CASE STUDY | MSSP

An IT managed services provider (MSSP) chooses Deep Instinct for endpoint protection, for its high prevention capabilities and Multi Tenancy solution

1 BILLION
FILES SCANNED

700+
MALICIOUS CAMPAIGNS DETECTED

THE COMPANY

Description: A technology consultancy group that provides managed IT & security services, based in North America

Industry: MSSP
Company Size: SMB
Environment: 10,000 endpoints

THE NEED

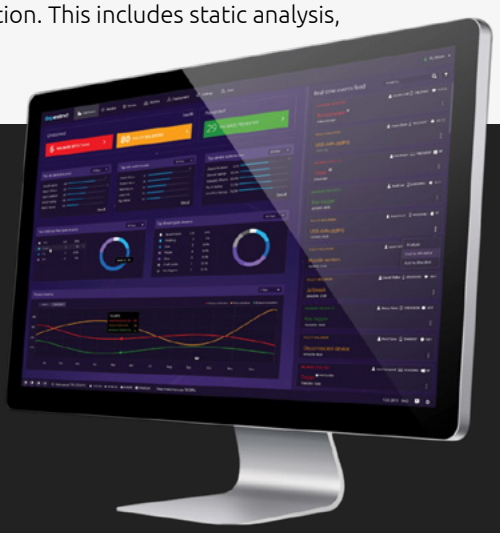
Following a recent ransomware attack on several of their customers, the company was looking for a more advanced endpoint security tool.

They evaluated several next-gen endpoint protection solutions, and were looking for a solution that can:

- Provide prevention against unknown threats.
- Provide multi- tenant architecture, and not just a virtual offering around it to be able to truly support their operation.
- Have the solution scale to their needs

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 on top of threats found in the organization. This includes static analysis, sandboxing analysis, screenshots and network dump of the potential threats.



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
089109

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

deepinstinct
BEFORE YOU KNOW IT