CIOReview
The Navigator for Enterprise Solutions

CYBER SECURITY SPECIAL NOVEMBER - 2017 CIOREVIEW.COM

20 Most Promising Cyber Security Solution Providers - 2017

Technological disruptions such as cloud, IoT, and mobility have made cybersecurity an absolute necessity to protect enterprises from threats like ransomware, DDoS and phishing attacks. In order to protect their clients' sensitive data, enterprises need to keep updating their approach towards cybersecurity as the attacks become increasingly sophisticated with the fast-paced technological evolution.

DDoS attacks on IoT devices can be quoted as one such instance. Though connectivity among systems is greatly valued, botnets or networks of infected computers can cause serious damage to the functioning of an enterprise. Even phishing attacks have moved beyond simple—from poorly constructed emails to creative ones with attractive offers that drive victims to click on links. Also, there is the increasing threat of ransomware, where the victim is monetarily exploited with their personal information as leverage. To counter these scenarios, enterprises' focus should shift from protection to prevention. It is critical to remember that safety, reliability, and privacy are an integral part of cybersecurity.

In answer to these demands for cybersecurity, there are numerous companies that offer solutions, but enterprises should invest in the right provider that suits their specific necessities in order to extract the full value of their investment. It is essential to identify the providers who understand the dynamics of the market and continue to upgrade their approach towards cybersecurity with regard to potential technological disruptions. In an effort to assist the decision-makers in upholding the safety of their working environments and the integrity of their clients' data, CIOReview has charted out "top 20 companies" offering tailor-made and efficient solutions for cybersecurity.

We present to you "20 Most Promising Cyber Security Solution Providers - 2017."

Company:
Advanced Cyber Security

Description:
ACS offers encryption at the keystroke layer and protects any data transmitted by the endpoint

Key Person:
Craig "CJ" Brunet
Chief Information Security Officer

Website:
advancedcybersecurity.com

Advanced Cyber Security

The New Perimeter in Security Starts at the Keystroke


Craig "CJ" Brunet

Steam emanating from a cup of coffee on his desk, the bespectacled stranger awaits a ping from the malware that he surreptitiously installed in the system of the CFO of a major financial institution. Bingo! The CFO has just accessed the URL of the central database and is now typing the authentication details, unaware of the keylogger component of the malware picking up each character in the background. Yet, something is not right. The screen of the anonymous 'man-in-the-stack' only displays a meaningless sequence of numbers from zero to nine. What the cybercriminal is unaware of is the fact that the company deployed a unique endpoint security protocol—that specifically renders malware components useless at the keystroke transport layer—Advanced Cyber Security's (ACS) EndpointLock™ Keystroke Encryption.

According to the Verizon Data Breach Investigative Report, malware instances accounted for 69 percent of the world's most notable breaches. Of this segment, 98 percent of the malware had a keylogger component, which captured critical information such as authentication credentials, PHI, PII, credit card numbers, and social security numbers at the very instant of transmission, the keystroke. "Since the world's best security protocols, antivirus software, and DLP tools begin serious encryption at the OSI layer, which is Layer 4, zero-day keyloggers often go unidentified," explains Craig "CJ" Brunet, Chief Information Security Officer of ACS. "We deploy directly into layer zero, within the kernel itself, and provide stronger and more secure encryption for the data being transmitted."

ACS EndpointLock™ interrogates the kernel before deploying, and if there is a compromise involved, an alert is sent to the security system admin via group policy orchestration (ePO). If the kernel is clean, the next operation involves installing the cryptography with the TPM chip of the endpoint device, using RSA 2048 encryption cryptosystem. Once the installation is complete, ACS' patented protocol, the Keystroke Transport Layer Security (KTLS) performs certain unique tasks. Working with Fortune 100 clients from financial, retail, healthcare, and processing sectors, ACS' technology is certified by Windows, MAC, Android, and iOS operating systems, and delivered through McAfee ePO and into the Intel TPM.

In a Windows or MAC environment, the cryptographic protocol creates a new 256-bit encrypted pathway for the transmission of keystrokes, bypassing the vulnerable slow stack area that is usually where keylogger components of malware are delivered, to perform message filtering and hooking. The KTLS™ protocol allows keystrokes to be encrypted, with a decrypt packet sent to the application requesting the stroke, and finally, the encrypted stroke itself is transmitted along the secure pathway directly into the application, which may be browser-based, installed software, dark screen Active Directories (AD) and so on. In parallel, the ACS EndpointLock™ sends a numerical sequence along the traditional OS pathway that wants to see data going to and from the endpoint coincidental with the instance of a stroke. This eliminates the capture of keystrokes, as the data is safely being transmitted along the encrypted pathway directly into the text box of an application.

> **"We deploy directly into layer zero, within the kernel itself, and provide stronger and more secure encryption for the data as it is being transmitted"**

ACS applies the same technology to Android and iOS devices, with the subtle difference of providing a geo-positioned encrypted keyboard to the endpoint which is the only keyboard accessible in the ACS-protected application. ACS delivers these capabilities in SDKs that can be integrated easily with any branded application and deployed as an update.

This technology expands the current security perimeter by starting the encryption at the point of data entry, the keystroke. Since this is exactly where so many breaches begin, adding KTLS™ protocol will be a game changer in the endpoint security space. This is the first technology that can actually prevent zero day keyloggers from being used to advance a breach. CR