CASE STUDY | TECHNOLOGY

Tier-1 technology software & hardware provider chose Deep Instinct's Deep Learning cybersecurity solution for threat prevention, operational efficacy and connection-less security

12
ENDPOINTS FOUND INFECTED WITHIN FIRST WEEK OF DEPLOYMENT

462
MALICIOUS CAMPAIGNS DETECTED WITHIN 3 MONTHS

SCORED 99% DETECTION & PREVENTION RATE ON MALWARE TEST DURING EVALUATION, WITH THE SMALLEST FOOTPRINT OF THE AGENT

THE COMPANY

A US-based, high profile Fortune 500 technology software & hardware provider, with tens of branches deployed in more than 50 countries.

Industry: Technology

Company Size: Large Enterprise, over 50,000 employees in more than 50 countries

Existing Security solution: Traditional AV & next-gen EPP

Environment: 30,000 endpoints

THE NEED

The company was looking for an advanced endpoint security solution to augment their current existing Symantec Endpoint Protection solution, and to replace their Carbon Black Protection platform.

The company searched for solutions that could allow full protection when a device was not on their network, or when it was offline. They put their most of their efforts on the technical side, but also on the performance, monitoring and administrative capabilities. And so the company decided to evaluate six different solutions in the market.

They were looking to evaluate and determine which solution will provide better protection and meet their growing endpoint security needs to include safeguarding against APT and unknown malware threats.

Deep Instinct was the last vendor to be evaluated, and on the challenging malware test set, it scored a detection and prevention rate of over 99%. Besides the impressive detection rate, the customer was also impressed by the small footprint of the agent.

THE SOLUTION – DEEP INSTINCT™ THREAT PREVENTION PLATFORM

- **Deep Instinct™ D-Client:**
  - On-device agent includes D-Brain, powered by deep learning. Supports many file types, including PE, Office, PDF, Macros, Fonts, Images, Flash and many more.
  - Detects and prevents any malicious file before it is accessed or executed on the endpoint.
  - Lightweight with zero impact on the endpoints from initial installation. Low memory footprint (<150MB) and requires less than 1% CPU usage
- **D-appliance on the cloud:**
  - Centralized management console for easy monitoring of the entire organization's endpoint and mobile security and deployment status.
  - Provides tools for configuring the different organization's security policy.
  - Manages different policies for groups or individual devices
  - Deployed on public cloud (AWS)
- **Deep Classification:**
  - Rapid classification of malware (known and unknown) in real-time with no human involvement into seven different malware types, using Deep Instinct's unique deep learning malware classification module.
- **Remediation:**
  - Quarantine files, restore files remotely, delete files remotely, terminate running process, isolate device network – all to mitigate and operate current existing threats identified in the environment.
- **Advanced Threat Analysis:**
  - Tool set that performs advanced analysis of threats found in the organization. This includes static analysis, sandboxing analysis, screenshots and network dump of the potential threats.

THE RESULTS

Although protected by next-gen endpoint solution - over 10% of devices were found infected

Within the first week of deployment, 12 endpoints were found to be infected with malicious campaigns, including coin miners, worms, spyware and other PUA.

When the first deployment cycle of 1,500 endpoints was completed, a total of 147 devices were revealed to be infected – almost 10% of the protected devices, although Symantec Endpoint Protection supposedly protected them.

Hundreds of malicious campaigns found, including vicious dormant WannaCry ransomware

A total of 462 malicious campaigns were found including PUA and dual-use tools, and a total of 140 pure malicious campaigns, including dormant WannaCry ransomware waiting to run, several Spyware and info stealer families including Nymaim, Loki, Fareit and Agent Tesla, banking trojans including Emotet and other Worms and viruses

End-to-end protection against any file type

Other than binary files being found, Office and PDF files were found as well, leading to dropping other binary files, and a Flash file embedded with a new exploit in the wild was prevented to be run from the browser. Some of the endpoints were synced with Google Drive, and nine drives were found compromised with malicious campaigns. Those malicious campaigns included trojans and other hacking tools, including tools to scan and map the network. A few of them were also malicious files embedded with Metasploit's Meterpreter, running a Python reverse shell to a few IP addresses within the customer's network.

Request an online demonstration of Deep Instinct platform

Click here to set up a free consultation on your endpoint security environment and see how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities against unknown threats.

Request a Demo

TO GET STARTED WITH THE CYBERSECURITY REVOLUTION

ISRAEL

23 Menachem Begin Rd
28th Floor
Tel Aviv
Israel, 6618356

NEW YORK

501 Madison Ave
Suite 1202
New York City, NY
USA, 10022

SINGAPORE

The Working Capitol
1 Keong Saik Rd
Singapore
068907

+972 (3) 545-6600 www.deepinstinct.com contact@deepisntinct.com

deepinstinct
BEFORE YOU KNOW IT