CASE STUDY

CENTURY 21 RELIES ON CYNET FOR ADVANCED THREAT PROTECTION

OVERVIEW

INDUSTRY

Retail

ABOUT

Century 21 is a chain of department stores in the northeastern United States.

There are stores located in Brooklyn (NY), Long Island/Westbury (NY), Morristown (NJ), Paramus (NJ), Rego Park/Queens (NY), Lincoln Square/Upper West Side (NY) and Jersey Gardens Elizabeth (NJ) opened in April 2013, and Center City Philadelphia.

The company was founded in 1961, by Sonny Gindi and Al Gindi. The original store is located at 472 86th Street in Bay Ridge, Brooklyn. The Century 21 flagship location is in Lower Manhattan.

CHALLENGE

Enterprises of all kinds are targets for malicious cyber activity. This is especially true of the retail industry, which is one of the biggest targets for cyber-attacks.

In fact, the major security issue facing retailers is protecting the personal and transactional information of their customers. Sophisticated cyber criminals are increasingly attacking retail enterprises, stealing large numbers of financial and personal records.

First and foremost on the agenda for Century 21 security management was the protection of its customer data. As a forward thinking organization, Century 21 understood that prevention alone was not enough – they needed to be prepared for an advanced attack from unknown malware, Trojans or Zero Day Attacks.

Because of this, Century 21 was constantly looking at new technologies. Their goal was to ensure that they not only had the best prevention and perimeter security solutions, but also the most sophisticated solution for uncovering threats that had managed to bypass the prevention layer.

SOLUTION

Dan Groscost, Director of Network Technology at Century 21, found the solution he was looking for in the Cynet 360 platform. Cynet 360 could be installed within hours, and required virtually no IT resources for operation and maintenance. The rapid implementation enabled Century 21 to quickly and easily deploy Cynet and initiate a comprehensive, proactive, intelligence-driven approach to cyber-attack detection and remediation.

Upon installation, Cynet's agentless probe immediately began scanning Century 21's distributed network of Windows-based endpoints across multiple locations. It was the module-based, plug-and-play nature of Cynet's agentless solution that enabled thousands of endpoints to be scanned in only two-hours. During the extensive testing of Cynet 360, Century 21 was able to detect and immediately remediate potentially malicious threats.

> *"After only a short period of scanning Century 21's endpoints, Cynet 360 detected and remediated threats which could have become malicious had we not dealt with them."*
>
> **Dan Groscost, Director of Network Technology, Century 21**

In order to secure their customer data with one of the most advanced solutions available, Century 21 decided to deploy a full implementation of the Cynet 360 platform, to help detect and remediate threats that had bypassed their prevention layer. Cynet uses a unique approach for threat detection, which includes the collection, correlation and analysis of hundreds of indicators across organizational endpoints, files, networks and users. This allows Cynet to detect potential threats, anomalies and unsigned malware that have never been seen before, enabling them to bypass existing detection solutions.

To support this process, Cynet's integrated 24/7 Monitoring takes an eyes-on-glass look at potential threats to reduce false/positives ratio, provide insight for remediation and help to prevent future attacks. The full scope of a potential threat is clearly highlighted on Cynet's Security Management Dashboard. Malicious threats and potential attacks can be rapidly mitigated by quarantining or deleting files, blocking users or taking systems offline.

ABOUT CYNET

Cynet 360 is an all-in-one solution providing a comprehensive platform for rapid detection, remediation and forensics of the most sophisticated threats hitting organizations today. Cynet's advanced detection technology rapidly identifies malicious threats that have succeeded in bypassing the organization's prevention layer including: Malware, Trojans, Ransomware and others.

In addition to manual and automatic remediation of uncovered threats, Cynet provides advanced forensic capabilities including identification, extraction, analysis, and interpretation of data via static analysis, context aware sandboxing, deep file scans, and the deployment of decoys. Cynet's integrated 24/7 Monitoring utilizes front-line security intelligence to verify the validity of threats, assisting customers with remediation while eliminating false positives.

Cynet was chosen as one of Ten Innovative Network Security Startups by Network Computing and was named a Top Ten Endpoint Security Solutions of 2015 by CSO Outlook. Visit our website: www.cynet.com.

For more information on setting up a Demo or Proof of Concept, please contact us: info@cynet.com.

Cynet
PRECISE THREAT DETECTION