SOLUTION BRIEF

Protect the Endpoint's Vulnerability to Uncatalogued Malware

The only solution to stop zero-day keyloggers and man-in-the-middle attacks

McAfee and Advanced Cyber Security (ACS) have joined forces to bring you two highly strategic patented cybersecurity solutions that can stop zero-day keyloggers from capturing credentials needed to advance an attack and a multifactor out-of-band authentication solution that prevents data theft by man-in-the middle attacks.

McAfee Compatible Solution

- ACS EndpointLock with McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1

The Business Problem

Up until now, organizations have lacked the ability to fully protect their endpoints from a zero-day keylogger, the single biggest threat that is leveraged in the first stages of almost all advanced threats. A keylogger is a type of surveillance software that has the capability to record every keystroke you make on your keyboard, including credentials used in the authentication process. In addition, most keyloggers come with the ability to change their form and go on undetected as they quickly spread between the endpoints in your organization. In addition, each year, organizations encounter man-in-the-middle breaches, which can bypass traditional two-factor "in-band"/"single-channel" authentication.

McAfee and ACS Joint Solution

With ACS EndpointLock (ACSEL) keystroke encryption software, McAfee and ACS provide the missing link in endpoint security by encrypting all of an endpoint's keystrokes, thus blocking credentials and other sensitive data from ever being stolen. With keystroke encryption, ACSEL encrypts all keystrokes at the lowest possible layer in the kernel and stops advanced threats in their tracks. ACSEL protects the vulnerable endpoint from exposing sensitive information, such as data entered during provisioning of corporate VPN profiles, login credentials, and private company information that can lead to a costly data or network breach.

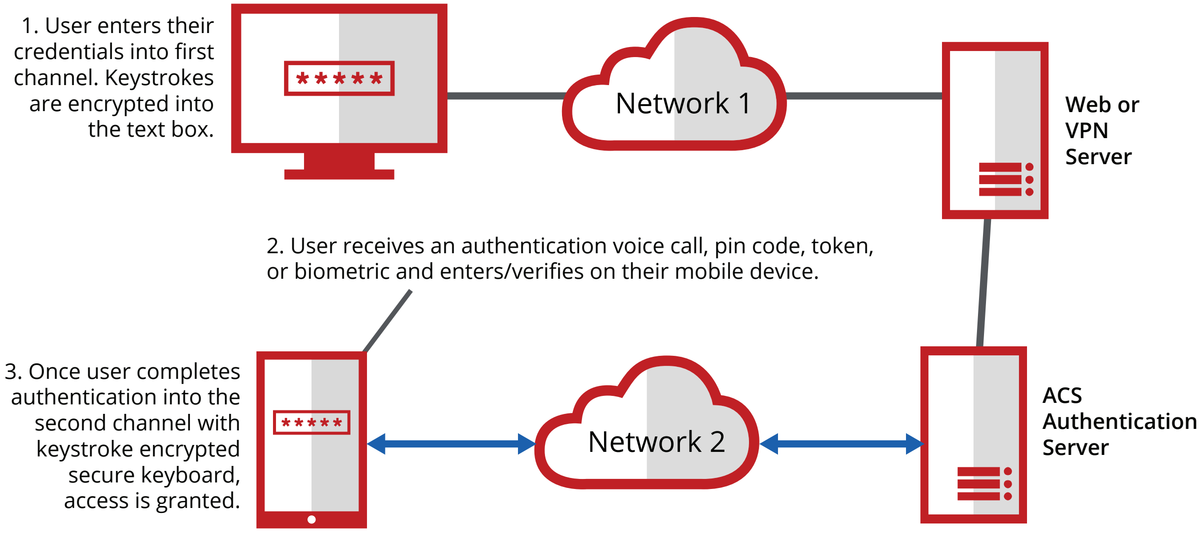
EndpointLock with patented keystroke encryption technology benefits:

- Elimination of keylogger capture of keystrokes at all deployed endpoints
- Easily deployed as part of group policy
- Event management and reporting options consolidated through McAfee ePO software
- Kernel level alerts of deep compromise
- Takes remediation action on the end node based on the file reputation change

CyGate Keystroke Encrypted Out-of-Band Multifactor Authentication

- The only authentication system that prevents keyloggers.
- Seven out-of-band methods.
- Out-of band, dual channel authentication that evades man-in-the-middle attempts
- Deployment options: on premises, in the cloud, or in hybrid environments

CyGate Keystroke Encrypted Out-of-Band Multifactor Authentication



1. User enters their credentials into first channel. Keystrokes are encrypted into the text box.

2. User receives an authentication voice call, pin code, token, or biometric and enters/verifies on their mobile device.

3. Once user completes authentication into the second channel with keystroke encrypted secure keyboard, access is granted.

Figure 1. Three easy steps of the CyGate Keystroke encrypted out-of-band multifactor authentication process.

ACSEL comes with additional features, including anti-screen scraping, anti-clickjacking, anti-subversion, and kernel compromise warning. All of EndpointLock's patented features work seamlessly in the background—without causing any latency.

ACS CyGate combines patented keystroke encryption with patented out-of-band multifactor authentication to provide the most secure, affordable, and flexible authentication for banks, corporations, universities, government agencies, healthcare, and social networking.

Keystroke Transport Layer Security (KTLS)

Both ACSEL and CyGate utilize keystroke transport layer security (KTLS), an ACS-patented cryptographic protocol that provides for the encryption and transport of keystrokes originating from the kernel at the time of secure boot and entry into any application or web browser. While secure sockets layer (SSL) and transport layer security (TLS) begin strong cryptography at Layer 4, or the transport layer within OSI, KTLS begins strong cryptography from the kernel level at Ring 0 and encrypts all keystrokes. This closes a large vulnerability gap that has existed in endpoint security.

About Advanced Cyber Security

The Advanced Cyber Security KTLS protocol brings a new layer of security to the endpoint, with patented proactive solutions that help to stop advanced threats in their initial stages and prevent their advancement.

About EndpointLock Deployment and Management with McAfee ePolicy Orchestrator

Advanced Cyber Security's EndpointLock (ACSEL) integration with McAfee ePO software provide deployment, property reporting, and event reporting. ACSEL can be installed/deployed on the McAfee ePO software-managed client nodes automatically. ACSEL sends its own properties of the client node to the McAfee ePO software server. Events are generated, depending on the license status of the product, ACSEL's services status, and driver status. These events are forwarded to McAfee ePO software via the McAfee Agent.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com