Security Summit Treviso

Panda Security

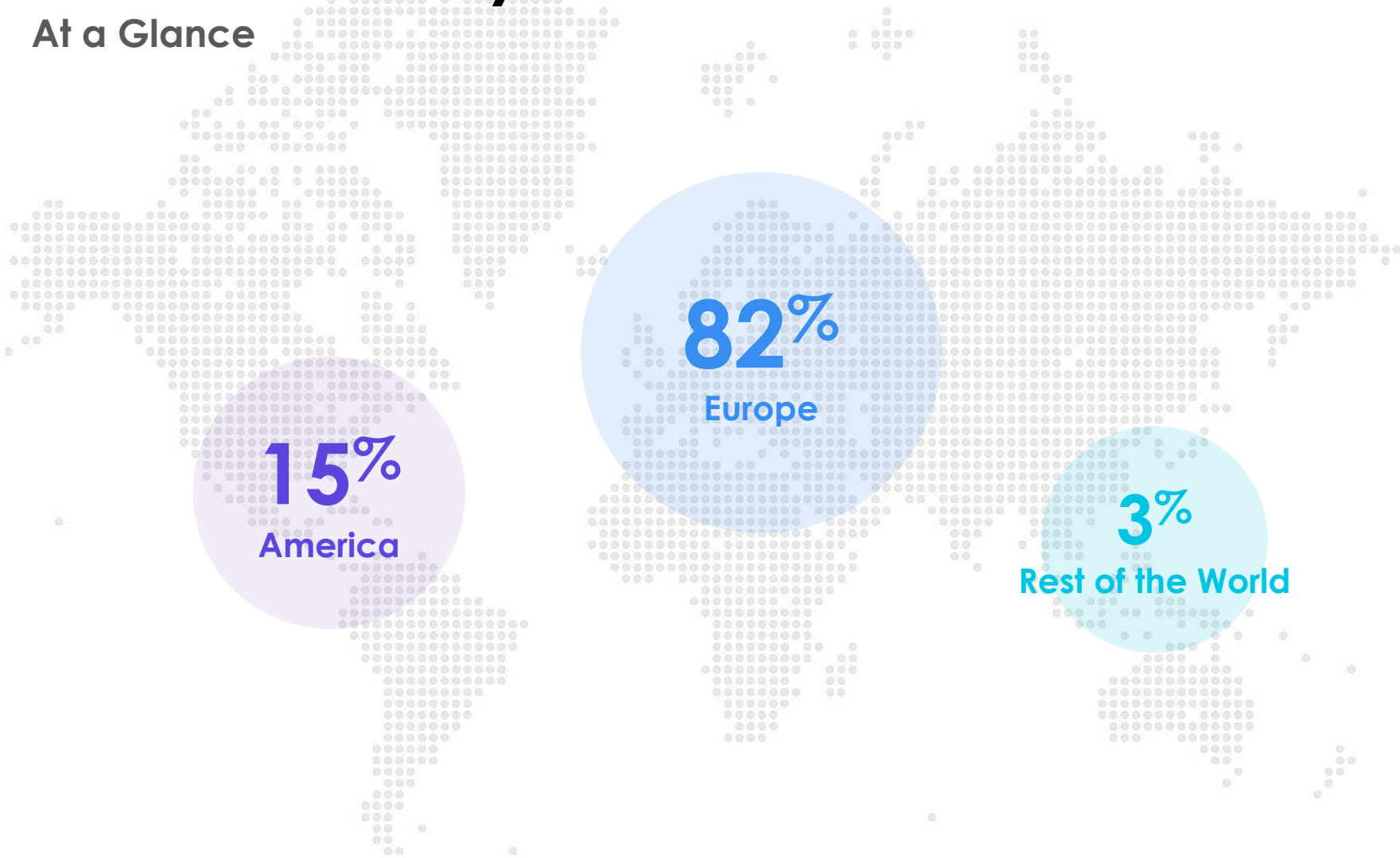
Diego Pretini
Territory Manager North

panda

pandasecurity.com

Panda Security

At a Glance



1990
Fundation

+180
Distribution countries

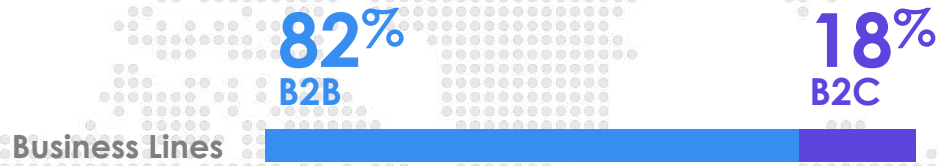
16
Subsidiaries

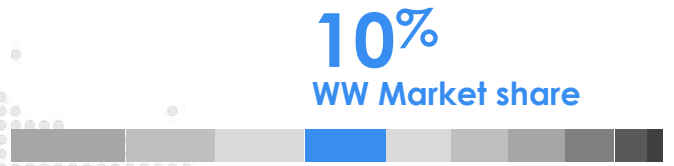
36
Country Partners

+550
Employees

Panda Security

Our Business



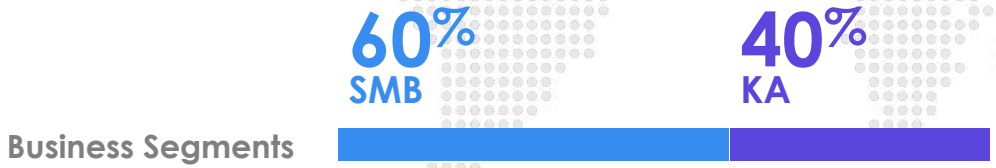


4th
World position

The Largest European

Next-gen Endpoint

Security Company



State of the Cybersecurity

More Attacks, and More Complex

#1. The increasing sophistication of cyber-attacks

Malware

Executable files
Fileless threats

Exploits

Malicious code-embedded
Script-based attacks

Insiders

Improper use of credentials
Data loss

Hacking Attacks

Lateral movement
Coordinated attacks

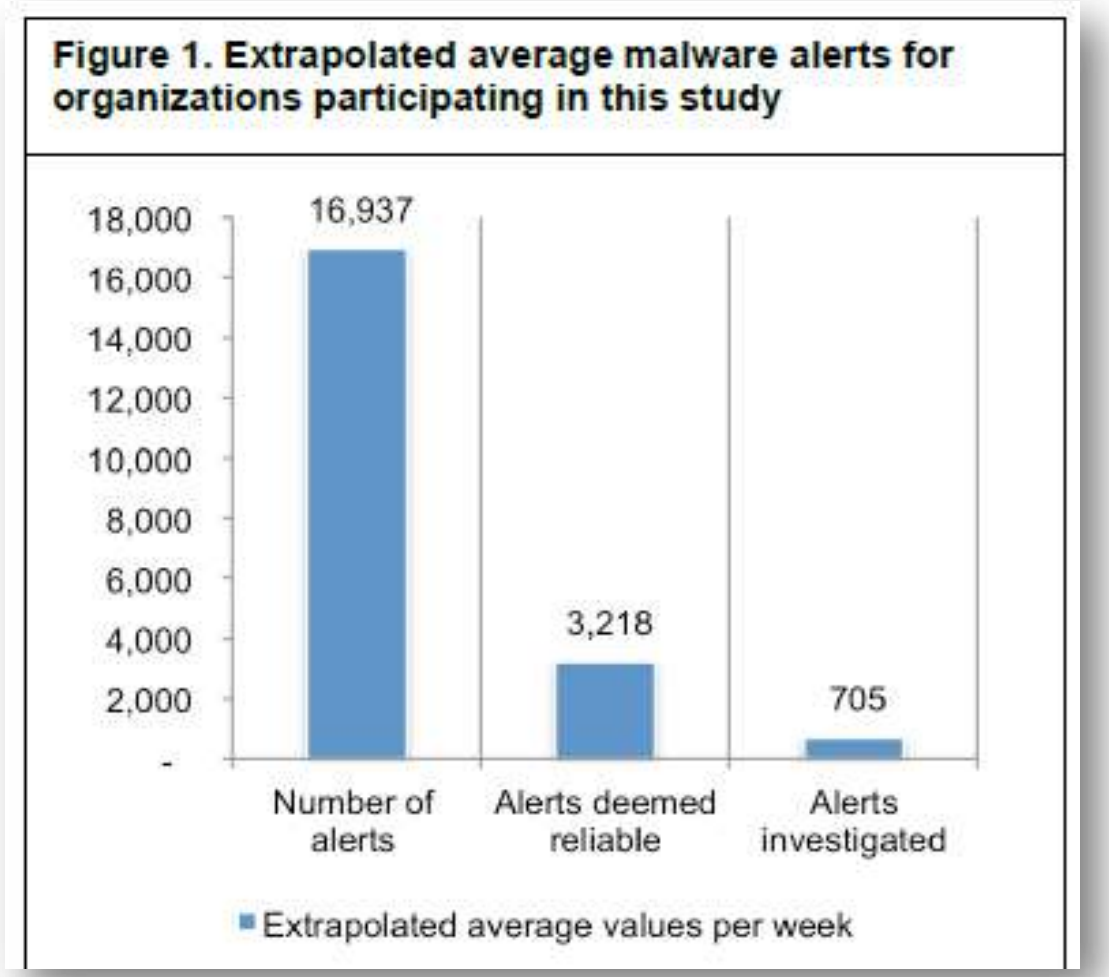
#6. Security solutions delegate. Unchecked Risk Alerts

Only 4% of alerts are ever investigated.

"Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence"

"It costs organizations an average of $1.27 million annually in time wasted responding to erroneous or inaccurate malware alerts"

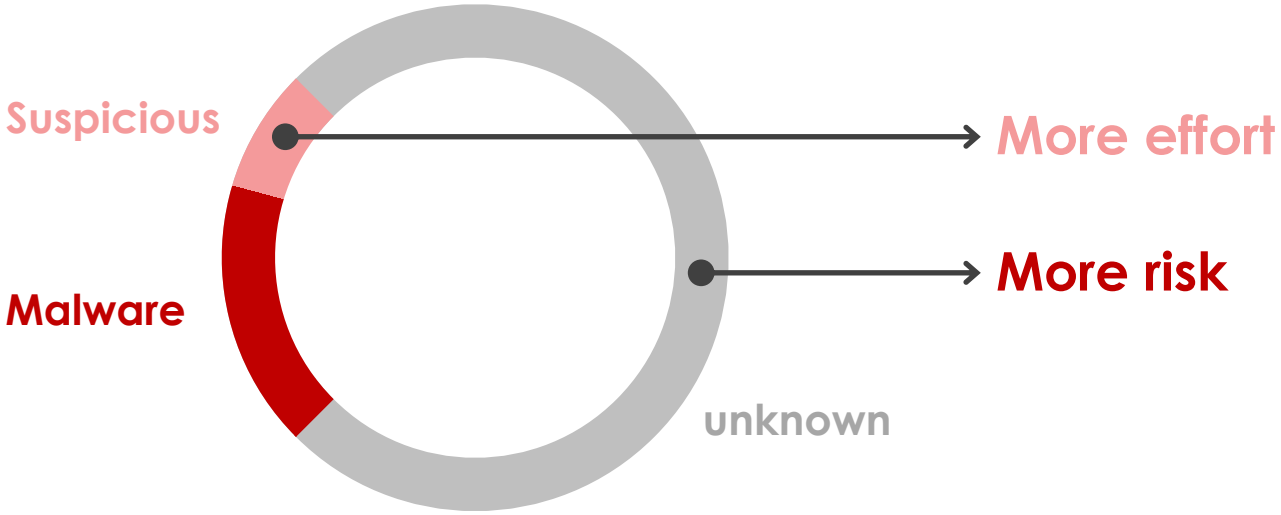
Source: EMA



Adaptive Defense 360, A new security model

EPP + EDR, Managed services-as-features on a single cloud-first architecture and a single lightweight agent

Il modello corrente…



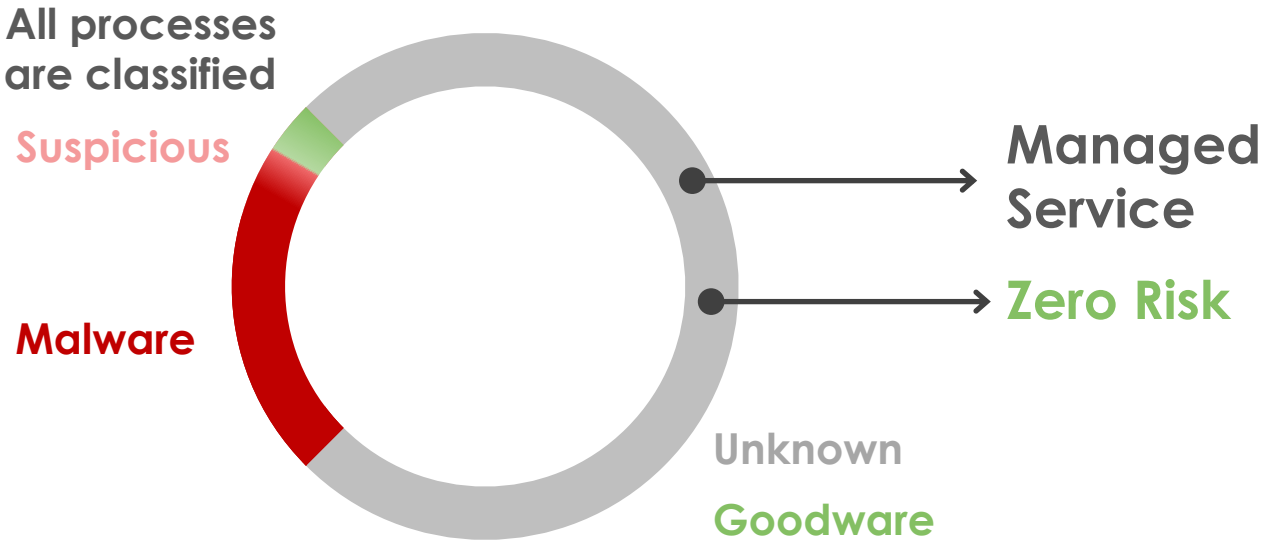
Le attività sospette devono essere investigate dal utente.
Lo sconosciuto non viene fermato.

…è basato sul **mero rilevamento dei processi malevoli noti**, questo significa:

- Tutte le attivita sospette devono essere investigate case-by-case.
- **Tutti I processi sconosciuti sono "concessi".** Ecco perchè gli hackers possono aggirare le protezioni così facilmente e avere percentuali di successo cosi elevate.

L’approccio Panda Adaptive Defense

Classificazione del 100% dei processi grazie ad un servizio gestito e Real-time visibility della telemetria delle macchine



Basato sulla **classificazione di tutti i processi eseguiti sul vostro** network.

- **Ogni azione di ogni programma è monitorata and analizzata in real time.**
- **Ogni comportamento è verificato dai managed service.** L’administrator non deve fare nessun tipo di indagine.

Massimo livello di protezione, meno impegno, zero rischi.

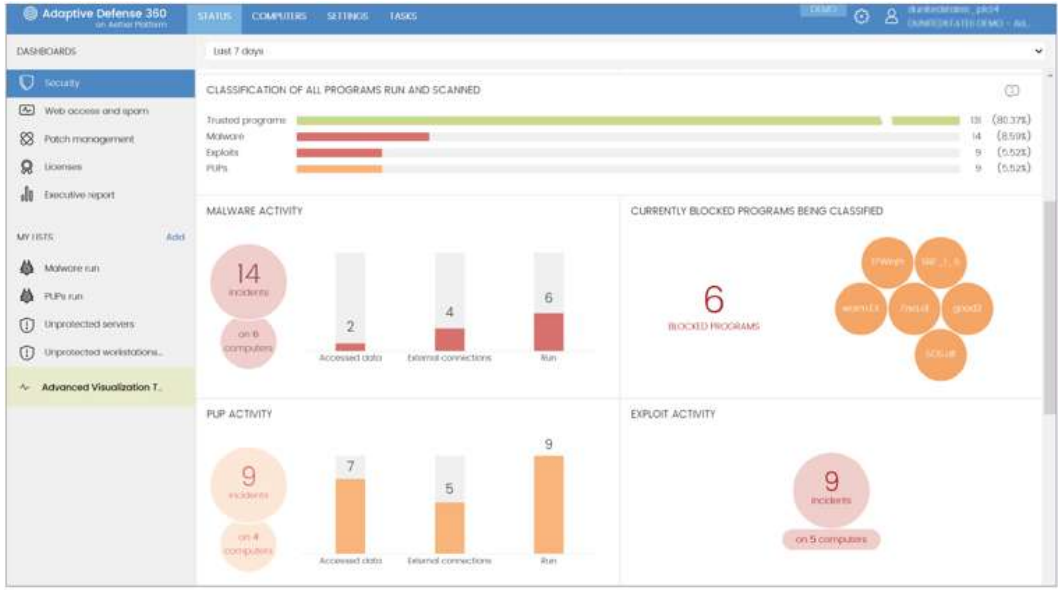
100% Attestation Service

Panda Adaptive Defense 360

Panda Adaptive Defense 360 is a cloud-based endpoint cybersecurity solution that **automates the prevention, detection and remediation** tasks, drastically reducing the **attack surface** at the endpoints.

It combines a **full-stack of EPP** and **EDR capabilities** in a single light agent. On top of that, two unique **Managed Services-as-Features**, included in the solution:

- 100% Attestation Service
- Threat Hunting and Investigation Service



Prevention, Detection and Response

In a single lightweight agent. Real-Time Visibility of all endpoint activity

100% Attestation service

Denies unknow process execution until classified by ML/Experts in near real-time. Max. prevention & Detection

Threat Hunting and Investigation Service

Led by Panda Security and MSSP' threat hunters. It discover new malwareless threats Techniques

Containement, Response. Attack surface reduction

It automates containment, remediation and Forensics, enabling actions to reduce the attack surface

Add-on: Panda Advanced Reporting Tool

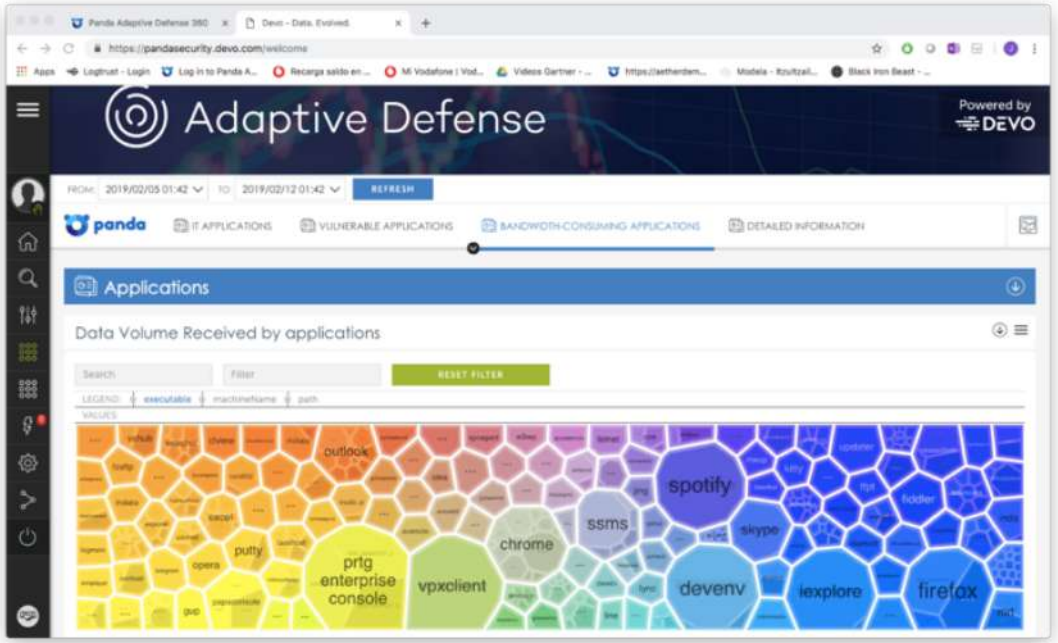
From data to actionable IT and security insights

Threat control: Determining the origin of security threats and applying security measures to prevent future attacks.

Manage access: Implementing more restrictive policies to access critical business information.

Monitor and detect: misuse of corporate resources that may have an impact on business and employee performance.

Correcting employee behavior that is not in line with the usage policies defined.



This module aggregates all the data gathered, correlating and graphically presenting it in real time to offer granular visibility into any event that takes place on the network.

The Advanced Reporting Tool dashboards include key indicators, searches and preset alerts across three areas:

- **Security incidents.**
- **Access to critical information.**
- **Network resources and applications used.**

Gartner Peer Insights Customers' Choice 2019

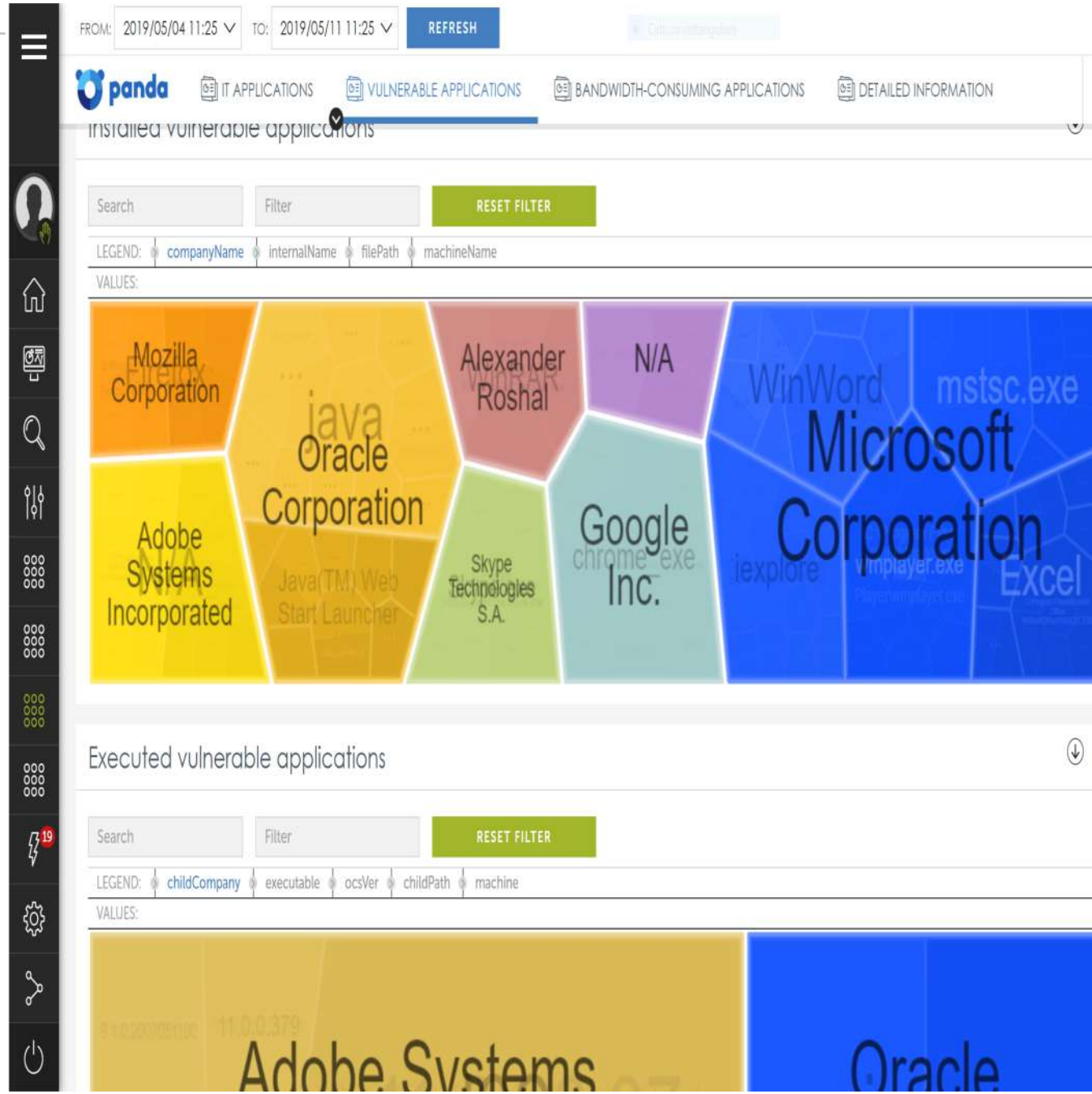
"By far the best, among all other EPP & EDR that I tested and can withstand direct or targeted attacks. No Antivirus or EDR and EPP solutions can offer 100% but, this is the closest."

Infrastructure and Operations. Education. Gov't/PS/ED <5,000 Employees

"Quite Better Than Other EDRs. AD is a powerful tool and the advanced console integrated with ART is very useful. Panda is able to block and classify different malware and to make the user feel safe."

Security and Risk Management. Communications. Gov't/PS/ED 50,000 + Employees


LulzSecITA
@LulzSec_ITA
Following
Ecco quello che non ci saremmo mai aspettati! #GDPR #GarantePrivacy garanteprivacy.it: privatebin.net/?c6df6a54929ff ... chi lo sa.. fin dove possiamo arrivare? #StayTuned #JustForLulz
FURFANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
Come evidenziato da Matteo Flora e confermato da Fabrizio Carimati, il sito del Garante utilizza una versione di Liferay - la versione 7.0, quando attualmente siamo alla 7.1 - dove dal 2018 sono note alcune vulnerabilità che ne minano la sicurezza. Quello di LulzSecITA, e forse con l'aiuto di Anonymous, potrebbe essere solo l'inizio delle pubblicazioni del materiale ottenuto dal sito Garanteprivacy.it.


FROM: 2019/05/04 11:25
TO: 2019/05/11 11:25
REFRESH
panda
IT APPLICATIONS
VULNERABLE APPLICATIONS
BANDWIDTH-CONSUMING APPLICATIONS
DETAILED INFORMATION
Search
Filter
RESET FILTER
LEGEND: companyName internalName filePath machineName
VALUES:
Mozilla Corporation
java
Oracle Corporation
Alexander Roshal
N/A
Adobe Systems Incorporated
Skype Technologies S.A.
Google Inc.
WinWord
mstsc.exe
Microsoft Corporation
iexplore
Excel
Executed vulnerable applications
Search
Filter
RESET FILTER
LEGEND: childCompany executable ocsVer childPath machine
VALUES:
Adobe Systems
Oracle


Reinventing
Cybersecurity.
panda
pandasecurity.com