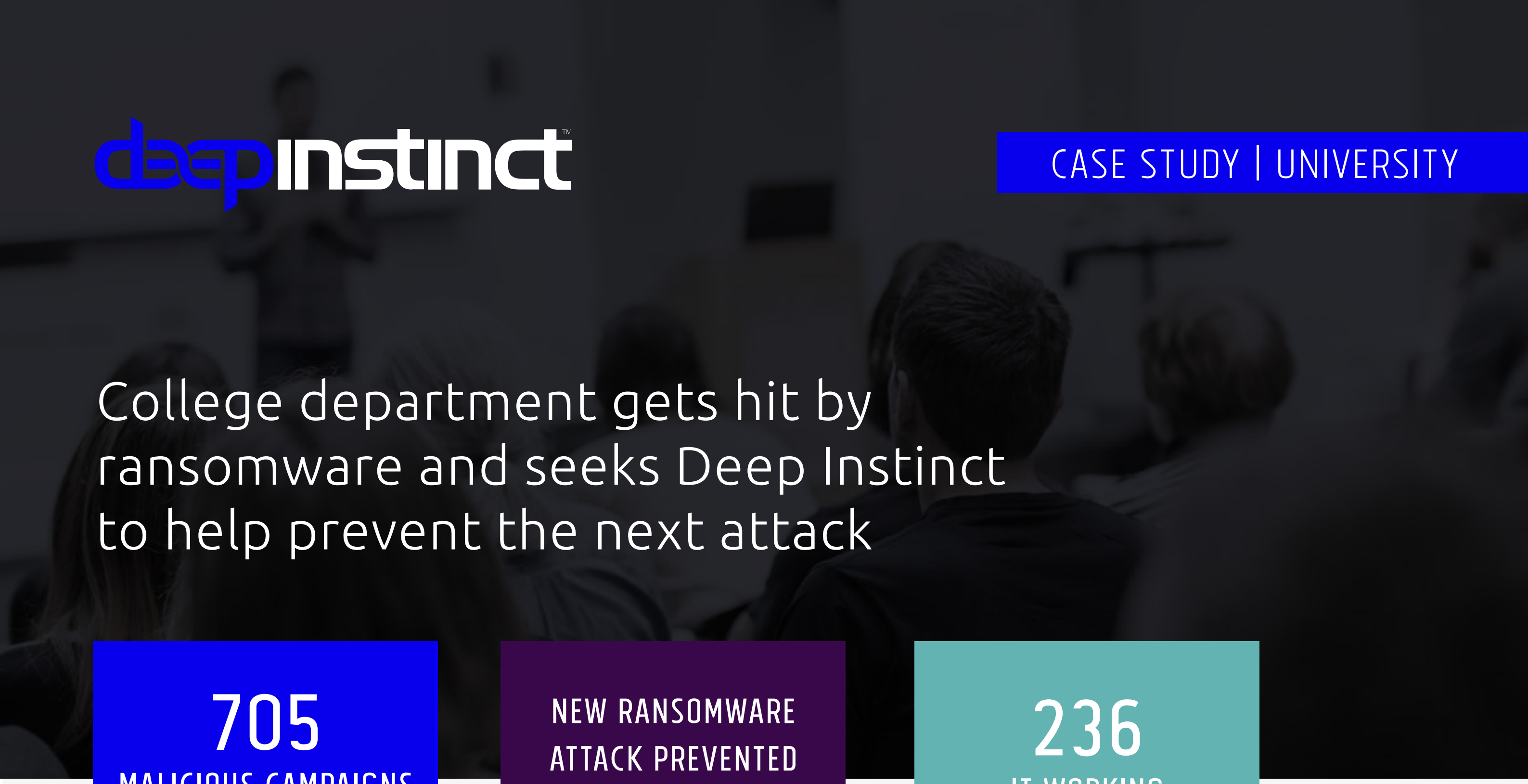

CASE STUDY | UNIVERSITY

College department gets hit by ransomware and seeks Deep Instinct to help prevent the next attack

705
MALICIOUS CAMPAIGNS DETECTED

NEW RANSOMWARE ATTACK PREVENTED IN REAL-TIME: 59 ENDPOINTS SAVED

236
IT WORKING HOURS SAVED

THE COMPANY

A college based in North America with over 90,000 students.

Industry: Education
Company size: Large Enterprise
Existing security solution: Traditional AV
Environment: 4,000 Windows endpoints

THE NEED: EXPLICIT RANSOMWARE PREVENTION

The college department in charge of recruiting students from other countries, was hit by a ransomware attack that spread in through the whole department. The effect was encryption of all the department's files, more than 2,000 documents, without the option to release them. Everything was lost.

At the time, they were only using one endpoint security solution, which was TrendMicro, and the customer understood that a traditional antivirus is not enough to protect against the next ransomware wave. The college was looking for a comprehensive endpoint security solution that could mitigate this ransomware threat and other possible APTs.

The college reached out to Deep Instinct and requested a proof of concept. After a successful POC, Deep Instinct was selected to secure the endpoints in the college.

> *"Deep Instinct has proven to be an integral security control in our environment. We use it in combination with another AV engine and Deep Instinct catches a lot of suspicious objects that aren't identified by the other product. Our environment is undoubtedly more secure with Deep Instinct."*
>
> **National College | IT security analyst**

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
- **Deep Instinct™ D-Appliance:**
  - Management Console for easy monitoring of the organization's security and deployment status.
  - Provides tools for configuring the organization's security policy.
  - Manages different policies for groups or individual devices.
- **Deep Classification:**
  - Rapid classification of malware (known and unknown) in real-time with no human involvement into seven different malware types, using Deep Instinct 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

Over 700 malicious campaigns detected

Within the first deployment cycle, 1,000 devices were deployed, and more than 220 million files were scanned within a month. Although the college had TrendMicro deployed, Deep Instinct was able to detect 705 malicious campaigns: mostly binary files, but also some malicious documents and malicious scripts.

APT campaign embedded as part of supply chain was prevented, unspotted by current traditional AV solution

One of the campaigns revealed was the CCleaner campaign, while it was still uncovered by traditional antivirus and other machine learning-based solutions. CCleaner, owned by Avast – a security vendor, is a well-known IT tool to remove redundant and temporary files. In some of its versions, a backdoor was bundled inside it, and that was signed by a digital certificate – making it much harder for traditional antivirus and machine learning-based endpoint security solutions to detect.

New unknown ransomware prevented in real-time before it was still revealed by the industry

During the period of deployment, the college also faced a new wave of ransomware again. This time it was GrandCrab, a sophisticated ransomware distributed by email. Before it was still revealed by the industry, Deep Instinct was able to prevent the threat and save 59 endpoints inside the organization. By doing so, Deep Instinct saved approx. 4 working hours for re-imaging each machine, and so 236 IT working hours were saved for the college.

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

BEFORE YOU KNOW IT