

**FINIX**

*Technology  
Solutions*

**Nuovi strumenti per  
proteggere gli end point dalle  
minacce informatiche:**

**La soluzione  
Morphisec**

**FINIX**  
TECHNOLOGY SOLUTIONS

EXCLUSIVE  
ITALY FOR  
**FUJITSU**

# La situazione italiana\*

90%

delle imprese NON ha specialisti in sicurezza informatica

73%

NON ha implementato meccanismi di consapevolezza per i propri dipendenti

45%

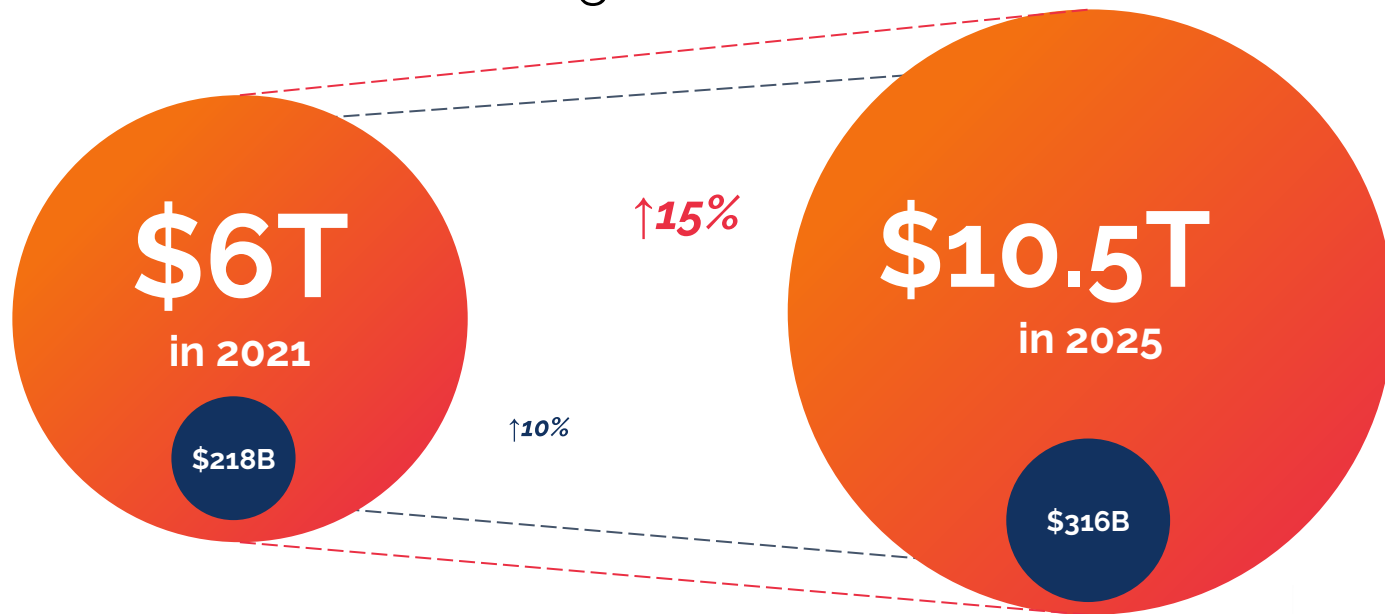
NON ha un SOC (Security Operations Center) per rilevare e rispondere a un attacco informatico

L'**Agenzia per la cybersicurezza nazionale** raccomanda di "**procedere** urgentemente **ad un'analisi del rischio** derivante dalle soluzioni di sicurezza informatica utilizzate ... in particolare la **sicurezza dei dispositivi** (endpoint security), ivi compresi applicativi **antivirus, antimalware ed endpoint detection and response** (Edr)"

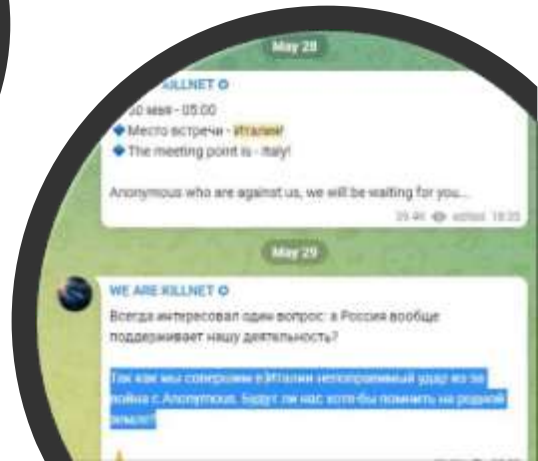
*\*Secondo un'indagine di Minsait, società di Indra leader nella consulenza negli ambiti della Digital Transformation e dell'Information Technology*

# Cosa ci attende in futuro

- Gli investimenti in infrastrutture di cyber security sono in aumento, tuttavia, la criminalità informatica è dilagante nonostante l'aumento degli investimenti



# Gli attacchi sono sempre in prima pagina



# Se le soluzioni esistenti funzionano, allora perché avvengono violazioni che infliggono così tanti danni?



**Si tratta di attacchi sconosciuti!**

- Ransomware
- New malware
- Varianti di attacchi già noti
- Vulnerabilità mai aggiornate





*FINIX Technology Solutions*

# La soluzione Morphisec

**MORPHISEC** è una **piattaforma completa di prevenzione** degli endpoint

- **Migliora l'efficacia e l'usabilità** di EDR/XDR (se in uso)
- **FA prevention**, unica vera strategia di protezione dagli attacchi sconosciuti, rispetto ad altre soluzioni che fanno leva sulla detection e remediation (che richiede ore o settimane se non mesi)
- **Combina perfettamente la protezione tradizionale** basata sulla firma necessaria per la conformità GDPR **con la potenza della protezione avanzata** contro le minacce zero-day e fileless

# Cosa è la Moving Target Defense - MTD

Morphisec ha rivoluzionato la protezione degli endpoint con la sua tecnologia **Moving Target Defense**, che blocca istantaneamente e in modo deterministico gli attacchi.

**L'agent di Morphisec agisce sulle applicazione in esecuzione cambiandone la struttura della memoria e trasformandola da un'entità nota in un mappa sconosciuta.**

**A questo punto la minaccia, non trovando la struttura originale, non può eseguire l'attacco.**

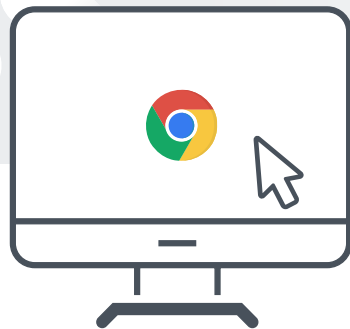
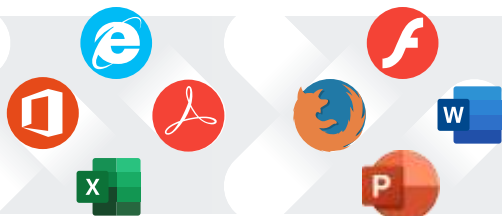
MTD nasconde le vulnerabilità e l'esposizione agli hacker, fermando ransomware, zero-days e altri attacchi evoluti





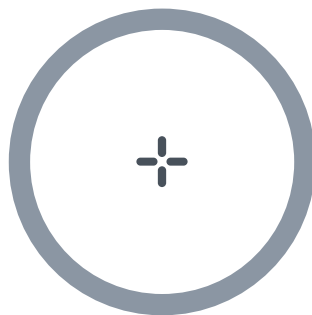
# Moving Target Defense

## Come funziona



Esecuzione di una applicazione su Endpoint

Struttura originaria della memoria



Statica, prevedibile e generalmente sfruttata per bypassare NGAV ed EDR

# Moving Target Defense

## Come funziona



# Morphisec e Microsoft Defender Antivirus

Member of  
Microsoft Intelligent  
Security Association



Rischio di violazioni mitigato

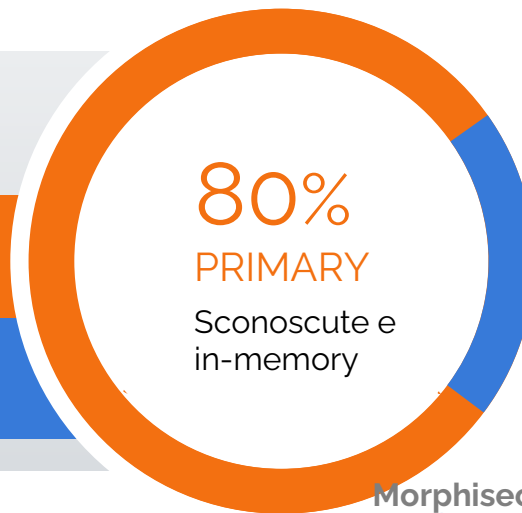
Windows 10



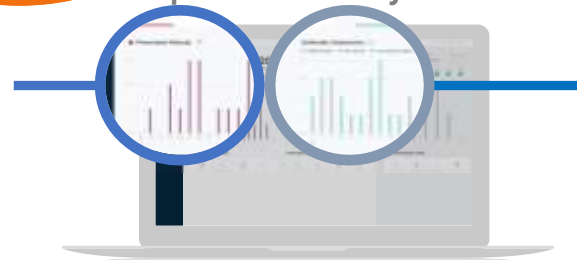
**MORPHISEC**  
Moving Target Defense



Defender AV



Morphisec Security Center



Lower  
TCO



Maggiore  
Efficienza  
Operativa

**FINIX Technology Solutions**

**FINIX**  
TECHNOLOGY SOLUTIONS

EXCLUSIVE  
ITALY FOR  
**FUJITSU**

# Morphisec e le altre soluzioni

Rischio di violazioni mitigato

Windows 10

 **MORPHISEC**  
Moving Target Defense

NGAV/EDR: McAfee, Symantec,  
TrendMicro, CrowdStrike...

80%

PRIMARY

Sconosciute e  
in-memory

RESIDUAL

Note &  
non-memory

Windows 7\*  
WS 2008\*

 **MORPHISEC**  
Moving Target Defense  
*Virtual Patching*

AV Compliance

\*Currently End of Life

Lower  
TCO



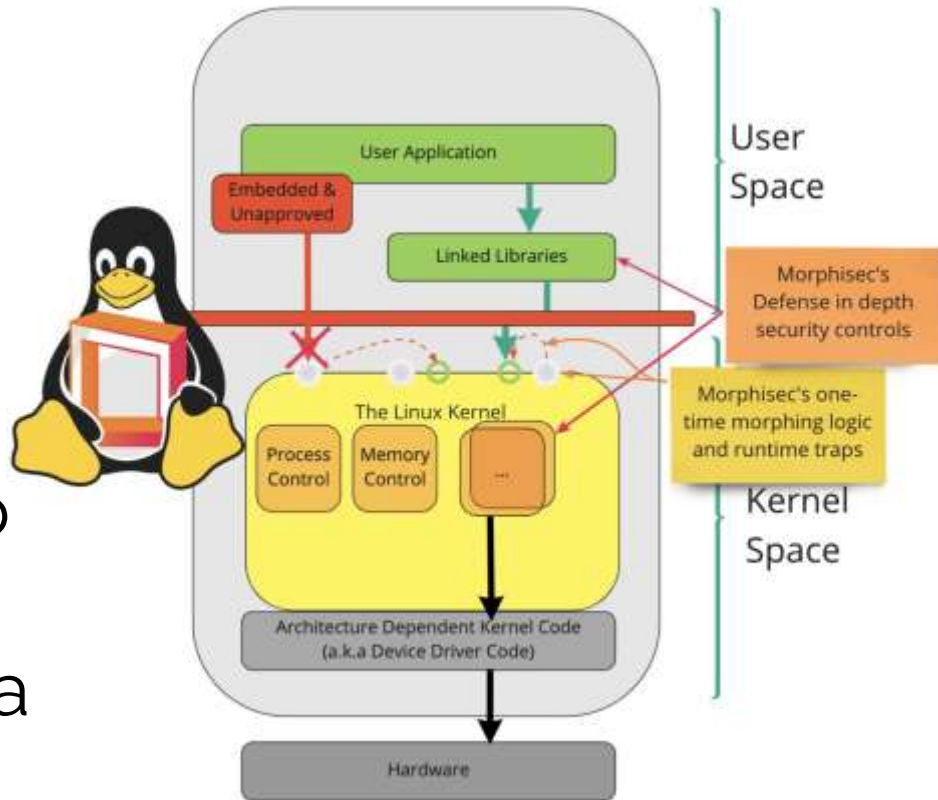
Maggiore  
Efficienza  
Operativa

**FINIX Technology Solutions**

**FINIX**  
TECHNOLOGY SOLUTIONS | EXCLUSIVE  
ITALY FOR  
**FUJITSU**

# La protezione Morphisec per Linux

La protezione di Morphisec avviene a livello di processo, identificato in modo univoco da un numero (PID), che gli viene assegnato all'atto della sua esecuzione.



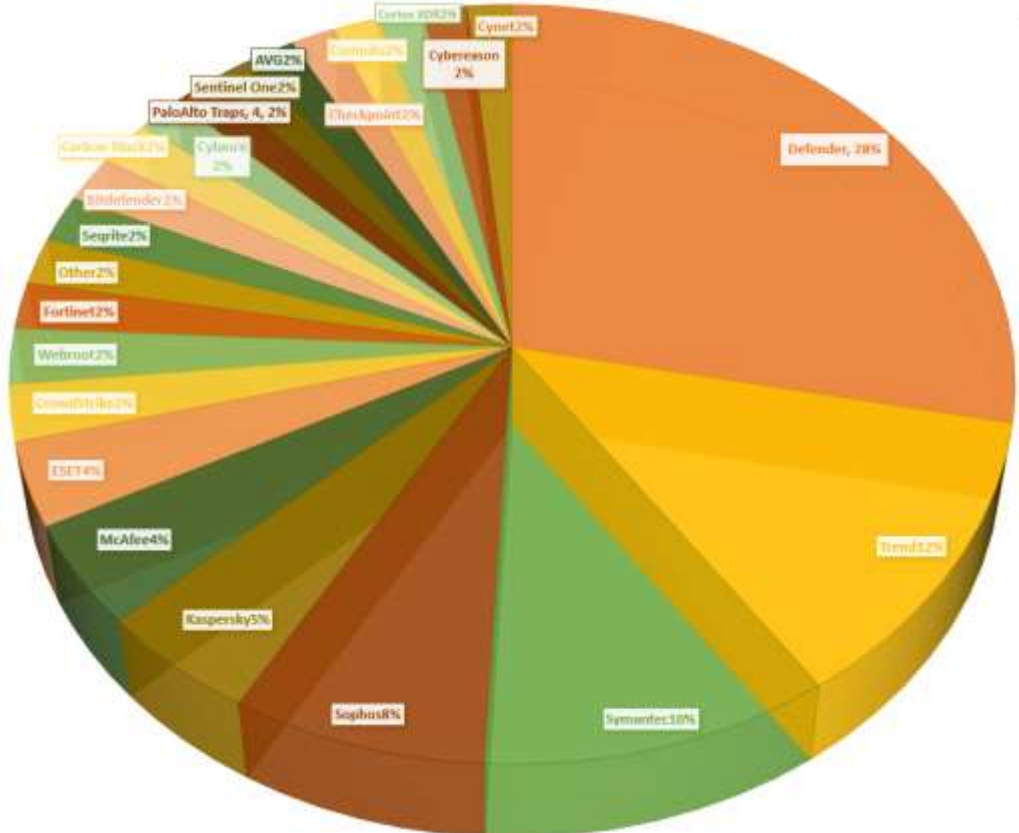
# Protezione Zero Days

APPLE ZERO-DAY del 2019 "BITPAYMER CAMPAIGN"  
Bug di iTunes per Windows



C:\Program Files (x86)\Apple Software Update

# Gli ambienti di lavoro di Morphisec



**ATTACK DETAILS**

12 JUN 2018 4:45 PM POWERPNT.EXE ATOM BOMBING EXPLOIT

Injecting Process: C:\Windows\System32\cmd.exe

Process Signature: Hyper-V Microsoft Corporation | log server: 0x00000000

Process File path: C:\Windows\System32\cmd.exe

Command Line

**DRPHISEC**

5 NOT PROTECTING

20 OFFLINE

50 COM

Prevented Attacks: 17

Defender Detections: 25

TOP ATTACKED APPS

TOP DETECTED APPS

**MORPHISEC**

DETECTIONS Last 30 Days

Detections on 6/17/2018

Users (2)	Category (2)	Operation System (2)	Subscribers (2)
Hyper-V Microsoft Corporation	Hyper-V	Windows 10	Robert
Hyper-V Microsoft Corporation	Hyper-V	Windows 10	Robert
Hyper-V Microsoft Corporation	Hyper-V	Windows 10	Robert

Dashboard



# Chi è Morphisec

Fondata nel  
Luglio 2014

Technologie provenienti da  
Ben Gurion University Cyber  
Research Labs

Detiene 8 Brevetti

Lancio nel  
Maggio 2016

110 Dipendenti  
(Boston: Sales, Marketing, CTO; Israel: R&D,  
Customer Success)





***Grazie!***

*Vuoi sapere di più su FINIX?*

*Visita il nostro sito*

