CUMMINS ALLISON

Endpoint Security: Safeguarding your ATMs Against Cyber Attacks

In May 2016, a hacker group used Moneytaker malware to organize fraudulent transactions, stealing $8 million from 16 small community banks in the U.S.[1]

The financial sector has historically been at high risk for cyber-attacks due to the vast amounts of money they process and sensitive personal data they store. According to a recent report, financial institutions are experiencing 300 percent more cyber-attacks than any other market sector.[1]

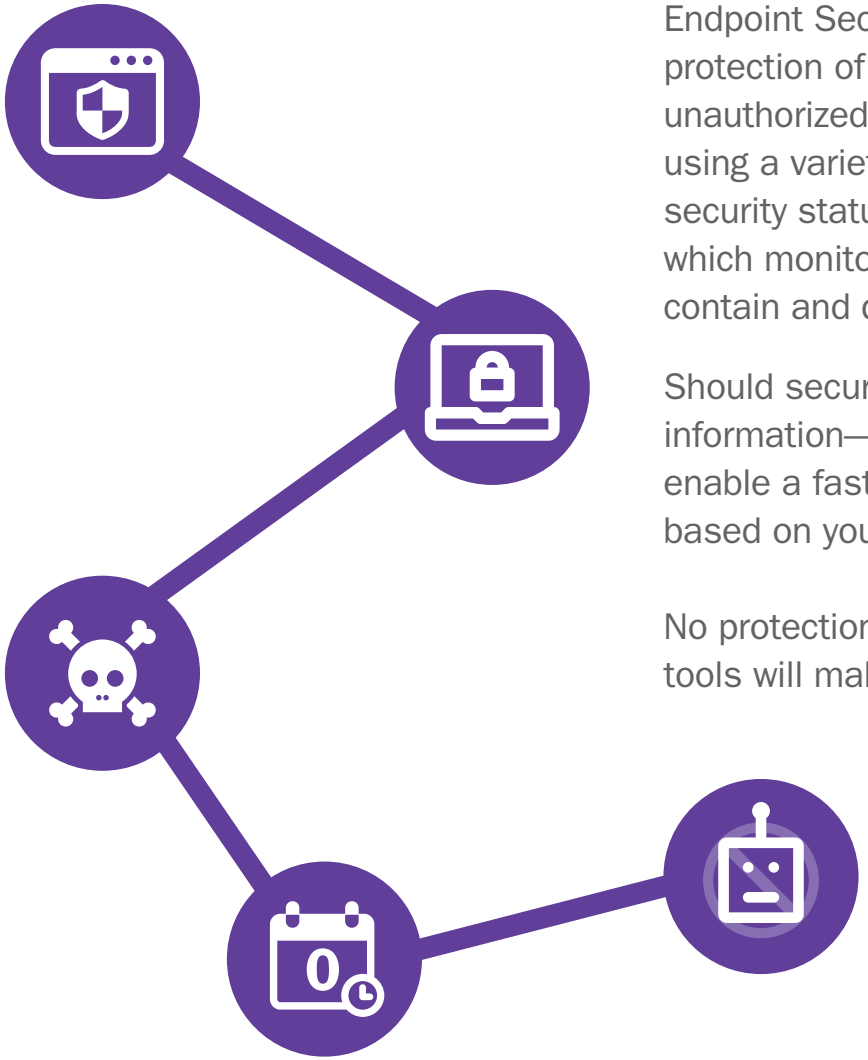
Despite higher risks, the financial sector has achieved the most favorable rating in terms of security effectiveness.[2] With FIs as a prime target for cybercriminals the importance of preventing threats before they can damage ATMs cannot be overestimated.

And it isn't just the big banks that need to worry. In recent years, the targets of hackers and malware attacks are increasingly small to mid-size banks and credit unions. In fact, banks and credit unions with annual revenues of less than $35 million accounted for 81% of hacking and malware breaches at financial institutions in 2016.[3] Many of these FIs lack the resources to invest in robust data security systems and the technical expertise to support them.

This eBook explains the Endpoint Security techniques used on Cummins Allison ATMs to minimize ATM attacks by cybercriminals.

[1] Check Point, 2016 Security Report.
[2] BitSight Insights, "Which industry has the most effective security posture?, http://bit.ly/2ksr3UN
[3] Beazley, "Hackers target smaller financial institutions," July 2016, https://www.beazley.com/documents/Insights/201607-hackers-target-smaller-financial-institutions.pdf.

Stop Malware and Ransomware at the Endpoint



Endpoint Security is a managed service that provides real-time endpoint protection of your ATMs. A software agent on the ATM prevents an unauthorized application or tool from being installed onto the system by using a variety of security controls. This agent continually monitors the security status of your ATMs and reports back to a management server which monitors connected endpoints (ATMs) based on policies which block, contain and quarantine any potential threats.

Should security events occur, incident reports provide actionable information—origination of attack, scope of damage, impact to ATM—to enable a faster and more effective response. Reports can be customized based on your organziation's requirements.

No protection is absolute. But a combination of awareness and preventive tools will make your ATMs as safe as they can be.

Types of Protection

Access control and program protection

Access control protects endpoints and ensures ATMs are compliant with deployed security policies. A firewall controls the inbound and outbound network traffic, allowing only authorized communication.

Protection against unauthorized software ensures only legitimate, approved programs are allowed to run and perform tasks on endpoints. Unapproved applications and untrusted applications are blocked or terminated.

Encryption and port protection

To safeguard against data theft, full disk encryption and port protection are used. Encryption software automatically protects all information on the hard drive—including user data, the operating system, temporary files and erased files.

Media encryption and port protection secures removable media devices such as USB flash drives, backup hard drives and CDs and enables restricting or blocking of physical ports.

Ransomware protection

Ransomware encrypts data files and employs the use of ransom to regain access. Anti-ransomware prevents these threats by using a behavioral analysis engine capable of detecting, blocking, disabling and removing the most sophisticated ransomware infections from the ATM. It also restores any encrypted data as part of its automated remediation capability.

Zero-day protection

The term ‘zero-day’ refers to an attack that is unknown to the software’s developer or the public at large.

To prevent these attacks, a technique called threat emulation picks up malware at the exploit phase and employs an advanced sandboxing engine to pre-screen and run any suspicious program in a virtual environment (or “sandbox”) and decide whether the program is safe or not. Potential threats are identified, blocked, and eliminated.

Anti-bot protection

Bots are malicious, stealthy software that invades your network and allows criminals to remotely control your ATM. Anti-bot software prevents communications by detecting infected machines and preventing them from participating in criminal network activity such as denial-of-service attacks or automated spam messaging.

Summary

Cummins Allison's Endpoint Security is part of our Managed Services offering, and when paired with Software Maintenance and Remote Support provide a comprehensive software security offering. Software Maintenance ensures availability of Microsoft Windows patches and Cummins Allison software fixes for your ATMs.

Protect your ATM assets from active and persistent threats with Endpoint Security. Get in touch with us to dive deeper and find out how we can help you better protect your ATMs.

Contact your local representative, visit **cumminsallison.com/atm**, or call 800-786-5528.

CUMMINS ALLISON

852 Feehanville Drive
Mt. Prospect, IL 60056
800 786 5528
cumminsallison.com

023-1990