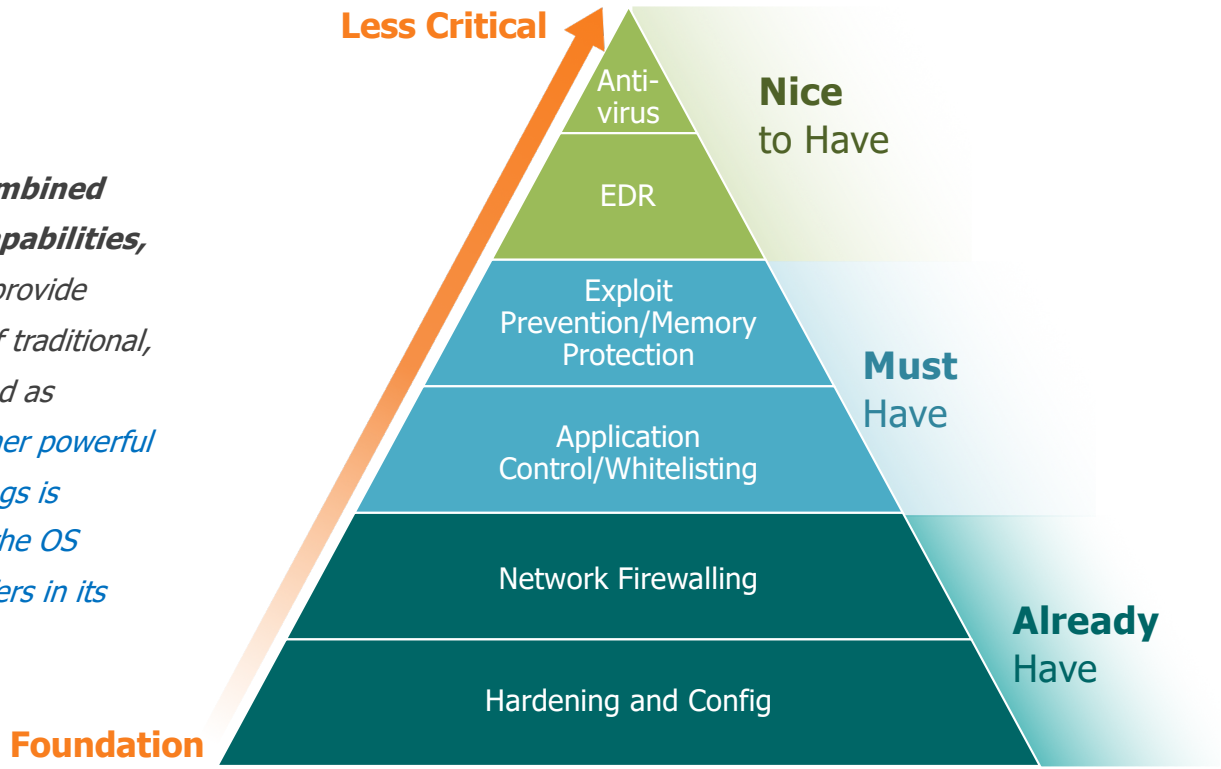
Cloud Server Workload Protection

Gartner

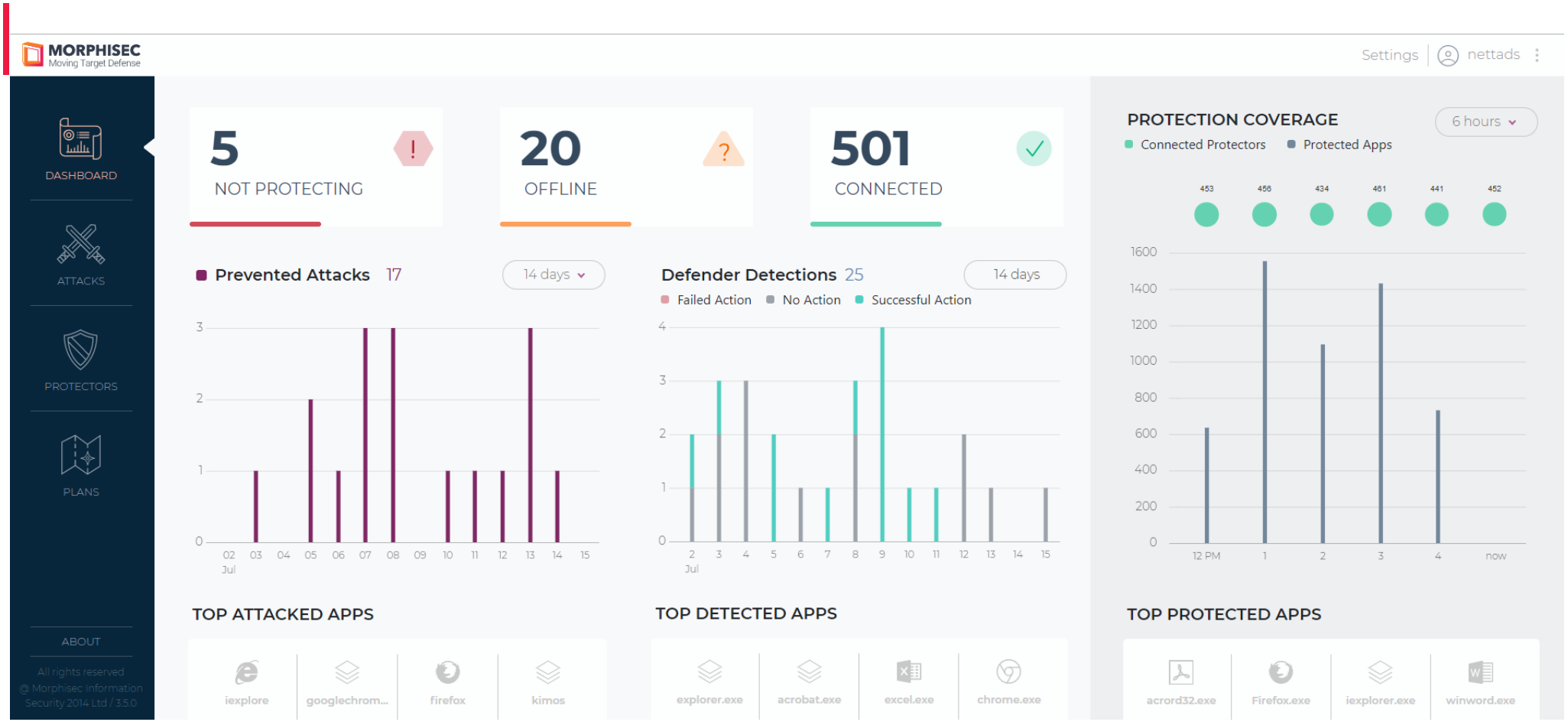
'**Exploit prevention/memory protection.**

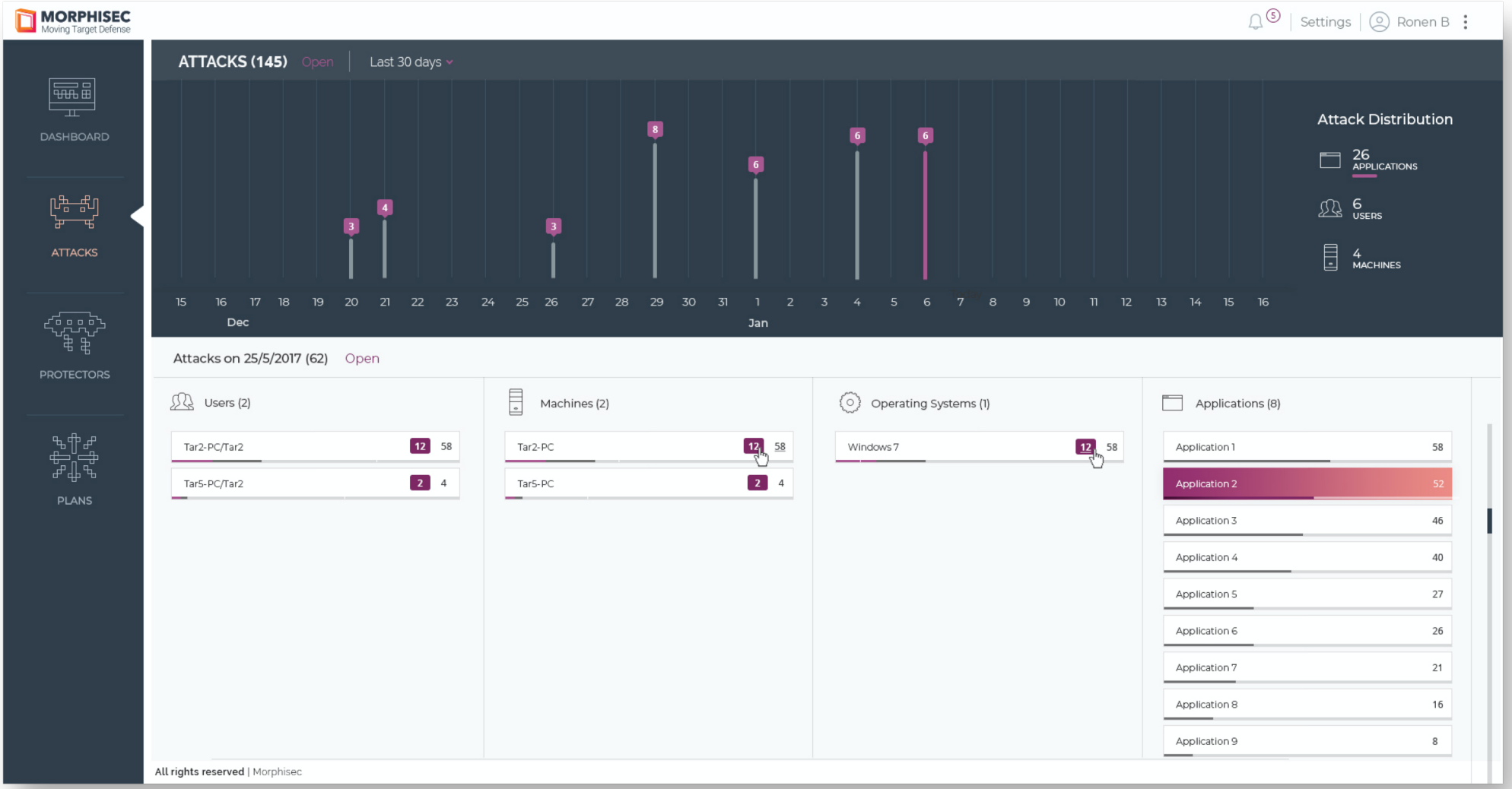
Application control solutions are fallible and ***must be combined with exploit prevention and memory protection capabilities,*** *Exploit prevention and memory protection solutions can provide broad protection against attacks, without the overhead of traditional, signature-based antivirus solutions. They can also be used as mitigating controls when patches are not available. Another powerful memory protection approach used by some CWPP offerings is referred to as* ***moving target defense*** *— randomizing the OS kernel, libraries and applications so that each system differs in its memory layout to prevent memory-based attacks."*

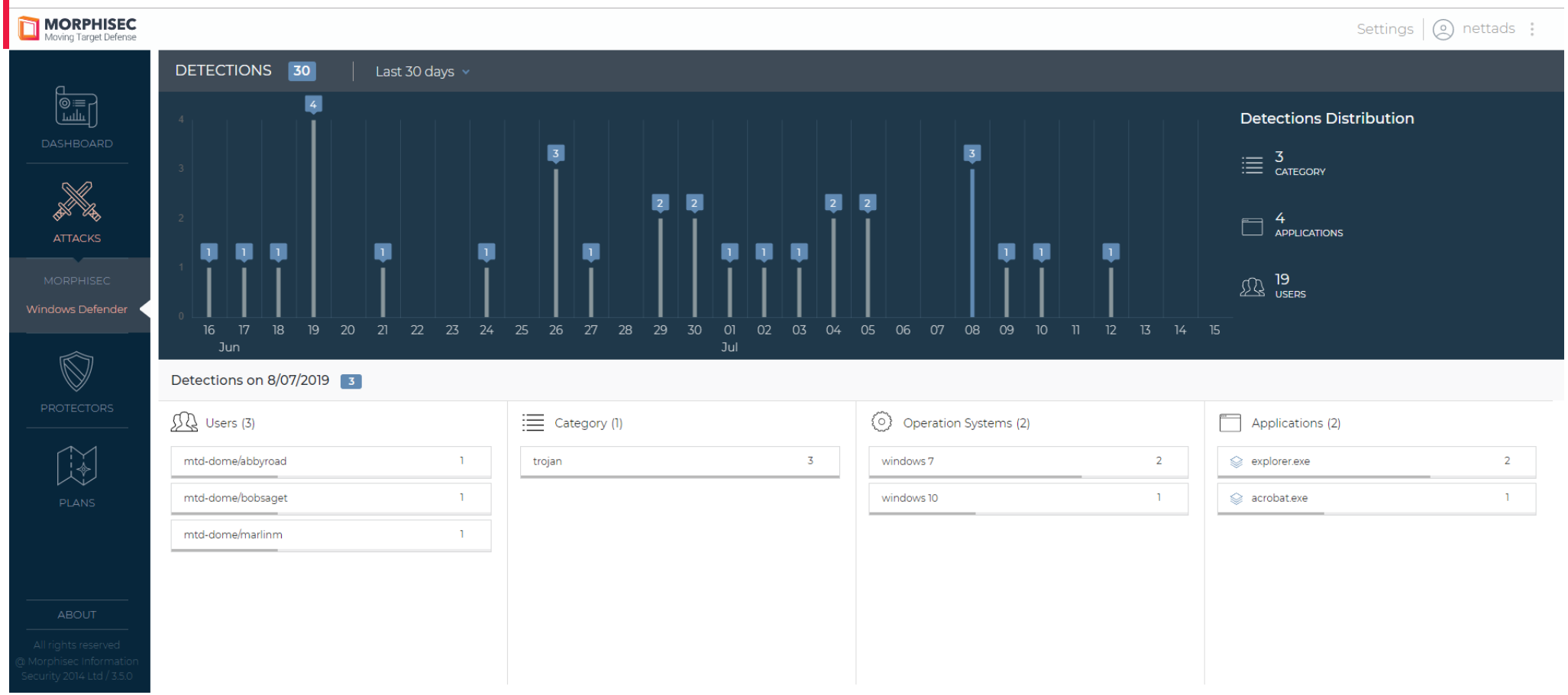


CWPP Controls Hierarchy

* Market Guide for Cloud Workload Protection Platforms, Endpoint and Server Security: Common Goals, Divergent Solutions


MORPHISEC
Moving Target Defense
Settings
nettads
DASHBOARD
ATTACKS
PROTECTORS
PLANS
ABOUT
All rights reserved
@ Morphisec Information Security 2014 Ltd / 3.5.0
5
NOT PROTECTING
20
OFFLINE
501
CONNECTED
Prevented Attacks 17
14 days
Defender Detections 25
14 days
Failed Action
No Action
Successful Action
PROTECTION COVERAGE
6 hours
Connected Protectors
Protected Apps
453
456
434
461
441
452
TOP ATTACKED APPS
iexplore
googlechrom...
firefox
kimos
TOP DETECTED APPS
explorer.exe
acrobat.exe
excel.exe
chrome.exe
TOP PROTECTED APPS
acrord32.exe
Firefox.exe
iexplorer.exe
winword.exe


MORPHISEC
Moving Target Defense
Settings
Ronen B
DASHBOARD
ATTACKS
PROTECTORS
PLANS
ATTACKS (145) Open
Last 30 days
Attack Distribution
26 APPLICATIONS
6 USERS
4 MACHINES
Dec
Jan
Attacks on 25/5/2017 (62) Open
Users (2)
Tar2-PC/Tar2 12 58
Tar5-PC/Tar2 2 4
Machines (2)
Tar2-PC 12 58
Tar5-PC 2 4
Operating Systems (1)
Windows 7 12 58
Applications (8)
Application 1 58
Application 2 52
Application 3 46
Application 4 40
Application 5 27
Application 6 26
Application 7 21
Application 8 16
Application 9 8
All rights reserved | Morphisec


MORPHISEC
Moving Target Defense
Settings
nettads
DASHBOARD
ATTACKS
MORPHISEC
Windows Defender
PROTECTORS
PLANS
ABOUT
All rights reserved
@ Morphisec Information Security 2014 Ltd / 3.5.0
DETECTIONS 30
Last 30 days
Jun
Jul
Detections Distribution
3 CATEGORY
4 APPLICATIONS
19 USERS
Detections on 8/07/2019 3
Users (3)
mtd-dome/abbyroad 1
mtd-dome/bobsaget 1
mtd-dome/marlinm 1
Category (1)
trojan 3
Operation Systems (2)
windows 7 2
windows 10 1
Applications (2)
explorer.exe 2
acrobat.exe 1

MORPHISEC
Moving Target Defense

Settings | Ronen B

DASHBOARD
ATTACKS
PROTECTORS
PLANS

← Back **ATTACK DETAILS**

Archive | Export | Attack Log

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

Demo / Robert

12 Jan 2018 / 9:10 AM — Robert - Excast win 10 - V23

03:40 PM — iexplorer.exe

03:41 PM — Outlook.exe

powershell.exe

04:45 PM — Powerpnt.exe

ATTACKED PROCESS - EXTENDED INFO

Injecting Process:

C://Windows//System32//wbem//WmiPrvSE.exe

Process Signature:

Signer: Microsoft Corporation

Signed on: 12Feb2017

Process File path:

C://Windows//System32//wbem//WmiPrvSE.exe

Command Line

Ecosystem and Technology Partners

SIEM/SOAR

Virtual Platforms

Technology Research

The Next Generation Cyber Infrastructure (NGCI) Apex Program

Challenges Defending Against Advance Threats

Status Quo AV, NGAV, and EDR		MORPHISEC Moving Target Defense
▪ Requires discovery ▪ After the fact	**Time**	▪ Instantaneous, early, and effortless
▪ Malware focus ▪ Poor at unknown attacks	**Vectors**	▪ Prevents evasive, unknown attacks ▪ Virtual patch
▪ Alerts ▪ Complexity	**Simplicity**	▪ Disables attack framework ▪ 'Set and forget' ▪ Time to value
▪ Cost burden on defender ▪ Endless escalation	**ROI**	▪ Shifts costs to attacker ▪ Low TCO ▪ Defense in Depth

Strategic Value Proposition

Security as Business Enabler

MTD

Prevent unknown and known attacks
End points and hybrid server workloads
Future-proof
Window 7 compliance

Rapid time to value
Simple operations
Reduced cost of stack
Empowers security teams

Operational continuity
User productivity

Risk Reduction → Operational Savings → Business Enablement

Rapid Customer Ramp

4,700,000

Protected Endpoints

Channels

GuidePoint Security – Leading Security Innovation
OPTIV
shi
orange
security by SECOM
VERINT

Financials

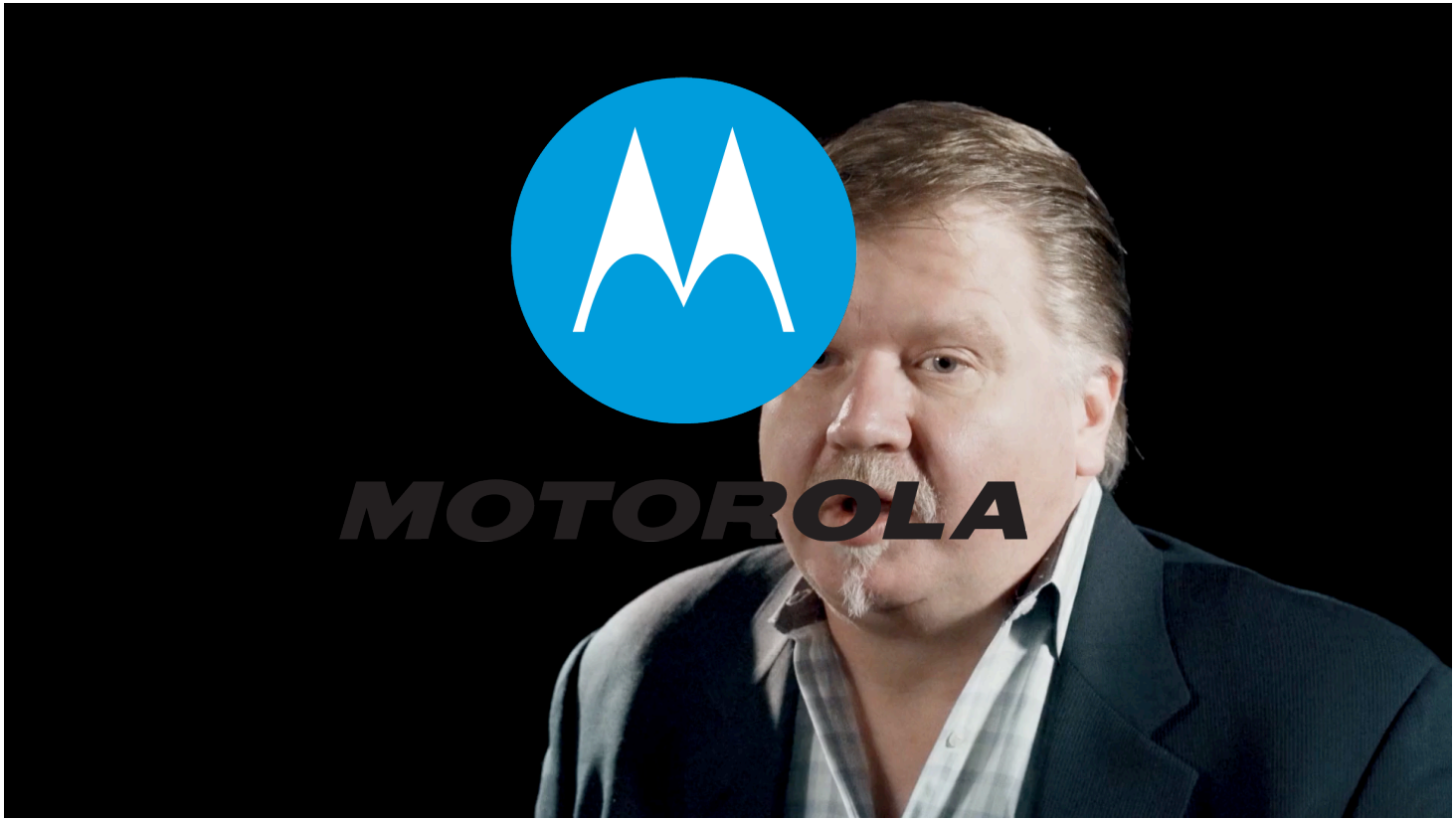
YES BANK
BlackRock
富邦銀行 Fubon Bank
BEA
Merrick Bank
GSA Capital
Leumi Card VISA

Manufacturing

ELEMENTIS Specialties
ESSAR
Radiall
RHEINMETALL GROUP
MOTOROLA
LAVA MOBILEPHONE
IMPERVA – Protecting the Data That Drives Business

Services

LOS ANGELES POLICE FEDERAL CREDIT UNION
PSA – The World's Port of Call
orange
Lagardère
Alegria
TRANS LINK
FREEMAN Health System
MAERSK
Ridgecrest Regional Hospital
CHOATE – Choate Hall & Stewart LLP


MOTOROLA

MORPHISEC

Moving Target Defense

Powerful Security.
Operationally Simple.

Gartner
Cool Vendor
2016

CITRIX Ready

Microsoft Partner
Virus Information Alliance

pwc
People's
Choice
Award
2016

Case Study
Freeman Health

- Deploy a solution able to protect against the "What you don't know" threat
- No impact to device performance
- Solution that does not interfere with existing desktop security strategy or tools
- Vendor must have a strong support structure with solid knowledge of the security world
- Solution must provide user with protection from doing the wrong thing
- Easy to deploy and manage

"The ROI of Morphisec is the ability to use resources to target other problems."

Skip Rollins, CIO

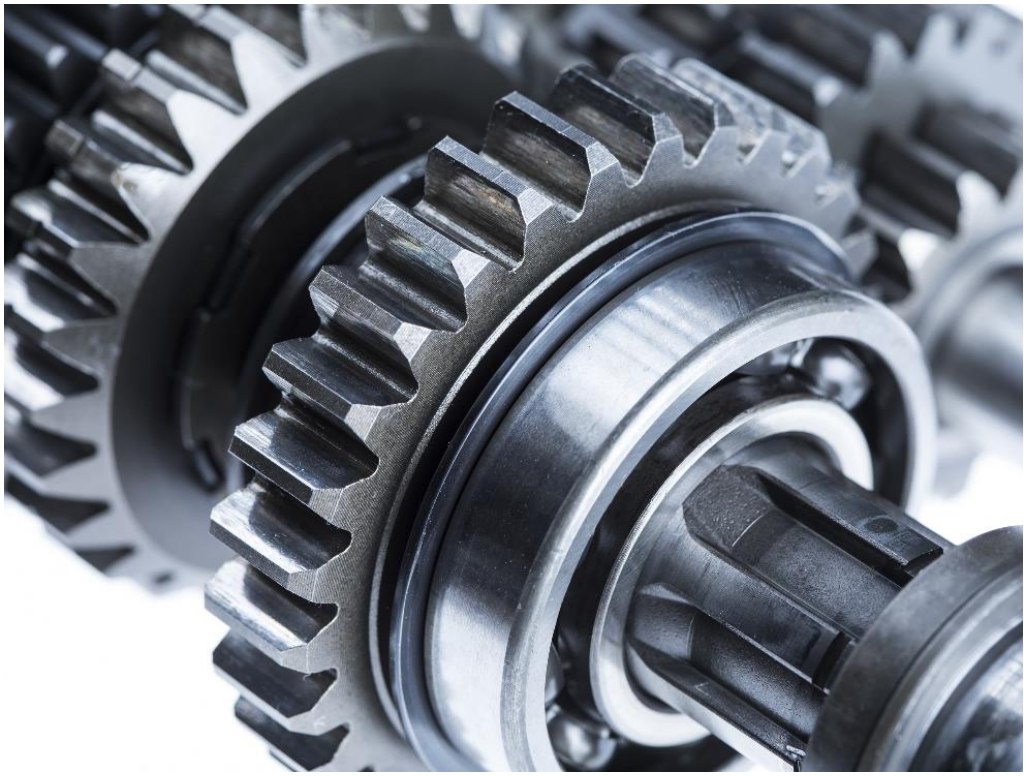
Case Study
Essar

- Needed ATP for all business units
- Lean security team
- Tested against highly advanced attacks
- 10,000 seats
- Simple to deploy and manage

"I was amazed at how easy Morphisec was to deploy and to operationalize, plus it delivers advanced threat protection, that evades signature-based tools. Morphisec enables us to focus on the critical patching initiatives around Windows, and covers the application-based vulnerabilities with Moving Target Defense."

Keyur Desai, CISO

Case Study
Manufacturing



- ATP required by BoD
- Lean security team
- Aversion to overhead
- CIO accelerated rollout
- 60 attacks / month
- 18,000 seats, < two hours per week

"I was amazed that we could roll out an entire new crucial defense layer that quickly and smoothly. I credit not just the ingenious simplicity of the software but also the high level of cooperation between my teams and Morphisec support and engineers."

CISO

Case Study
Global Tech Company

Situation

- Breach is unthinkable
- Need true prevention
- "Not one minute of analyst's time"
- We have "One-of-everything"
- Evaluated all options

Outcome

- Selected Morphisec
- Fast, easy deployment
- Stop 30 attacks per month
- < 2 hours per week on Morphisec
- Morphisec is a fixture of security program

"With Morphisec, we met our goal of securing our company against advanced attacks without adding staff resources, burdening security with false alerts or sacrificing performance."

Security Officer,
NASDAQ-listed Security Software Company

About Us

MORPHISEC
Moving Target Defense

Founded in
July 2014

Technology out of
Ben Gurion University Cyber Research Labs

9 Patents
in various stages

Product launched in
May 2016

100 Employees
(Boston: Sales, Marketing, CTO; Israel: R&D, Customer Success)

Funding
Backed by strategic and financial investors

MORPHISEC

Moving Target Defense

info@morphisec.com | www.morphisec.com