Prevention
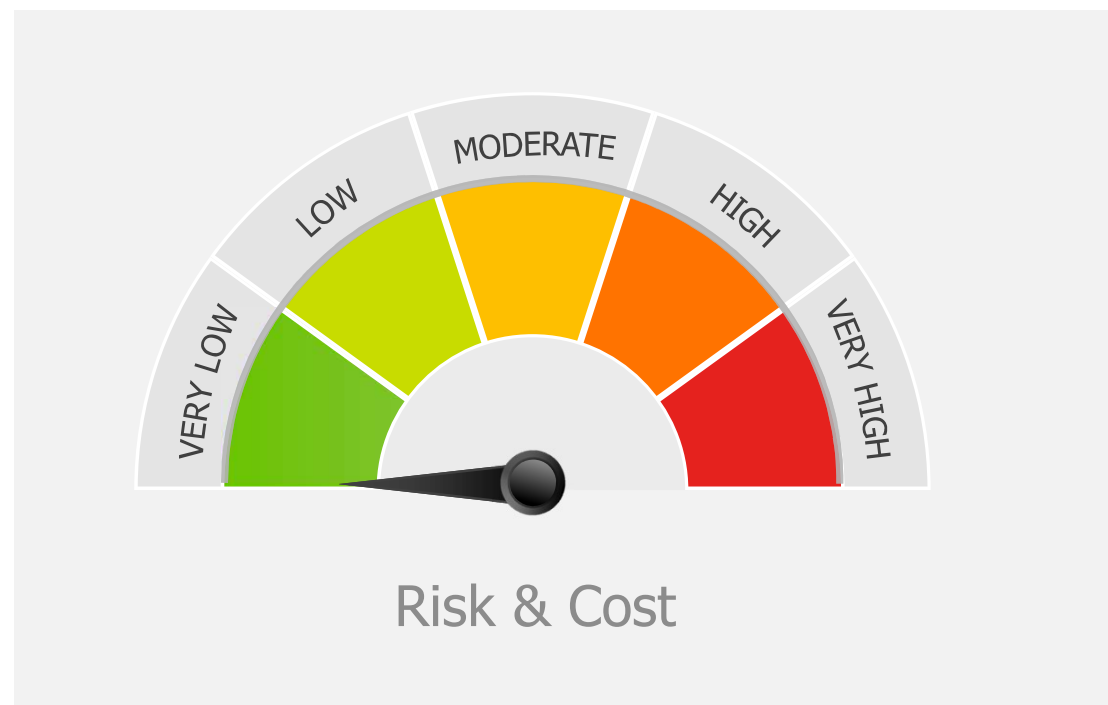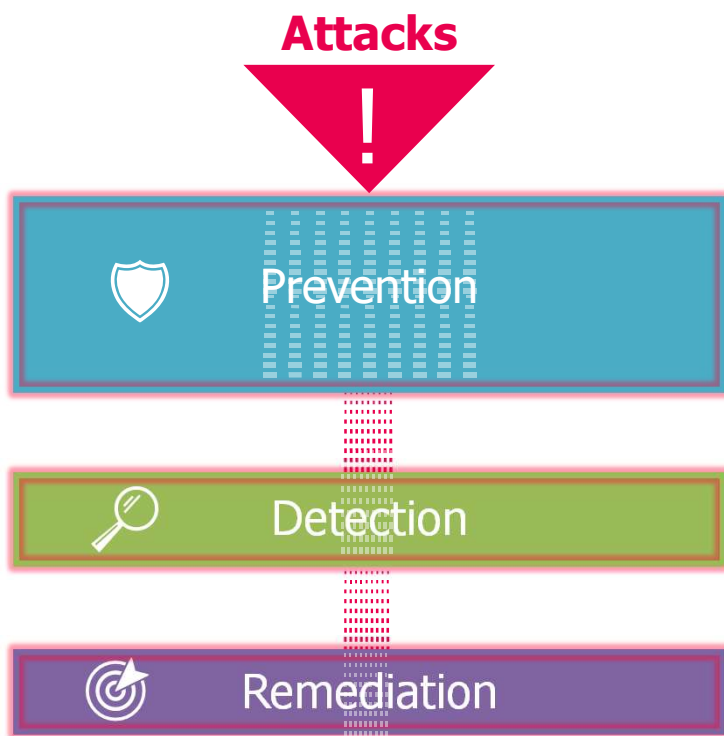# The Most Strategic Element in the Security Architecture

IDEAL
architecture

MORPHISEC

Prevention
The Most Strategic Element in the Security Architecture

EXISTING
architecture

Attacks

!

Prevention

Detection
Behavioral, AI, Sandbox, Knowledge Based

Remediation

LOW

MODERATE

HIGH

VERY LOW
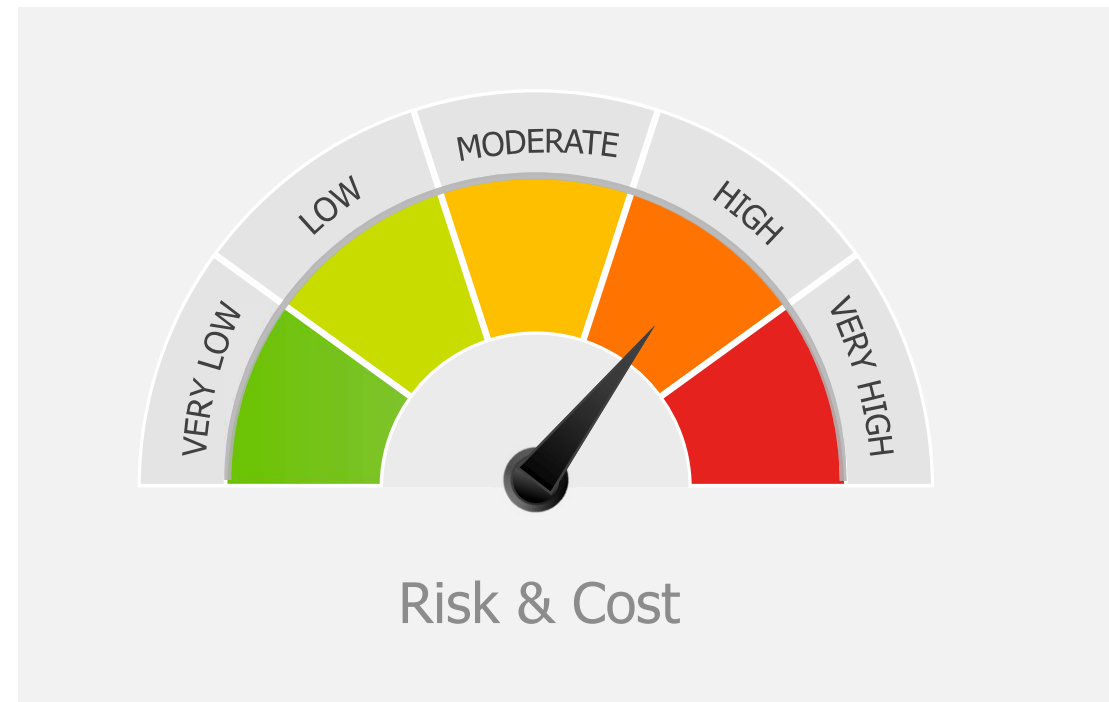
VERY HIGH

Risk & Cost

MORPHISEC

Prevention
The Most Strategic Element in the Security Architecture

MORPHISEC
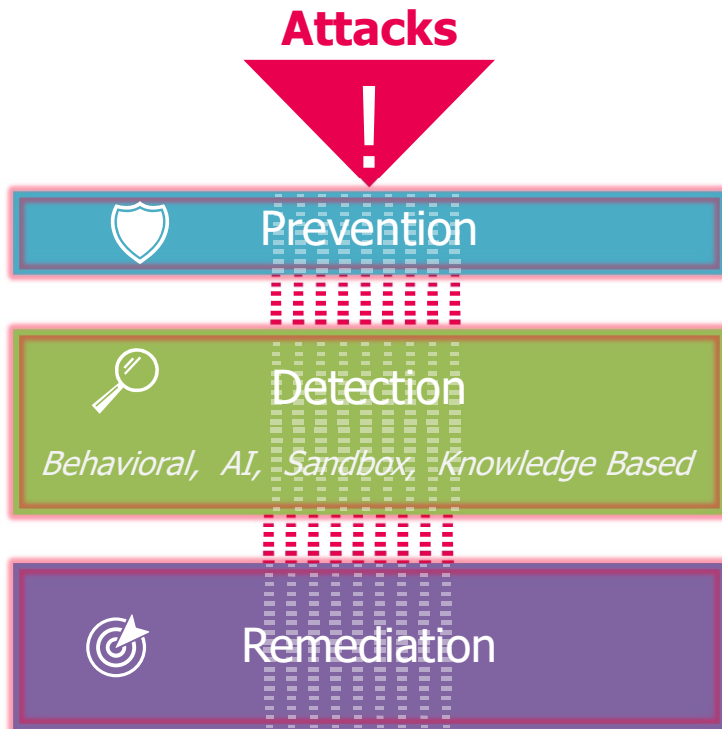architecture

Attacks

!

Prevention
Real Time, Deterministic,
No knowledge

Detection

Remediation

LOW

MODERATE

HIGH

VERY LOW

VERY HIGH

Risk & Cost
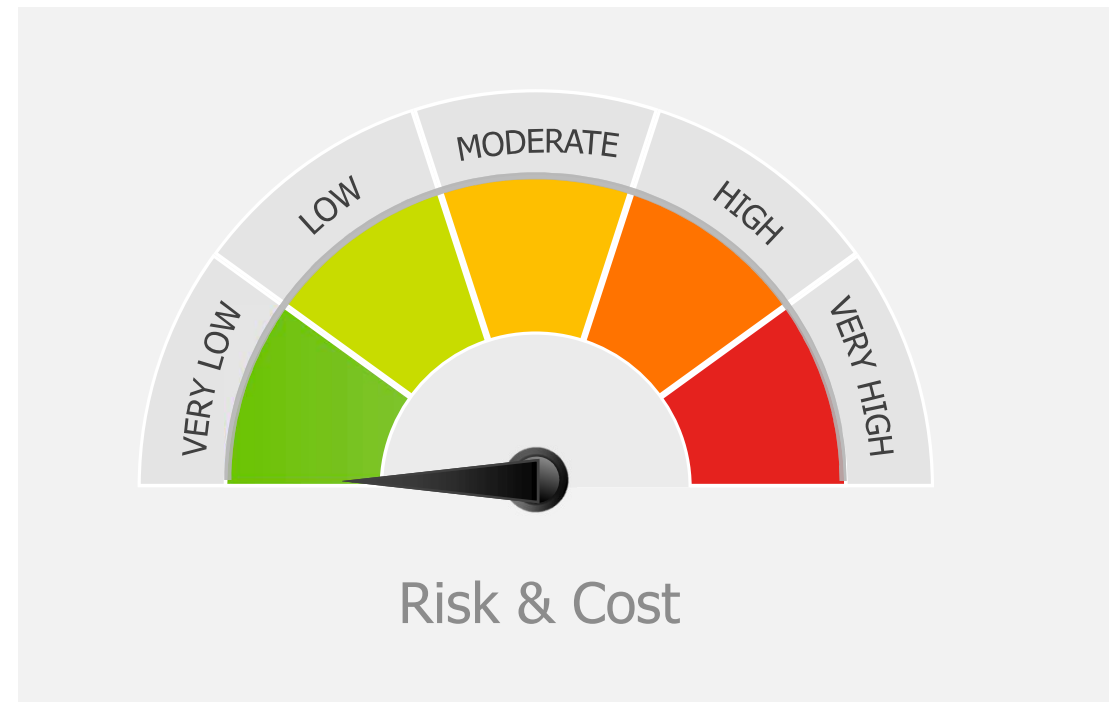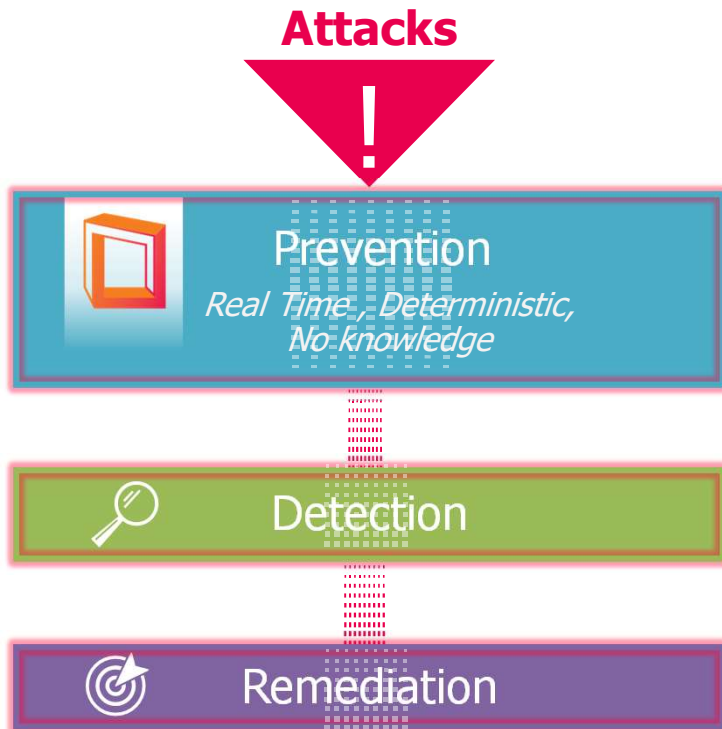
MORPHISEC

Moving Target Defense

Attacker's Advantage:
Predictable static targets

Defender's Advantage:
Unpredictable moving targets

A *Fundamental Change*
in Cyber Defense

EXISTING SOLUTIONS
Reactive Detection

MORPHISEC
Proactive Prevention

Memory
A Mission Critical Battlefield

ADVANCED
Attacks
!

ORGANIZATION

Network

FW / GW / IPS / IDS

Data Center

Endpoint

AV

MEMORY
App/OS Vulnerabilities

MORPHISEC
Moving Target Defense

DISK
Malware

Denial-of-Attack stops attacks at initial penetration stage, before malware downloaded from C2C or if malware already persistent and tries to evade

Command & Control Server
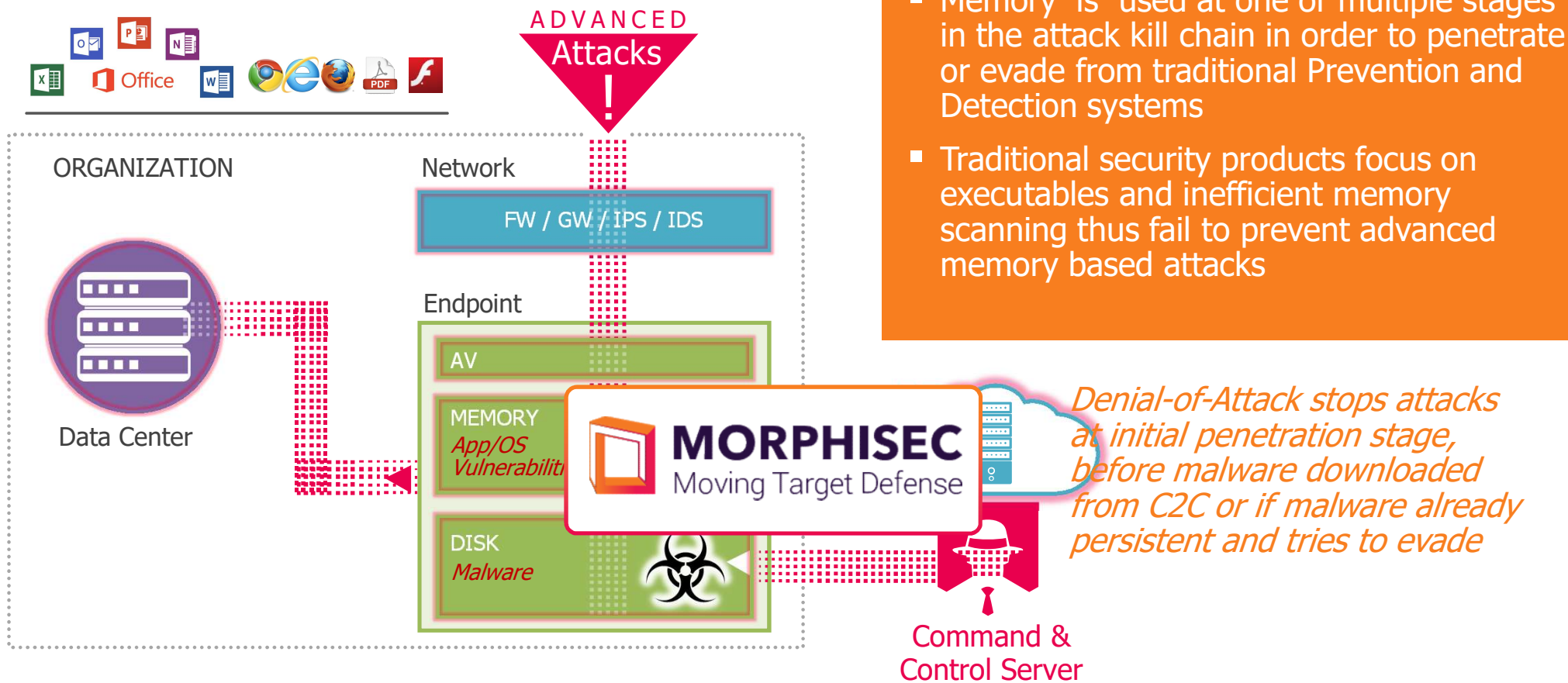
- Most of advanced attacks uses memory resources and vulnerabilities in applications and operating systems.

- Memory is used at one or multiple stages in the attack kill chain in order to penetrate or evade from traditional Prevention and Detection systems

- Traditional security products focus on executables and inefficient memory scanning thus fail to prevent advanced memory based attacks

MORPHISEC

Moving Target Defense
Implementation

AV

Memory

Morphed Application Memory

Disk

End Point

MORPHISEC
Moving Target Defense
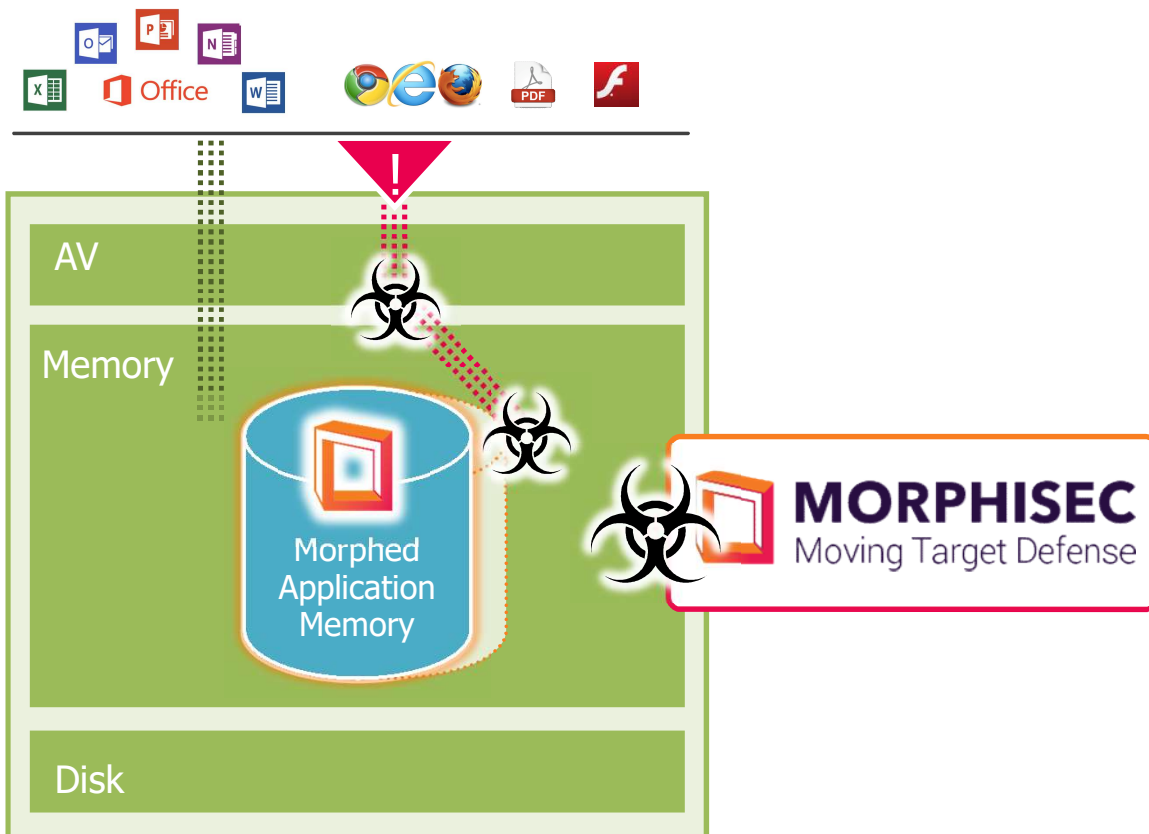
Prevention
Prevents zero-days, targeted and unknown attacks, with no prior knowledge

Deterministic
Eliminates false positives

Resilience
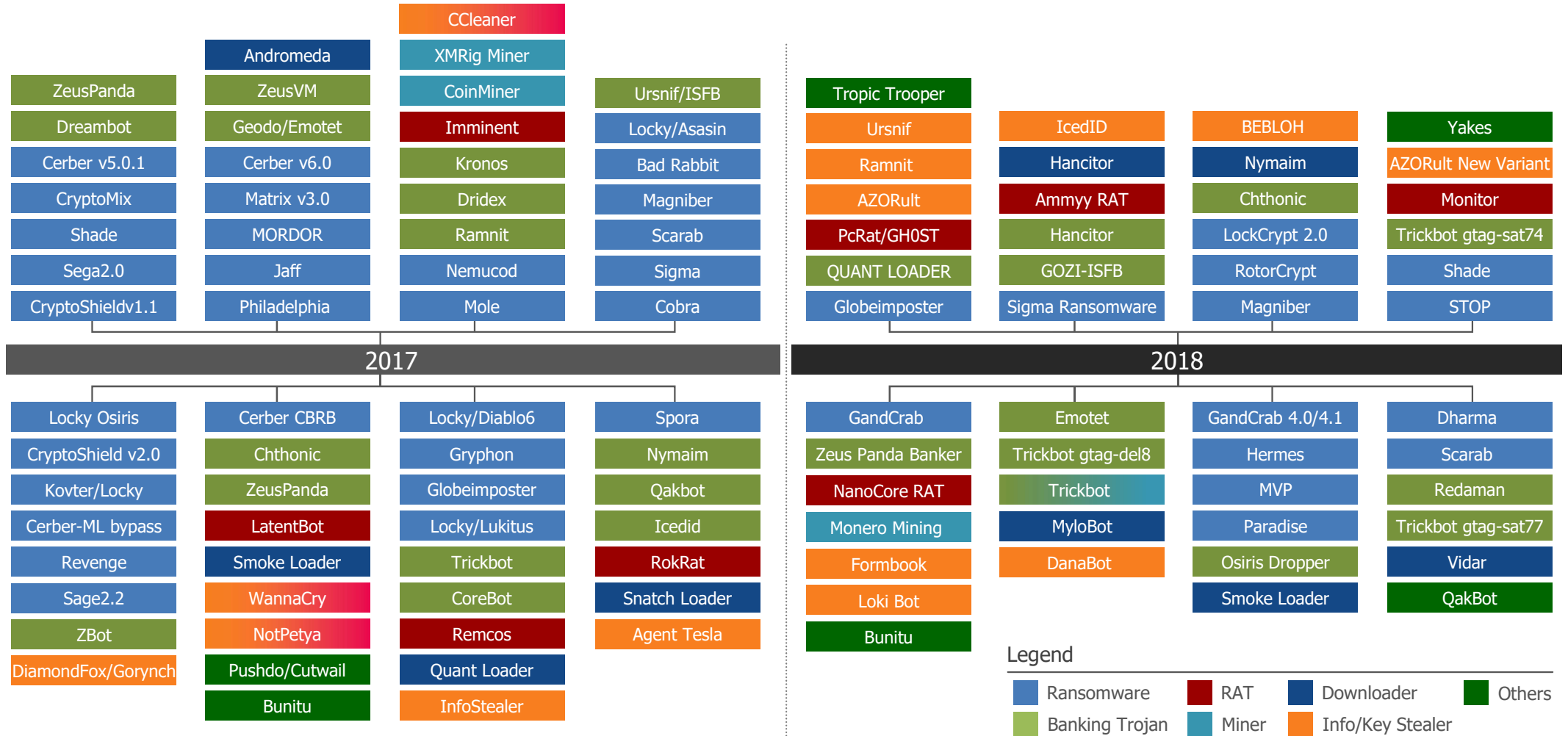Randomization of each process – Moving Target

MORPHISEC

Protection Coverage

	Infiltration	Pre-execution	Execution
E-Downloads	Non-Executable Attachments	Zip, Scripts, Payload	Payload / Fileless
	Documents	Exploitation, OLE, Macro	Payload / Logical
	Links	Shortcuts, Shares, Web	
Web	Drive by Downloads	Exploit Kits (Prevalent)	Payload
		Malicious Script	Flash, Java, VB, Plugins
Physical		Payload	
		Kernel Exploitation	
Network	Kernel Exploitation	Shellcode Injection User-mode	
		Persisting Through Kernel	
	Additional Network Based Attack	Lateral Movement	Payload

MORPHISEC

Malware Prevented by Morphisec

2017

		CCleaner	
	Andromeda	XMRig Miner	
ZeusPanda	ZeusVM	CoinMiner	Ursnif/ISFB
Dreambot	Geodo/Emotet	Imminent	Locky/Asasin
Cerber v5.0.1	Cerber v6.0	Kronos	Bad Rabbit
CryptoMix	Matrix v3.0	Dridex	Magniber
Shade	MORDOR	Ramnit	Scarab
Sega2.0	Jaff	Nemucod	Sigma
CryptoShieldv1.1	Philadelphia	Mole	Cobra

Locky Osiris	Cerber CBRB	Locky/Diablo6	Spora
CryptoShield v2.0	Chthonic	Gryphon	Nymaim
Kovter/Locky	ZeusPanda	Globeimposter	Qakbot
Cerber-ML bypass	LatentBot	Locky/Lukitus	Icedid
Revenge	Smoke Loader	Trickbot	RokRat
Sage2.2	WannaCry	CoreBot	Snatch Loader
ZBot	NotPetya	Remcos	Agent Tesla
DiamondFox/Gorynch	Pushdo/Cutwail	Quant Loader	
	Bunitu	InfoStealer	

2018

Tropic Trooper			
Ursnif	IcedID	BEBLOH	Yakes
Ramnit	Hancitor	Nymaim	AZORult New Variant
AZORult	Ammyy RAT	Chthonic	Monitor
PcRat/GH0ST	Hancitor	LockCrypt 2.0	Trickbot gtag-sat74
QUANT LOADER	GOZI-ISFB	RotorCrypt	Shade
Globeimposter	Sigma Ransomware	Magniber	STOP

GandCrab	Emotet	GandCrab 4.0/4.1	Dharma
Zeus Panda Banker	Trickbot gtag-del8	Hermes	Scarab
NanoCore RAT	Trickbot	MVP	Redaman
Monero Mining	MyloBot	Paradise	Trickbot gtag-sat77
Formbook	DanaBot	Osiris Dropper	Vidar
Loki Bot		Smoke Loader	QakBot
Bunitu			

Legend

Ransomware	RAT	Downloader	Others
Banking Trojan	Miner	Info/Key Stealer	

MORPHISEC

Attack Vectors & Exploits (Fileless) Prevented

Flash EK CVE-2016-4117	Meterpreter OilRig Campaign	
Silverlight EK CVE-2016-0034	Lsass Injection EternalBlue	Word EK CVE-2017-11882
JavaScript EK CVE-2015-2419	Word/EPS EK CVE-2017-0261	Flash EK CVE-2017-11292

2017

Macro shellcode Hancitor	Word/EPS EK CVE-2017-0262	Word EK CVE-2017-11826
PS Reflective Injection - Kovter	DNSMessenger Fin7	
VBS Reflective Injection - Kovter		
PS Meterpreter MuddyWater		

Flash EK CVE-2018-4878	Flash EK CVE-2018-5002	JavaScript (IE) CVE-2018-8460
Office CVE-2018-0802	Acrobat Reader CVE-2018-4990	JavaScript (IE) CVE-2018-8653
Office CVE-2017-11882	VB EK CVE-2018-8174	VB EK CVE-2018-8373	Flash EK CVE-2018-15982

2018

Use of EternalBlue & DoublePulsar for lateral movement	Monero via PROPagate injection technique	Cobalt Gang ThreadKit (latest)	FIN6 (Cobalt) FrameworkPoS
			TA505 AmmyRAT

Legend

Exploits

MORPHISEC

Preventing the Unknown

Exposure Is Built Into Detection-Based Security

Adobe Flash Zero-Day Attack (CVE 2018 – 4878)

Mitre Report | Adobe Patch | Symantec Update | AV/NGAV Updates

Status Quo — Window of Exposure → Delayed Start of Coverage →

Attacks ○

Moving Target Defense — Coverage from Moment Attack Created →

Nov	Dec	Jan	Feb
2017	**2017**		
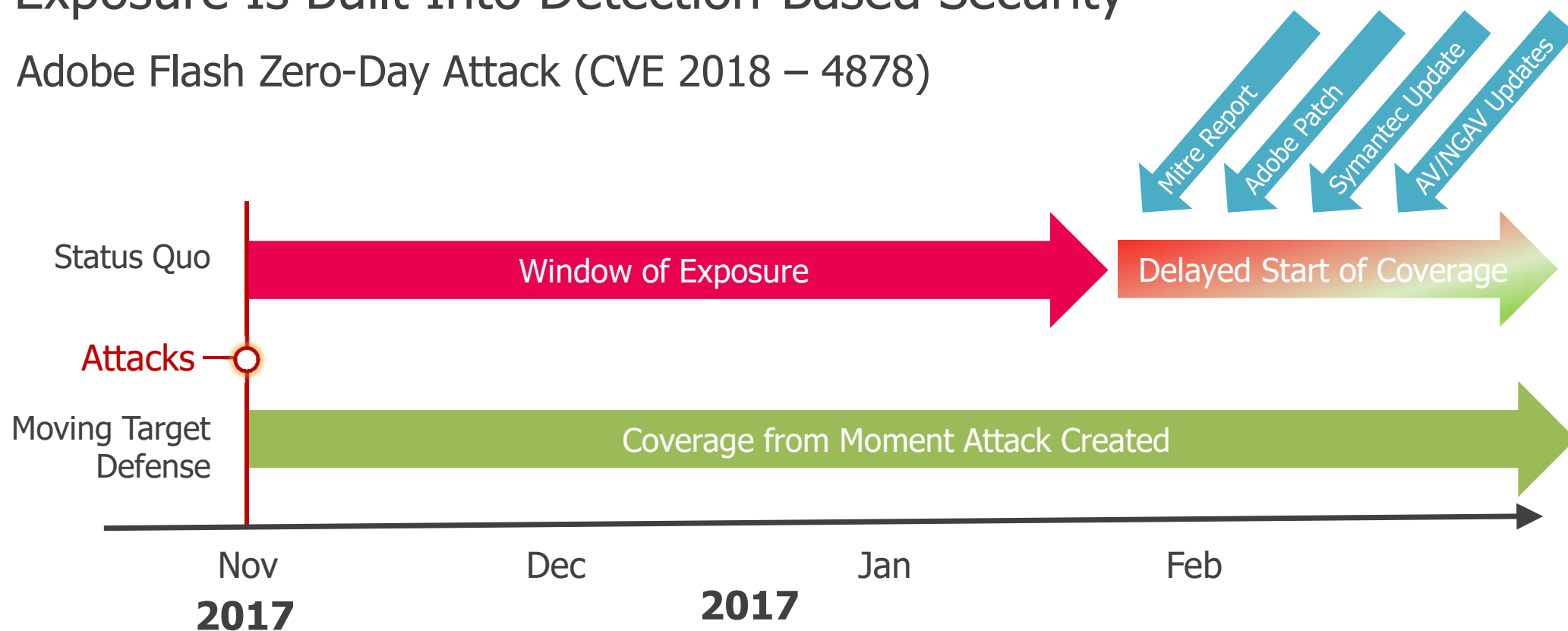
Need for Prevention Without Detection Is Acute

Morphisec Unified Threat Prevention (UTP) Platform
On-Prem, Private/Public Cloud

Active Directory

Enterprise SIEM

Management Server

Windows

Linux – Starting Q3/2019

PC/Laptops   Virtual Desktops   Virtual App   Server   Container   Serverless

2020

CiTRIX Ready   vmware®
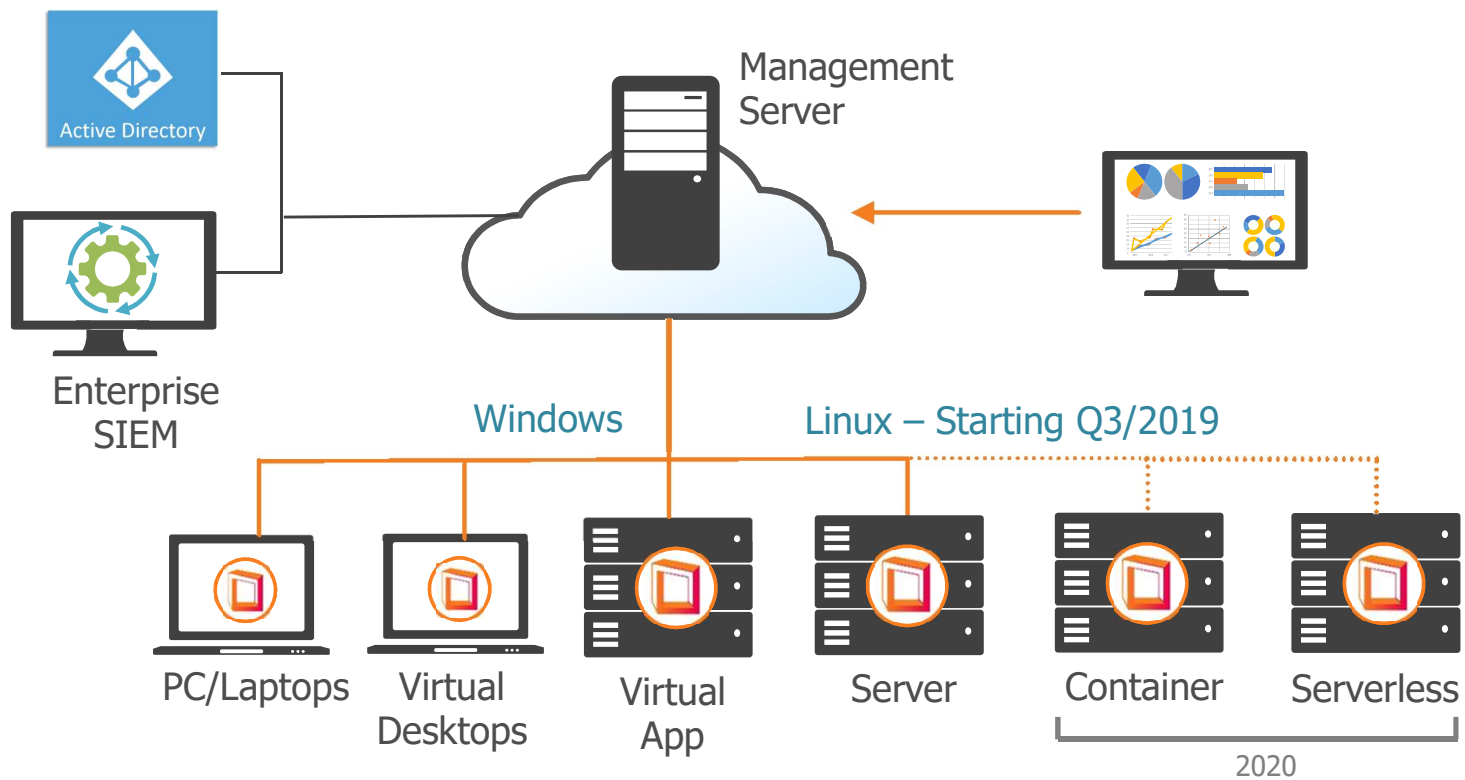
Install

- 2MB user mode agent
- SCCM / standard dist
- No reboot
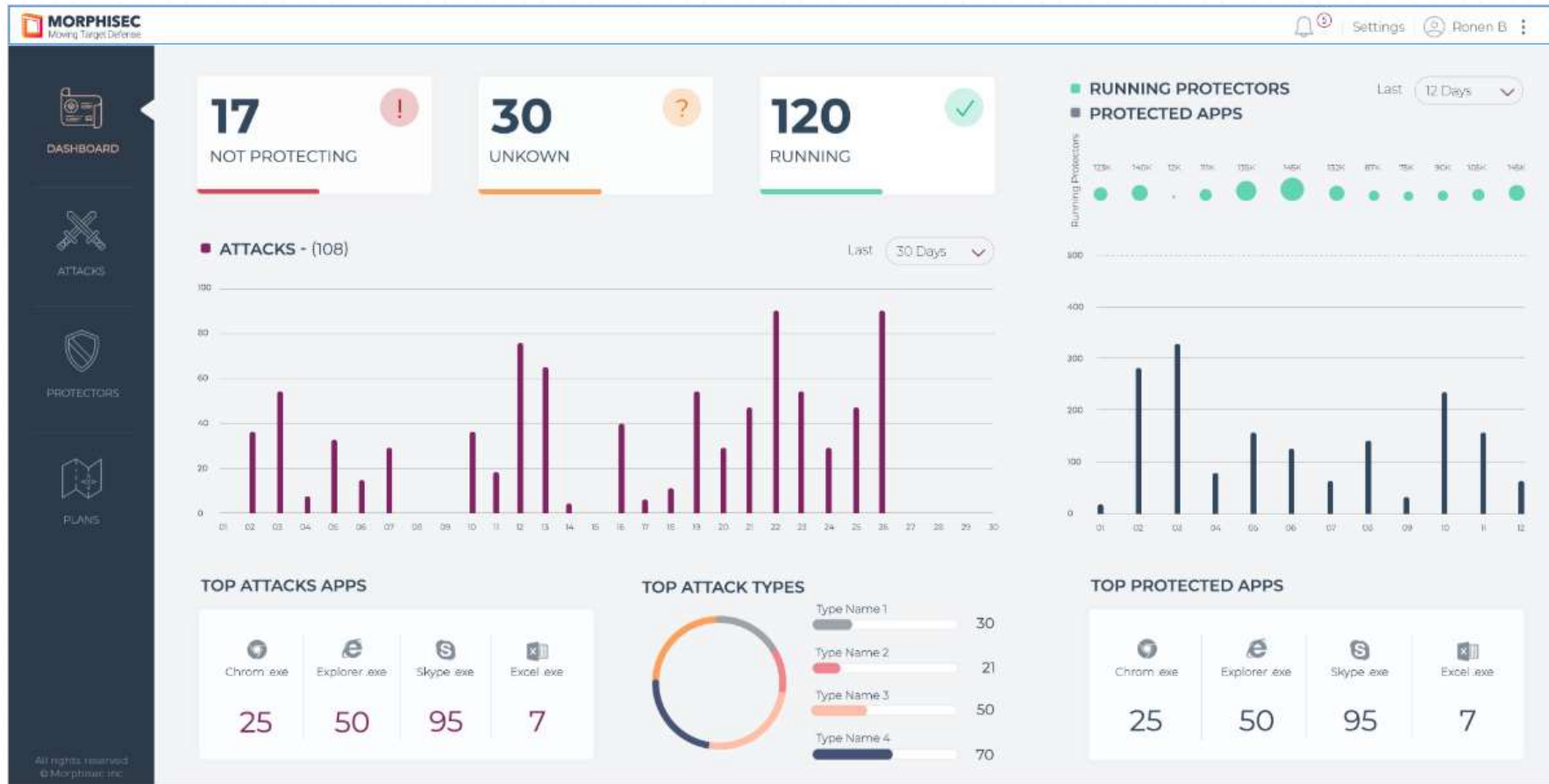- No configuration
- No rules / policies

Maintain

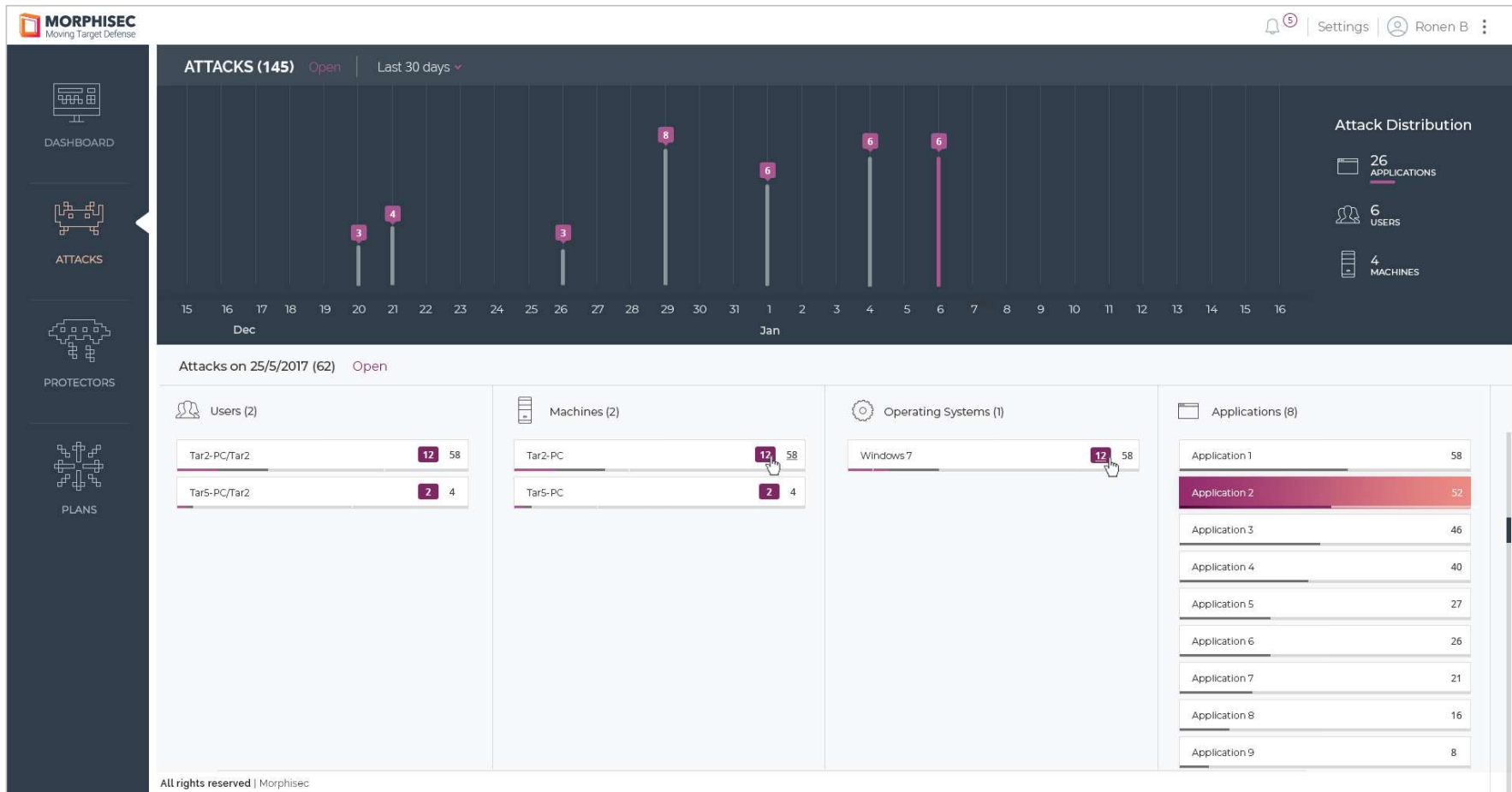- Prevention reports
- No updates
- Offline protection
- No CPU consumption

Control and Visibility

MORPHISEC

Control and Visibility

Control and Visibility

The Optimal Prevention Stack – the 80/20 rule

Windows 10

MORPHISEC Moving Target Defense

Defender AV

- Lower cost
- Higher operational efficiency

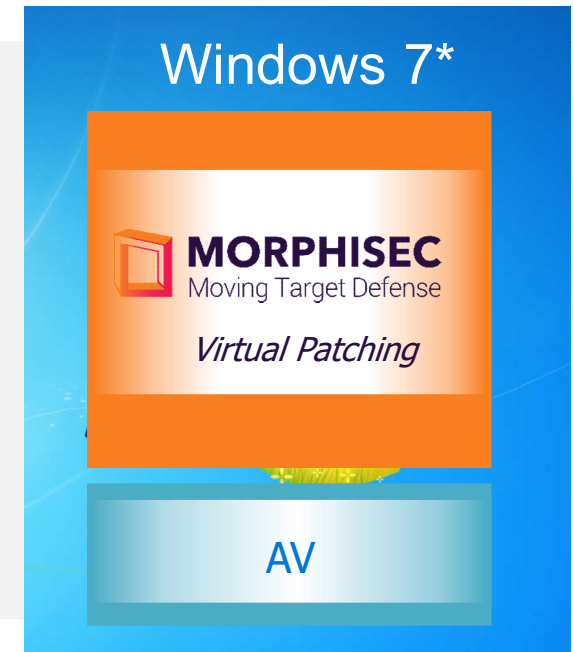## MITIGATED BREACH RISK

80%
Primary

Unknown, In-Memory

File-less attacks

Evasive malware

Exploits

Web / browser attacks File document attack

Supply chain attack

20%
Residual

Known & Non-memory

Windows 7*

MORPHISEC Moving Target Defense

Virtual Patching

AV

Compliance

* Extended Supports ends Jan 20'

Ecosystem and Technology Partners

SIEM/SOAR

Virtual Platforms

EDR

Windows
Defender ATP

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

Status Quo		Morphisec
▪ 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

Proactive prevention
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

MORPHISEC

Morphisec benefits to Enterprises – A CxO's perspective

Instantaneous, Effortless & Deterministic Prevention

Prevent Unknown Attacks
- Time
- Vectors

"Morphisec prevents unknown cyber attacks with zero time delay for discovery and detection"

- Richard Rushing,
  CISO Motorola

Set and Forget
- Time to value
- Ease of use
- TCO / ROI

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

- Skip Rollins, CIO
  Freeman Health

Risk Reduction
- Flat risk
- Virtual patch
- Defense in depth

"Morphisec is a core component of my defense-in-depth strategy."

- Adrian Asher, CISO
  London Stock Exchange Group

MORPHISEC

Rapid Customer Ramp

2.7M Protected Endpoints

100% Renewals

No Churn

Financials

Channeles

Manufacturing

Services