INTELLIGENCE DRIVEN DETECTION & RESPONSE

SERVIZI GESTITI DI CYBER SECURITY

certego

ABOUT CERTEGO

- **Founded** in **2013** by experienced cyber security experts & developers (**Honeynet Project, Cuckoo Sandbox, Thug, etc.**)
- **100 + customers** in **Europe, Middle East, US** and **Japan**
- Integrations with leading cyber security providers like **Fortinet, Cisco,** and **Check Point**
- Recognized by Gartner in 2015 & 2017 Worldwide Threat Intelligence Competitive Landscape
- Headquartered in Modena IT, with offices in Milan and US (Q1, 2019)

certego

ABOUT CERTEGO

PROVIDER OF SECURITY OPERATIONS CENTER AS A SERVICE

POWERED BY CERTEGO

PANOPTIKON SECURITY ORCHESTRATION

CYBER THREAT INTELLIGENCE PLATFORMS

ADAPTIVE CYBER DEFENSE

BREACH DETECTION

DIGITAL INVESTIGATION

INCIDENT RESPONSE COORDINATION

certego

MANAGED DETECTION RESPONSE OVERVIEW

- **MDR dened (source: Gartner)**
  - "Managed detection and response services allow organizations to add 24/7 dedicated threat monitoring, detection and response capabilities via a turnkey approach"
- **What does MDR offer?**
  - Provides cyber security resources and expertise to organizations looking to expand beyond prevention to address breach detection, response and round-the-clock monitoring
  - Ideal for:
    - Organizations with immature or non existent detection monitoring and response capabilities
    - Organizations looking for external validation of current Security
    - Organizations looking for external validation of current Security Operations efficacy

certego

WHY MANAGED DETECTION RESPONSE

- Many organizations have invested in preventative **security technologies (firewalls, IPS, AV, etc)**
- **Yet breaches still occur…**
  - Misconfigurations of **networking devices, security devices, servers and/or endpoints**
  - Unpatched vulnerabilities
  - Targeted attacks
  - End user mistakes
- The detection and response to breaches are a challenge to many organizations
  - Manual reviews or reports of voluminous logs is not efficient
  - Many organizations are **missing breach detection / response expertise**
  - Others missing **24/7 coverage** of **breach detection and/or containment**

certego

CERTEGO'S APPROACH

- **Certego's PanOPTIKON platform is key differentiator:**
  - Sensors monitor network traffic as well as receiving logs from network and security devices as well as SIEMs and host sensors
  - The sensor performs automated, multi-faceted analysis, event correlation to ag potential breaches to Certego's operations center for validation, classication of severity and containment response
- **Upon breach, Certego's customer is notied to begin containment process**
  - Optionally, automated responses (e.g., egress block rules in firewall) can be done

ABOUT CERTEGO

THREAT HUNTING ADD-ON
(ENDPOINT DETECTION & RESPONSE)

CONTINUOUS VA ADD-ON
(NETWORK VULNERABILITY SCAN)

TACTICAL RESPONSE
(AUTOMATIC FW RULES ENFORCEMENT)

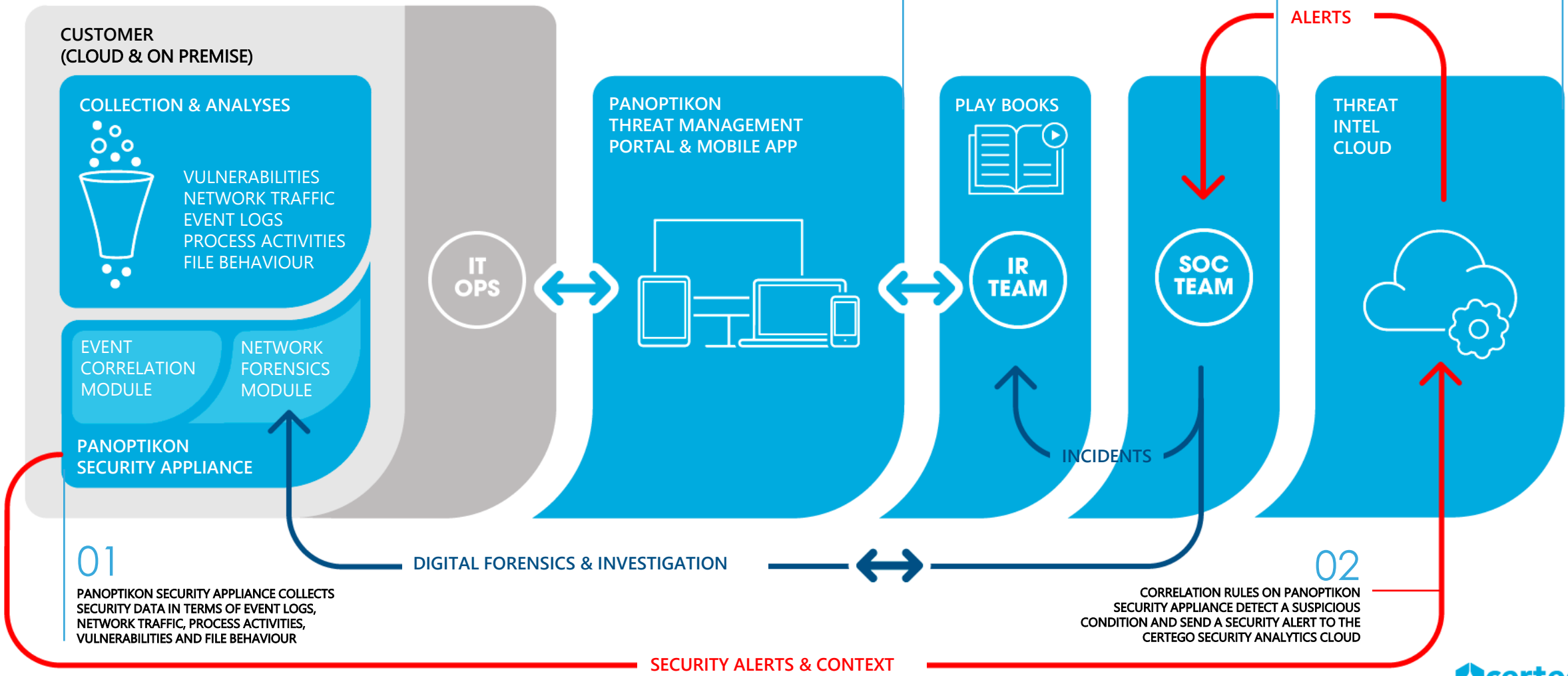
LOG MANAGEMENT

CERTEGO PANOPTIKON CORE SERVICES
(NETWORK SECURITY MONITORING & LOG COLLECTION)

PANOPTIKON SECURITY ORCHESTRATION PLATFORM

certego

PANOPTIKON SOP ARCHITECTURE



certego

PANOPTIKON CORE: SECURITY APPLIANCE

- **Function:**
  - Perform collection, analytics and interacts with Certego's Cloud Services
- **Capabilities:**
  - Advanced SIEM
  - 60K+ Threat Detection Rules
  - DDoS/Application Attack Detection
  - Zero-day & APT Detection
  - 50+ Antivirus Engines
  - Malware Callback Detection
  - Executable Analysis (Sandbox)
  - 4 x 10/100/1.000 Mbps Ethernet Ports (Sniffer Mode)
  - Full Packet Capture*

*Customer formal authorization is required

ANOMALY DETECTION | SIEM | NETWORK FORENSICS | SANDBOX | MULTIPLE AV ENGINES

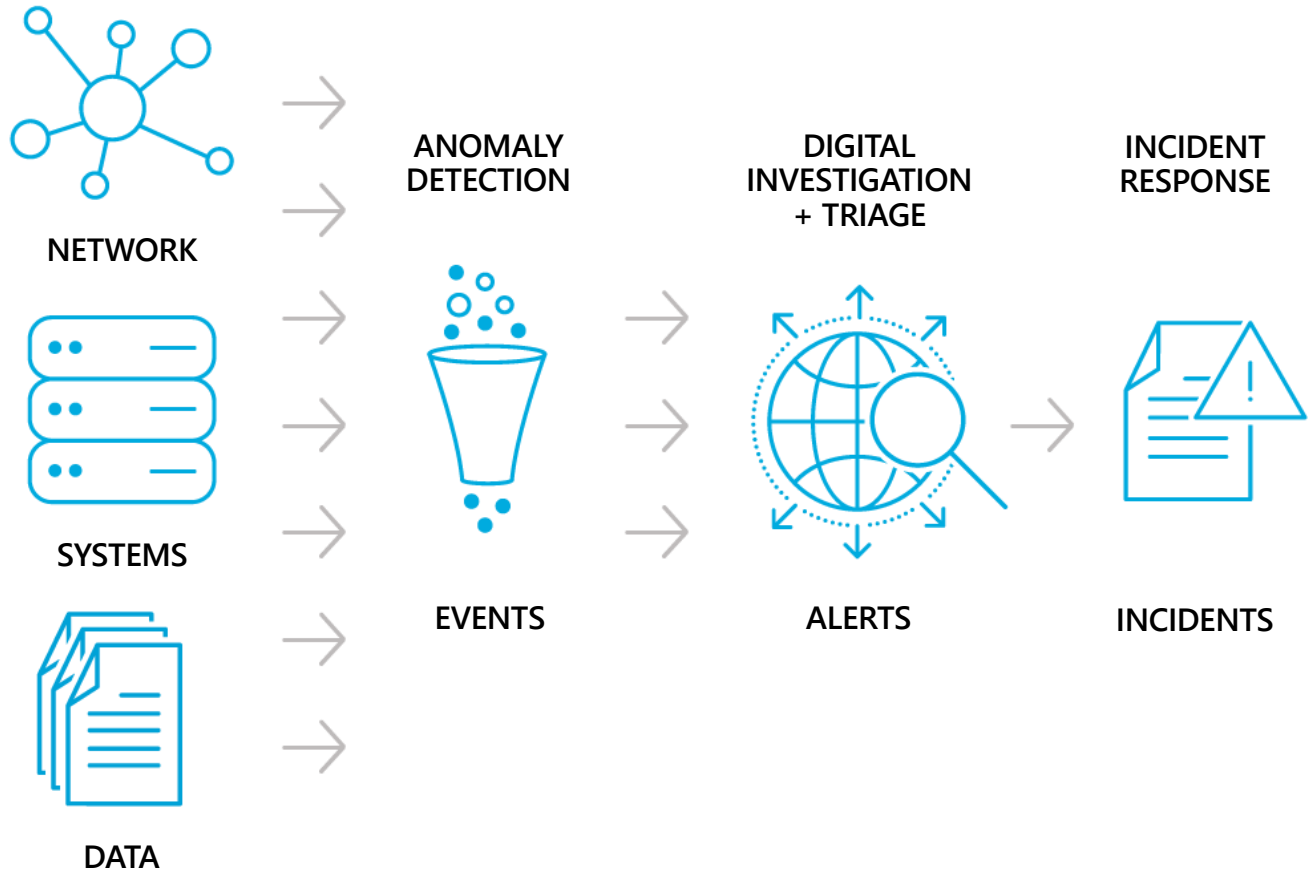
	INTERNET BANDWIDTH	USERS
NS50	NS50	250
NS100	NS100	2.500
NS200	NS200	>3.000

THREAT HUNTING ADD-ON

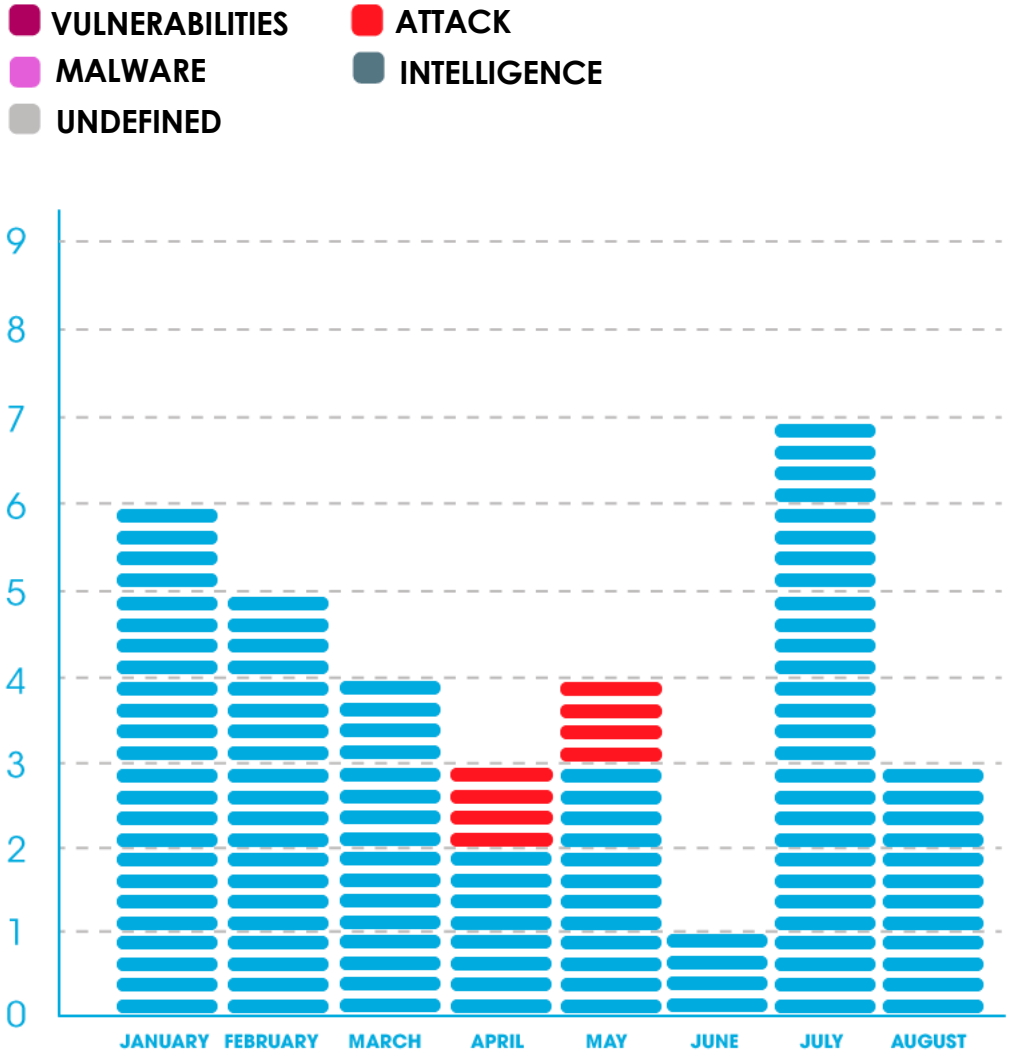
- **Telemetry Agent:**
  - Windows, OS X, Linux
  - Based on Carbon Black Cb Response
- **Continuous Endpoint Monitoring:**
  - Process Analysis & Timeline
  - Registry Actions
  - Child / Parent Process Investigation
- **CPU usage less than 1%**
- **RAM usage 20MB**
- **Network bandwidth 50 Bps**

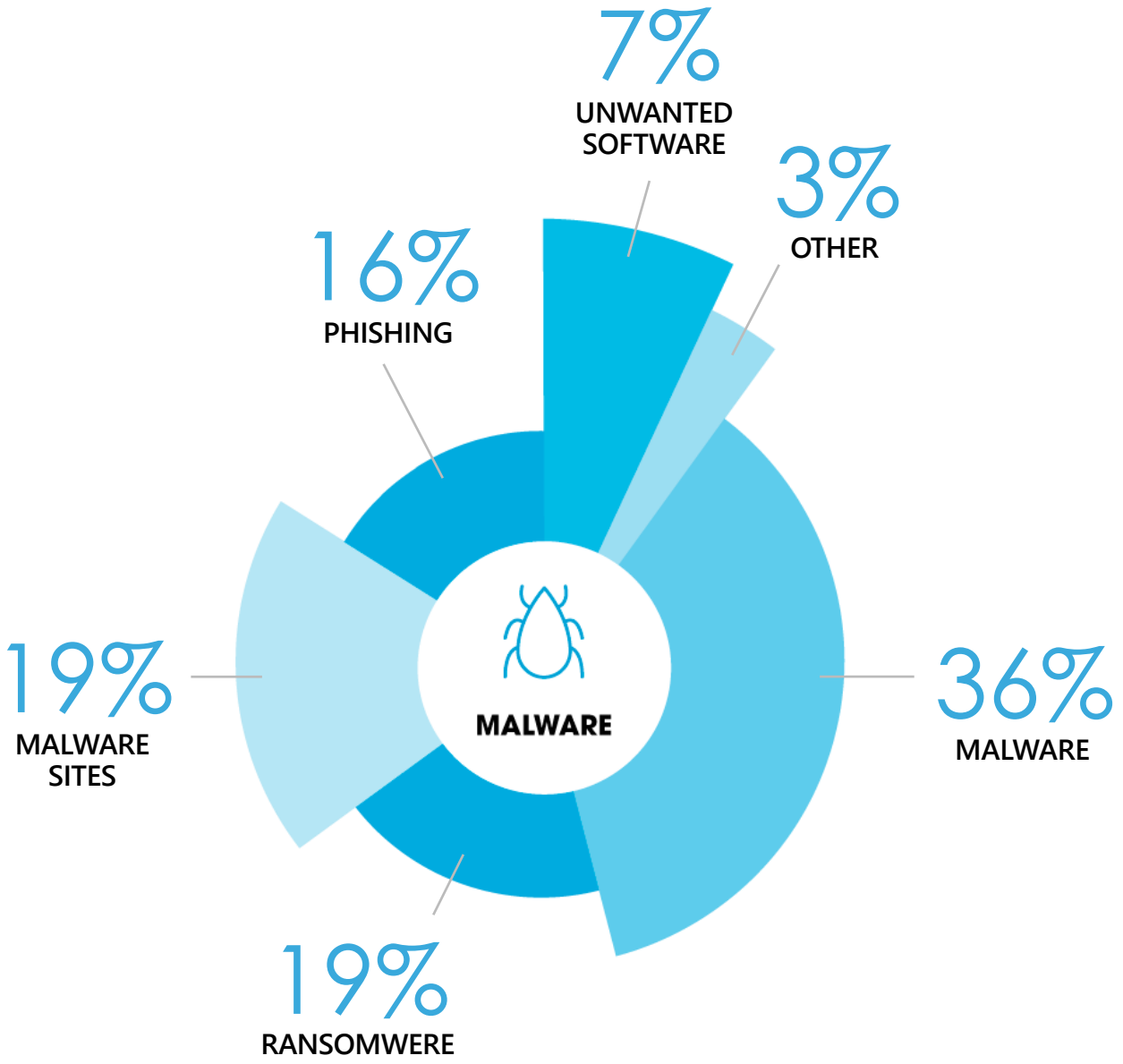
FROM DETECTION TO INCIDENT RESPONSE

- PanOptikon Security Appliance detects a suspicious condition and sends an Alert to the Certego Security Analytics Cloud
- Security Analytics Cloud enriches and classifies the Alert
- Classified Alerts are acknowledged by Certego SOC and are investigated using additional contextual information available on the Security Appliance
- Certego SOC validates the Alert and opens a ticket for a Cybersecurity Incident supporting and coordinating Response operations with the Customer



PANOPTIKON SERVICE REPORTS





certego

CUSTOMER USE CASE:

ITALIAN ASSET MANAGEMENT COMPANY

2014
CUSTOMER SINCE

INSTALLED IN ITALY, LUXEMBURG, IRELAND, TURKEY AND SWITZERLAND

DEPLOYMENT:

PANOPTIKON SECURITY APPLIANCE:

PANOPTIKON ENDPOINT AGENTS INSTALLED ON AWS AND GOOGLE CLOUD INSTANCES

PURCHASING DRIVER:

2.500
INTERNAL IP DEVICES

IMPROVE CYBER SECURITY AND OBTAIN COMPLIANCE TO SECTOR REGULATIONS

certego

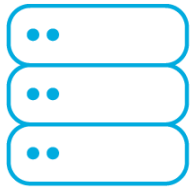
CUSTOMER USE CASE:

MAJOR EUROPEAN FASHION GROUP

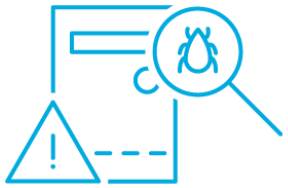
2015
CUSTOMER SINCE

INSTALLED IN ITALY, FRANCE, USA AND JAPAN

DEPLOYMENT:



PANOPTIKON SECURITY APPLIANCE:



PANOPTIKON ENDPOINT AGENTS INSTALLED ON CRITICAL SERVERS

PURCHASING DRIVER:

5.500
INTERNAL IP DEVICES

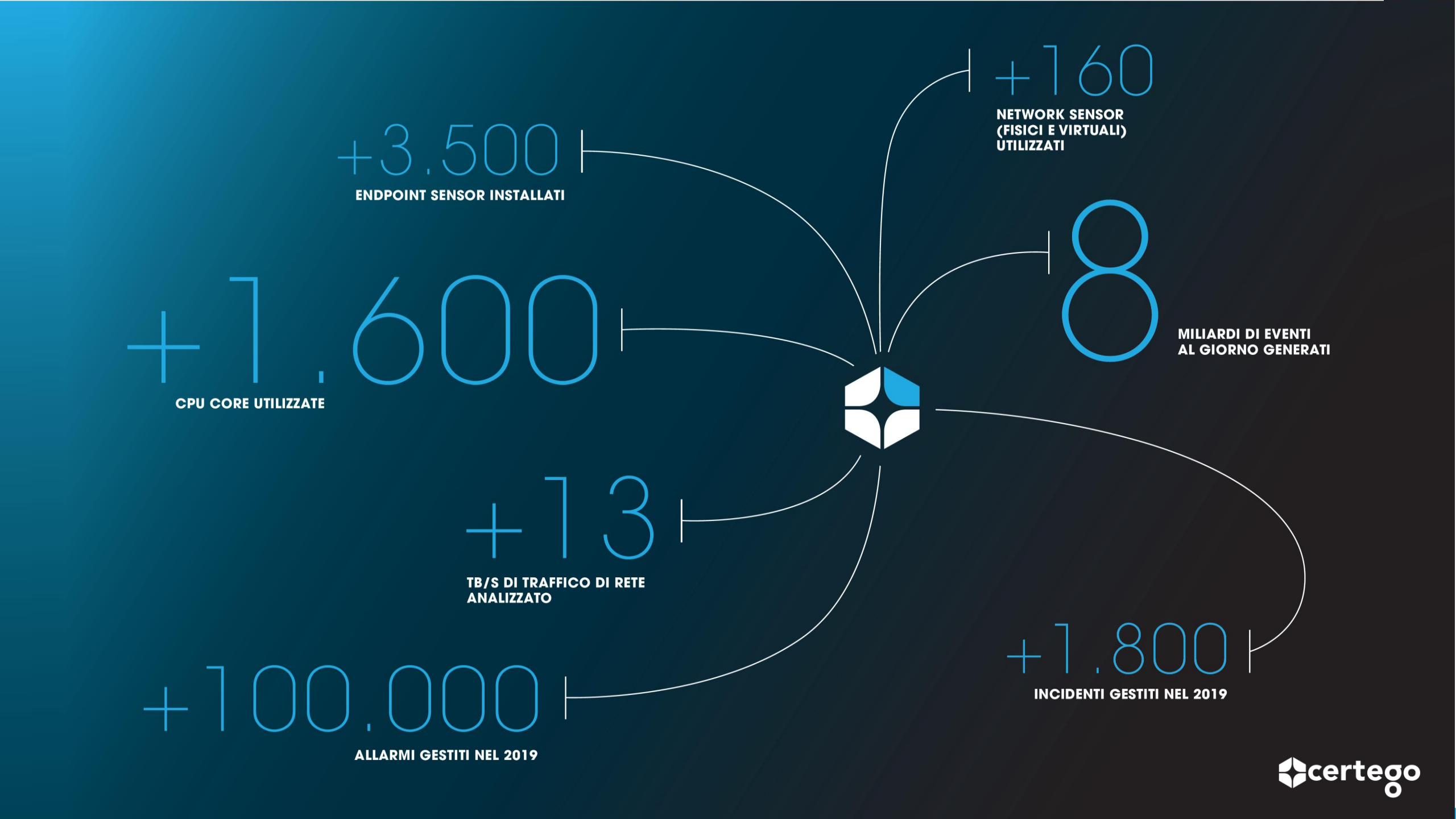
EXPERIENCED A MAJOR DATA BREACH PRIOR TO ENGAGING CERTEGO

certego

KNOWN AND TRUSTED

- ISO/IEC 27001:2017 since Feb. 2018
- ISO/IEC 9001:2015 since Feb. 2019
- Authorized User of "CERT" since Dec 2014
- FIRST.ORG Membership since Nov 2017
- EC3 Europol Supporting Partner since Apr. 2017
- Trusted Introducer: Listed since Jul. 2016, Accredited since Aug. 2019
- ENISA CSIRT Inventory
- Listed in Gartner Worldwide Threat Intelligence Services Competitive Landscape in 2015 and 2017 as Regional Player

certego


+160
NETWORK SENSOR (FISICI E VIRTUALI) UTILIZZATI
+3.500
ENDPOINT SENSOR INSTALLATI
8
MILIARDI DI EVENTI AL GIORNO GENERATI
+1.600
CPU CORE UTILIZZATE
+13
TB/S DI TRAFFICO DI RETE ANALIZZATO
+1.800
INCIDENTI GESTITI NEL 2019
+100.000
ALLARMI GESTITI NEL 2019
certego

CERTEGO S.R.L.

Via F.Lamborghini, 81 - Modena (MO) - Italy
+39 059 7353333 - www.certego.net
info@certego.net