defense (AMTD)** technology to run alongside its existing endpoint protection platform as a way to secure all endpoints and Bloomberg Terminals against in-memory exploits and other evasive attacks.

Morphisec is a prevention-focused technology, which is an important distinction relative to detection and response solutions according to the CISO —

"If an attacker successfully hacks the Bloomberg Terminals, they'd have full access to the firm's critical infrastructure, which would be devastating."

Unlike detection and response solutions, Morphisec doesn't need signatures or IOCs to act. Instead, it prevents advanced attacks by dismantling the attack's delivery mechanisms and kill chain, instantly stopping the event before it even begins. 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 5,000 customers trust Morphisec and its AMTD technology to stop supply chain attacks, zero-day attacks, ransomware, fileless and in-memory attacks, and more, from endpoint to the cloud.

Today the firm uses Morphisec AMTD to support its defense-in-depth strategy. The CISO views Morphisec as *"the perfect solution for business-critical applications that cannot tolerate downtime, residing in protected networks, as it doesn't need signatures or online connectivity to operate."*

Results

Upon first installing Morphisec six years ago, the firm instantly saw a 99 percent reduction in false positives, prevention of hundreds of browser credential theft attempts, and prevention of multiple attempted and significant cyber attacks every year. Crucially, system uptime is maintained since Morphisec is fully compatible with the firm's trading terminals, enabling uninterrupted software updates and trading operations.

Morphisec continues to provide the firm with value that goes beyond technology spend with the CISO noting that *"Morphisec saves our firm up to $10 million per year in operational, cyber damage and reputational costs, depending upon specific market volatility during prevented incidents".*

With Morphisec, the firm gets maximum protection with an operationally efficient and cost-effective solution, according to the CISO.

"Morphisec provides novel in-memory protection technology that's low maintenance and needs little overhead. Within our tech stack, Morphisec requires the least amount of care and maintenance—it's exceptional protection with sweet ROI."

"Morphisec was simple to install and easy to operate and has a negligible performance impact which matched our business needs," says the CISO.

"It's reassuring to know that Morphisec covers all of the firm's endpoints and our Bloomberg Terminal platform with an additional layer on systems that are running terminal software packages."

"A layered defense consisting of AMTD obstacles and deceptions significantly elevates an organization's security posture"
Get your complimentary report ***here.***

Gartner Tech Innovators in Automated Moving Target Defense

About Morphisec

Morphisec provides prevention-first security against the most advanced threats to stop the attacks that others don't, from endpoint to the cloud. Morphisec's software is powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity. AMTD stops ransomware, supply chain attacks, zero-days, and other advanced attacks. AMTD provides an ultra-lightweight, Defense-in-Depth security layer to augment solutions like NGAV, EPP and EDR/XDR. We close their runtime memory security gap against the undetectable cyberattacks with no performance impact or extra staff needed. Over 5,000 organizations trust Morphisec to protect nine million Windows and Linux servers, workloads, and endpoints. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more.

Schedule a demo now: morphisec.com/schedule