KEEPING FINANCIAL INSTITUTIONS OPERATING

PROBLEM

Maintaining ongoing availability of information

SOLUTION

enSilo

BENEFITS

- **Real-Time Attack Prevention:** stopping data from being altered or exfiltrated
- **Ongoing Uptime**: ensuring business continues, without disruption, even in an infected environment
- **Productivity:** enabling institutions to efficiently complete transactions and execute orders
- **Compliance:** helping protect the integrity and privacy of regulated data

Ensuring ongoing operations is a priority

When dealing with money, every moment counts. Any delays in trades, transfers, loan closures, etc. can have serious consequences (and costs) for both customers and the financial institutions they have trusted to execute those transactions. For example, brokerage firms can be found liable if they don't execute orders within contractual timeframes.

To protect their continuous operations and reputation and maintain compliance with industry regulations (such as the Payment Card Industry Data Security Standards (PCI DSS), Personal Information Protection and Electronic Documents Act (PIPEDA), etc.), institutions need to ensure the ongoing integrity, privacy and availability of their information. This is increasingly difficult, given the scope and sophistication of the attacks they are facing, which can disrupt their operations or hold their information hostage (ransomware).

Recently, the chair of the US Securities and Exchange Commission (SEC) admitted that cyber-attacks are the biggest risk facing financial systems. According to the ThreatMetrix Cybercrime Report, cyberattacks targeting the financial sector increased 40% over the past 12 months - a record 21 million fraud attacks and 45 million bot attacks were detected in the fourth quarter of 2015 alone. If an attack successfully compromises the information systems of an

individual or a department/division, it can compromise the institution's ability to complete transactions and execute orders in a timely fashion. To combat, financial institutions need to protect the integrity of their data and the ongoing operations of their revenue-generating employees (information systems). They need enSilo.

ENSILO'S DEFENSES

enSilo gives institutions the freedom to operate, even when compromised, with the confidence that sensitive data can't be tampered with or stolen. The solution hones in on and shuts down in real-time any malicious or unauthorized activity performed by an external threat actor, while allowing business to go on as usual. In this manner, enSilo stops data from being altered (encrypted), wiped or stolen, while enabling legitimate operations to continue unaffected.

enSilo gives financial institutions peace of mind, with:

Real-Time Attack Prevention

stopping data tampering or exfiltration from compromised information systems.

Ongoing Uptime

ensuring business can continue uninterrupted, even when information systems are infected with advanced malware, by preventing data from being altered, wiped or stolen.

Compliance with Regulations

helping institutions maintain the privacy and integrity of protected financial information.

Productivity

enabling revenue-generating employees to confidently complete transactions and execute orders.