USE CASE: CONTACT CENTER
DATA SECURITY SOLUTIONS

CONTACT CENTER STEPS UP THEIR ENDPOINT SECURITY TO REDUCE THEIR RISK OF A DATA BREACH.

CHALLENGE:

With sensitive information like social security numbers and credit card data continuously passing through their environment, contact centers have become prime targets for a cyber attack. Keylogging spyware is commonly used in the beginning stages of a breach to steal access credentials and other information needed to advance the breach.

✓SOLUTION:

Enable Endpointlock Keystroke Encryption at every endpoint to protect all data as it is entered into the device. This includes BYOD (Bring Your Own Device) employees who are accessing the network systems from their personal device.

EndpointLock Benefits:

- Protection from keylogging spyware, the number one malware component.
- Blocks screen scraping and clickjacking.
- Monitors the kernel and alerts of a compromise.
- Protects the vulnerable gap found at the point of data entry.
- Runs in the background, no employee training needed.

COMPANY OVERVIEW:

A Contact Center, providing sales and support across multiple channels including phone and live chat.
Other services include maintaining and managing online payment systems.

DETAILS:

Following a high profile data breach that occurred at the billing vendor of a large healthcare group, the Contact Center discovered they had the same vulnerability to zero-day keyloggers. The company deployed ACS EndpointLock Keystroke Encryption software to help prevent keyloggers from stealing access credentials and Personal Identifiable Information (PII).

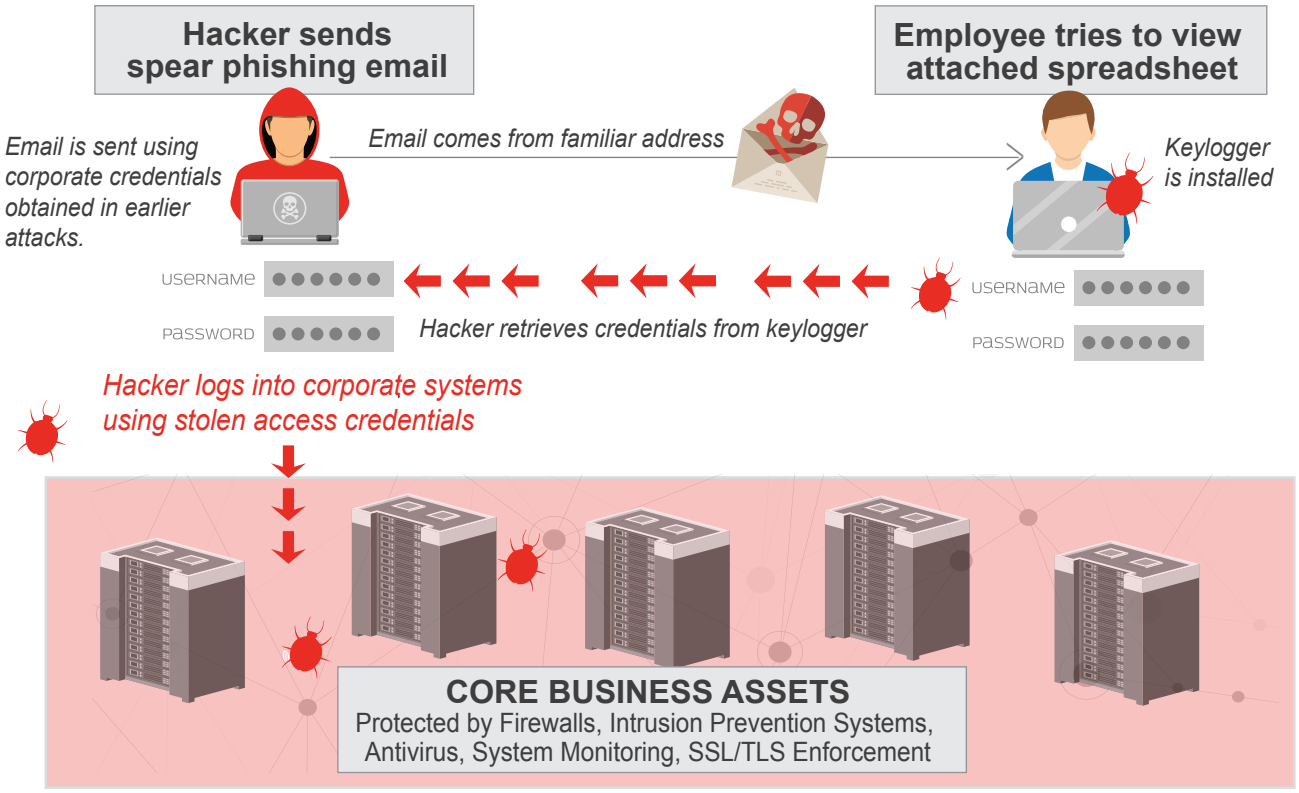
Keyloggers are commonly downloaded as a result of clicking on an infected link or phony file inside an email, text message, social media page or website. This practice of tricking unsuspecting victims into clicking on links that look legitimate is called “phishing”. According to recent reports, phishing was found in 90% of breaches and 95% of all phishing attempts that led to a breach, were followed by software installation, including keyloggers. Endpointlock uses ACS Keystroke Transport Layer Security (KTLS™) protocol to route keystrokes around the vulnerability (where keyloggers are installed waiting to capture every word you type).

Adding keystroke encryption filled a gap in the Contact Center’s endpoint security and helped to reduce the likelihood of a breach due to stolen credentials.

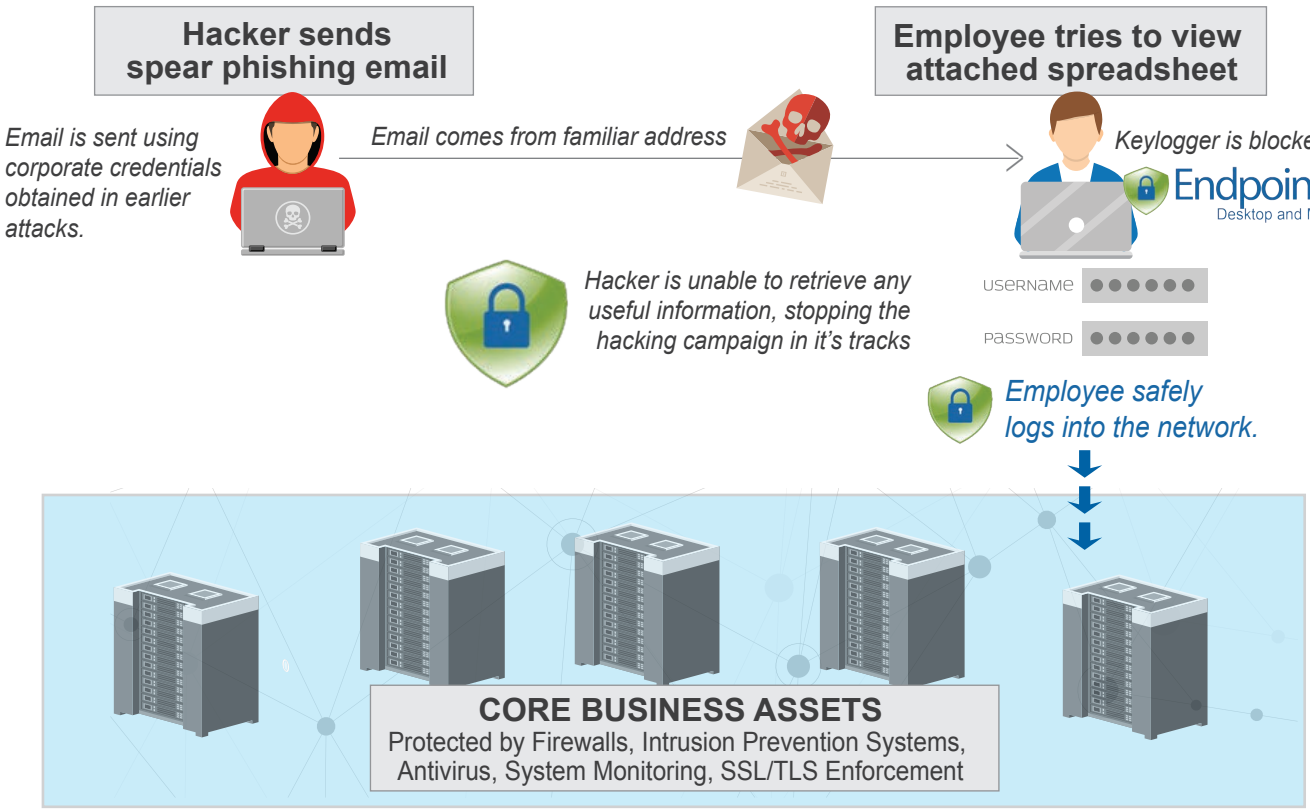
EndpointLock™
Desktop and Mobile Security

Results

BEFORE



AFTER



EndpointLock™
Desktop and Mobile Security