
B
PROTECTING 500 MILLION USERS WORLWIDE

Bitdefender

Gestione del rischio e nuovi scenari di attacco:

- Evitare il Data Breach ed essere conformi alla GDPR
- Ridurre il costo operativo della Security
- Mettere in sicurezza le applicazioni critiche

Francesco Speciale, Lan Service Business Team Manager
Denis Valter Cassinerio, Bitdefender Regional Sales Director Italy
Stefano Maranzana Lan Service Senior System Engineer

Bitdefender

Gestione del rischio e nuovi scenari di attacco:

- Ridurre il costo operativo della Security

Denis Valter Cassinerio, Bitdefender Regional Sales Director Italy

GDPR : cosa ci dice

I Dati includendo I dati Personali, sono diventati rapidamente l'essenza della economia globale.

Rappresentano un Nuovo "asset" fondamentale per il nostro progresso e per la nostra sicurezza.

“Bitdefender è una global IT security technology company”

– Florin Talpeș – Bitdefender CEO & Founder

Socio Clusit
Associazione Italiana per la Sicurezza Informatica

150+ OEM PARTNERSHIP

Bitdefender

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica

Bitdefender

GDPR
E’ ORA DI AGIRE…

GDPR Principali Impatti Organizzativi/Procedurali

Gestione Accountability	Attestazione documentata degli adempimenti privacy presi in carico; controllo sui trattamenti effettuati, responsabilità e compiti assegnati, misure di sicurezza implementate
Gestione Data Breach	Definizione ed implementazione di piani di gestione e relativa organizzazione e test, utilizzo di strutture informative per documentare gli eventi di Data Breach, organizzazione e mezzi per rispettare le tempistiche di legge
PIA (Privacy Impact Assessments)	Definizione ed implementazione di metodi per condurre, documentare e gestire nel tempo le attività di PIA ed eventuali conseguenti Prior Consultation con il Garante Privacy
Misure contrattuali Titolare-Responsabili	Definizione/Aggiornamenti clausole ed istruzioni, gestione della casistica dei Responsabili in 'cascata'
Misure contrattuali trasfer	Definizione//Review/Aggiornamenti degli strumenti legali adottati per il trasferimento dati cor , invent to in es
Gest diritti, consenso informato	Rev proced inform Procedure integrate per l'esercizio dei diritti nel rispetto delle tempistiche di legge
Formazione	Formazione del personale preposto ai trattamenti dati personali
Data Protection Officer	Per le aziende che devono prevedere tale figura: assegnazione dei compiti e gestione delle comunicazioni ed operatività previste dal Regolamento
Gestione one-stop-shop	Per le aziende che fanno business in più Stati Membri UE: adozione ed implementazione di procedure per il rapporto con la Lead Privacy Authority
Gestione raccordi compliance	Gestione raccordi normativi nei riguardi degli adempimenti D.Lgs 231/01 e coordinamento con altre compliance aziendali (es. normativa giuslavoristica)

MONITOR ALERT DETECT EX POST

Bitdefender

DATA BREACH

ATTENZIONE

Il contenuto che segue è adatto ad un audience un po'…

NERD

Il problema principale: gli Endpoint “compromessi”

62% dei breach sono stati assocati ad attività di hacking

51% dei breach includono malware

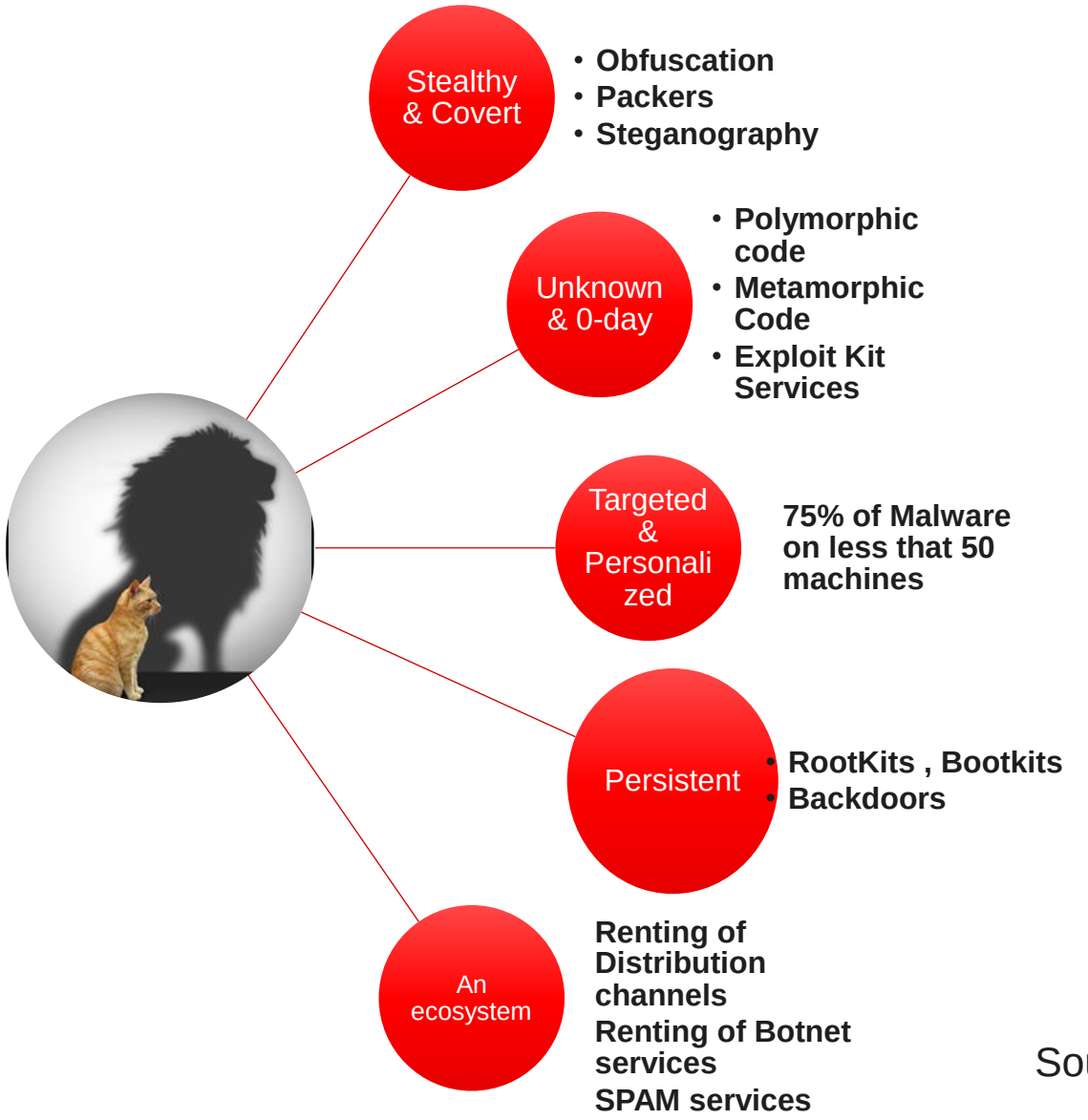
66% del malware è stato installato attraverso le mail

Le minacce hanno riguardato gli endpoint

92% degli attacchi di phishing che hanno portato ad un breach è seguita l’installazione di software di varia natura

Source: Verizon 2017 Data Breach Investigations Report

L'ASCESA DEL MALWARE "MODERNO"

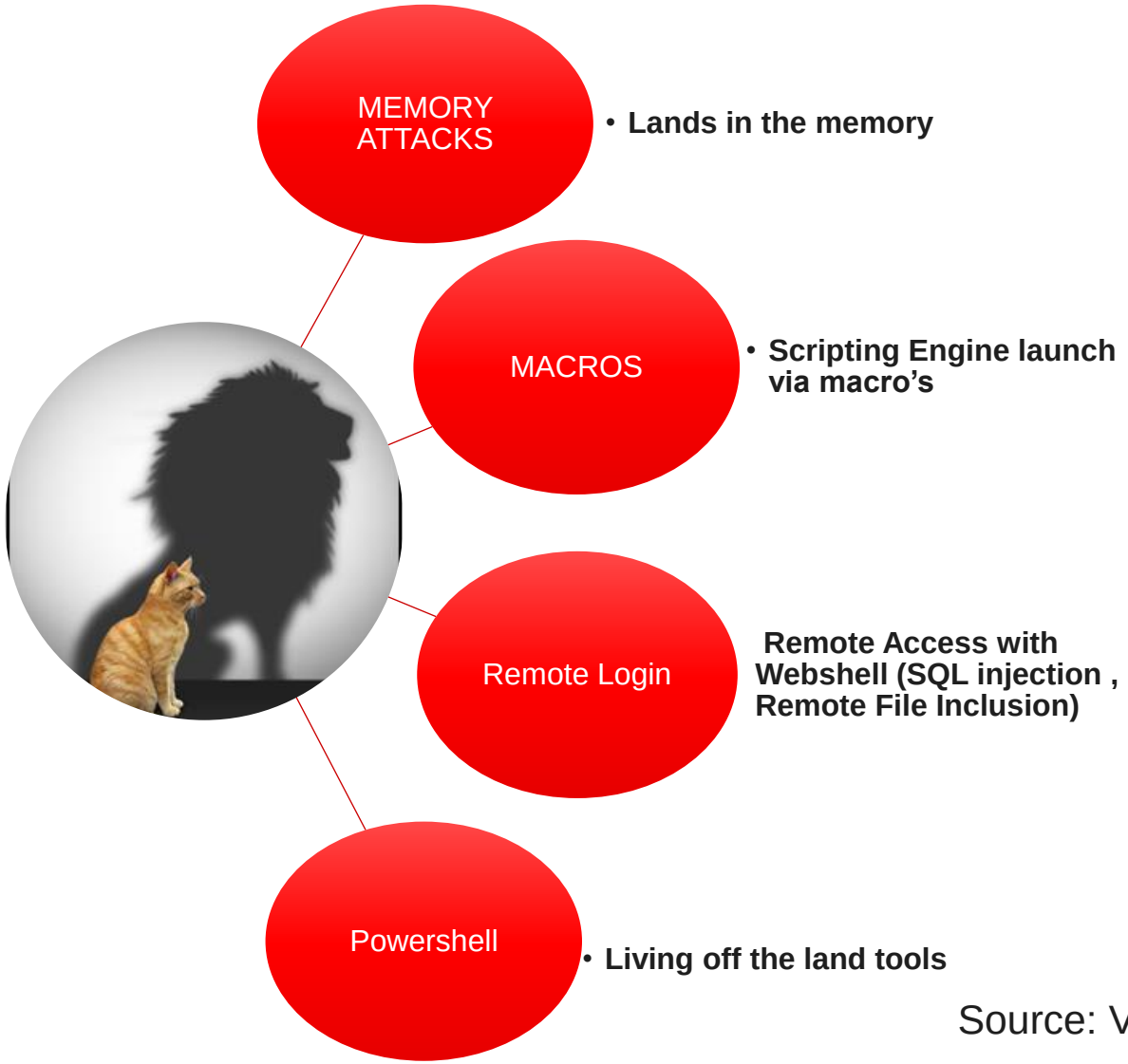


51%

Dei breach derivano da malware

Source: Verizon 2017 Data Breach Investigations Report

…E L'ASCESA DEGLI ATTACCHI «NON-MALWARE»



49%

Dei breach non usano malware

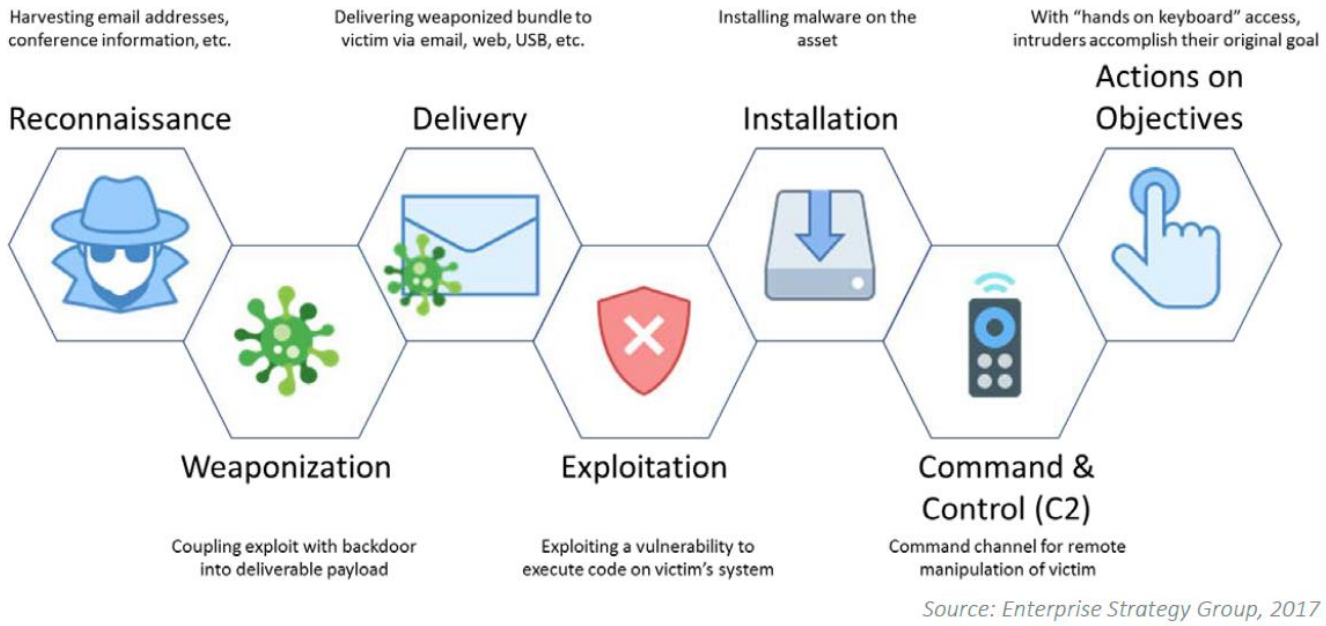
Source: Verizon 2017 Data Breach Investigations Report

FILE BASED ATTACK

MALWARE COMUNE DI MASSA
- Già identificati in passato e basati sul riconoscimenti di firma.

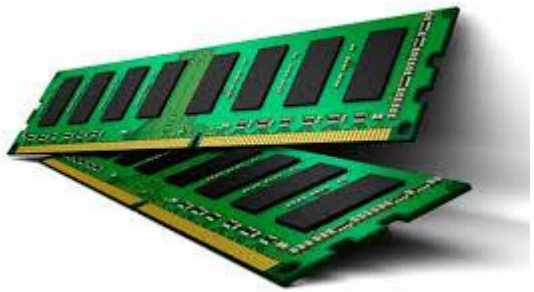
MALWARE «MIRATO»
- Malware disegnati per specifiche organizzazioni e per i quali non esistono firme

MUTAZIONI DI MALWARE ESISTENTE
-Malware che agisce sulla modifica del valore crittografico dell'hash per evitare il riconoscimento



FILELESS ATTACK

BASATI SU ACCESSO ALLA MEMORIA
- Attacchi che utilizzano lo spazio legittimo in memoria destinato ad un applicazione.



MODIFICA MALEVOLE DEL CONTENUTO
- Attacchi che utilizzano uno specifico contenuto in una applicazione come le macro o i pdf.

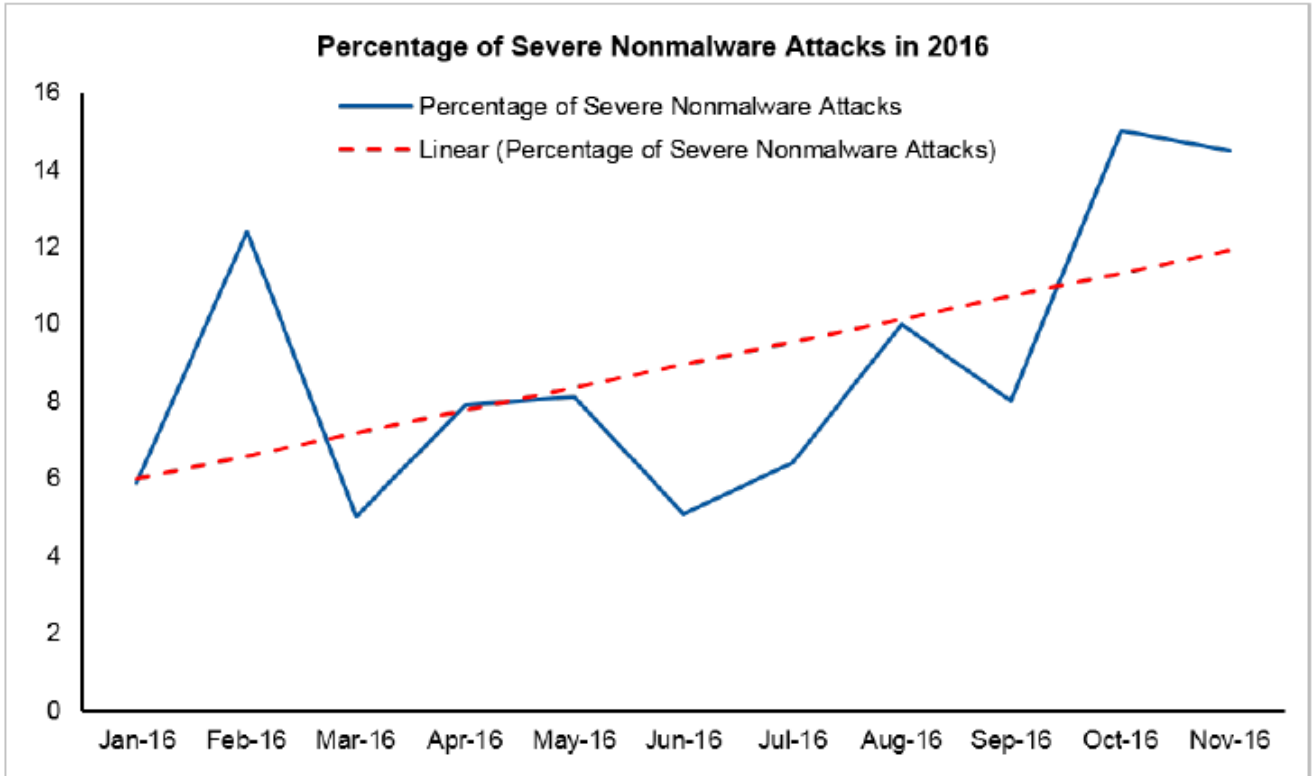
BASATI SUGLI SCRIPT
-Attacchi scritti con un linguaggio script come Javascript o PowerShell

MODIFICA DELLE CHIAVI DI REGISTRO
- Attacchi di tipo file-less che risiedono nel registro del sistema operativo

ROOTKITS
- Attacchi di tipo Kernel a livello di disco ma non diretti al file system del sistema operativo

EVOLUZIONE DEGLI ATTACCHI FILE-LESS

Figure 1. The Upward Trend of Fileless Malware Attacks



Source: Gartner: Get Ready for «Fileless» Malware Attacks Feb 17

Continua crescita degli attacchi di tipo File-less

Virtualmente almeno 1 attacco file-less per azienda a livello mondiale.

NEXT GENERATION ENDPOINT SECURITY

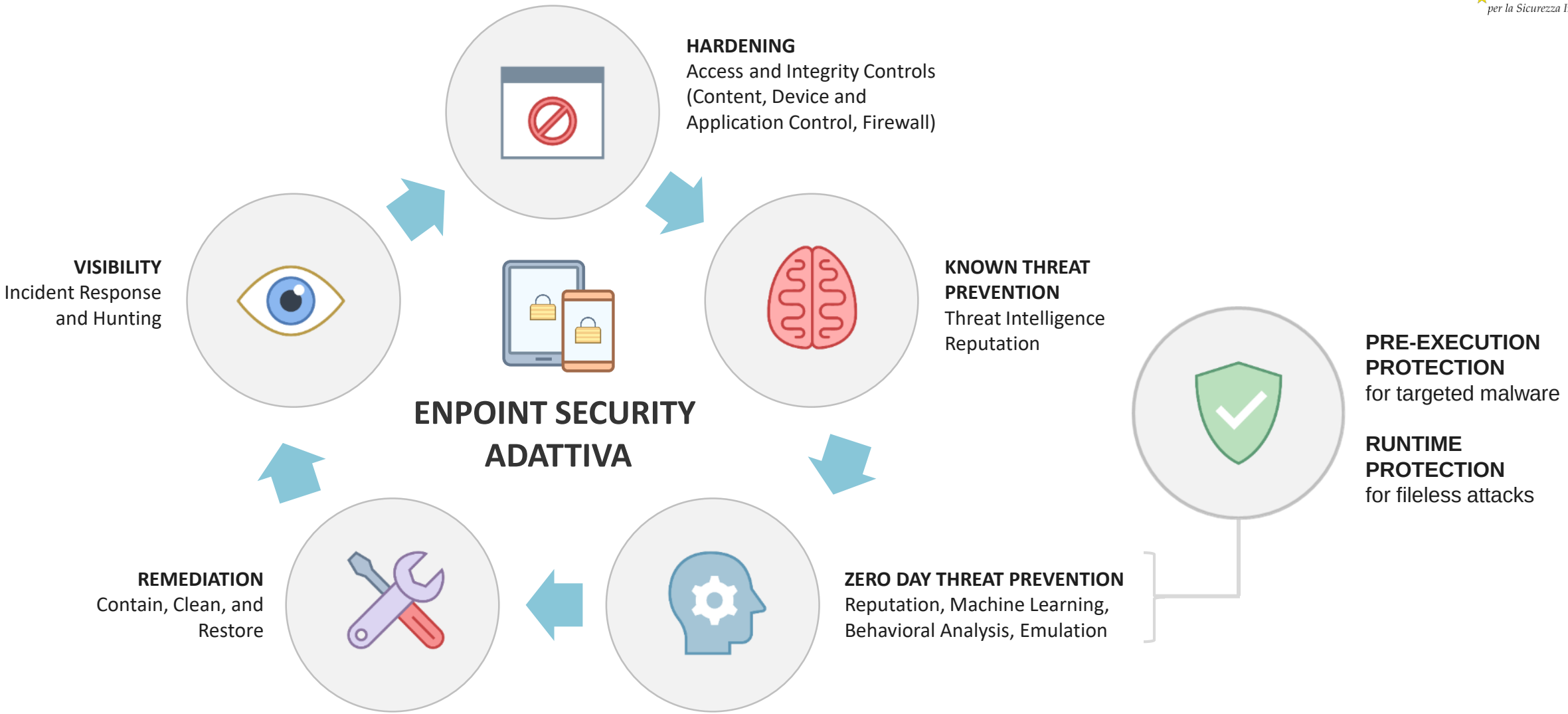
Categoria	Descrizione	Utilizzo
Machine Learning	Crea un modello statistico	Identificazione anomalie dal modello di riferimento
Ispezione ed analisi degli eseguibili	Analisi in fase di pre-esecuzione. Il codice non viene eseguito	Controlla multiple proprietà del malware per definire uno score di rischio ed una soglia di accettazione
Container	Ambiente sicuro (Sandbox) per l'esecuzione di codice	Ulteriore layer pre-esecuzione.
Analisi Statica/ Dinamica del malware	Monitoraggio post esecuzione del codice	Ispezione del codice in un ambiente «sicuro» per identificazione/prevenzione del malware.
Threat Intelligence Integration	Update continui degli indicatori di compromissione (IOC) e tattiche, tecniche e procedure (TTP) utilizzate per l'attacco.	Blocca exploit e malware con una real-time intelligence e associazione ai pattern di attacco.

ESG :An Adaptive and Layered Approach to Endpoint Security June 2017

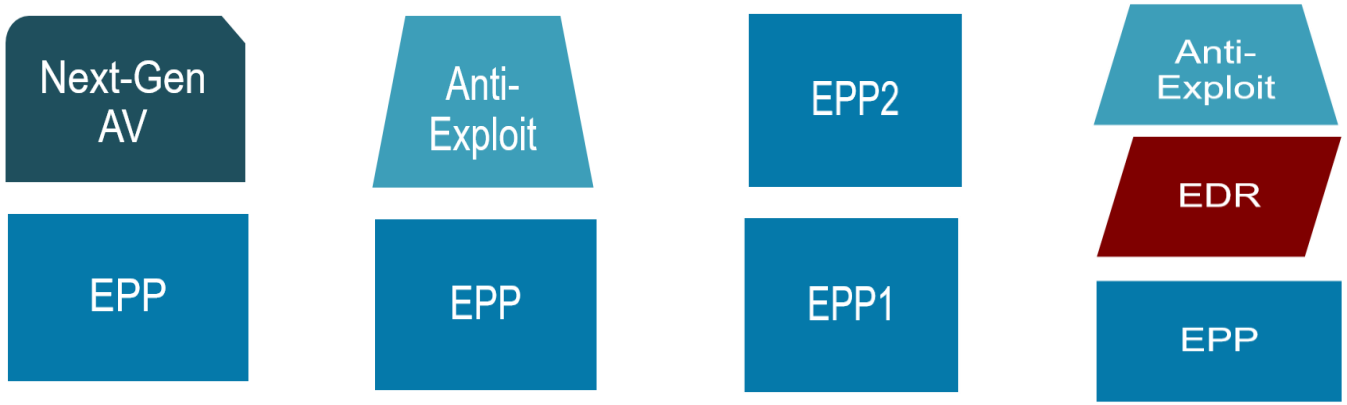
L'Endpoint Security: per ridurre il rischio diventa "funzione del contesto" Protection+Detection (EPP+EDR)

Bitdefender

SOCIO Clusit Associazione Italiana per la Sicurezza Informatica



LA REALTA’ DELLE INSTALLAZIONI ATTUALI

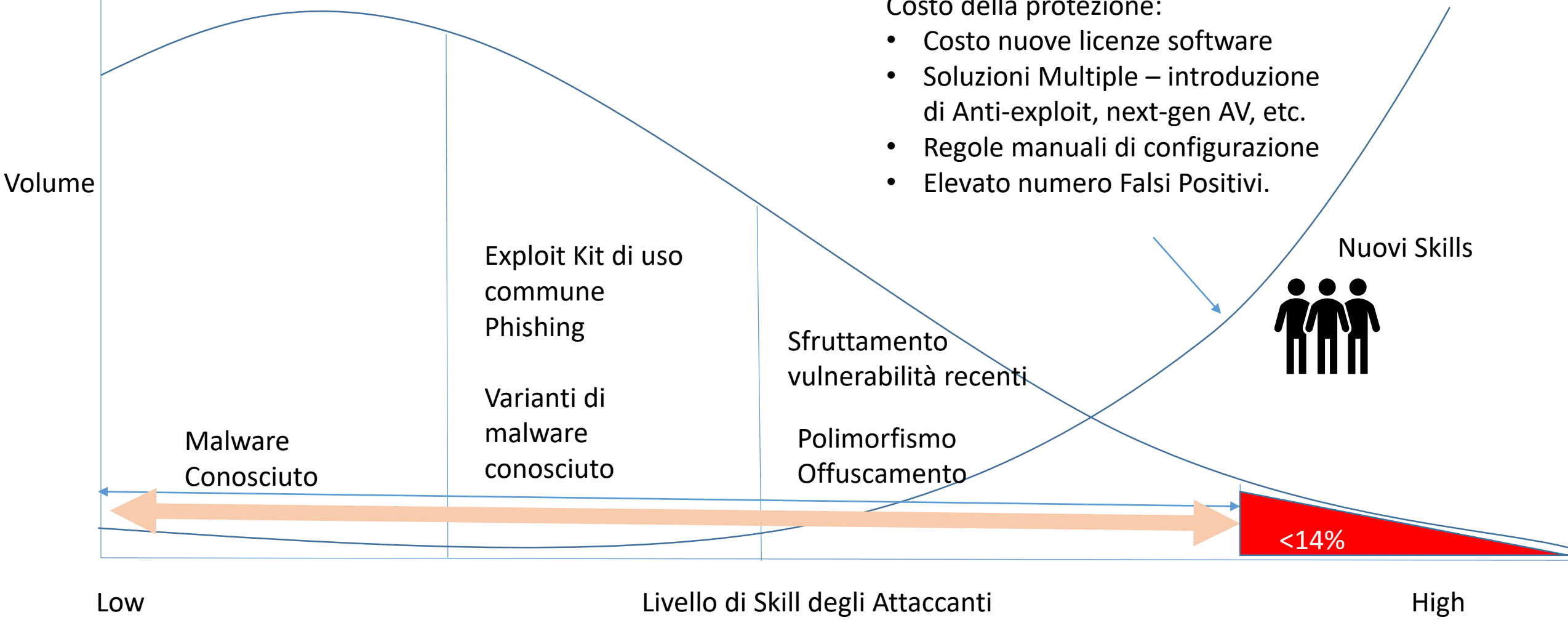


Ole organizzazioni sono obbligate ad “installare più di un prodotto
(console multiple, agenti multipli…instabilità, incompatibilità aumento costi operativi)

Costo della Endpoint Security – Prima della "Layered Next-Gen" -

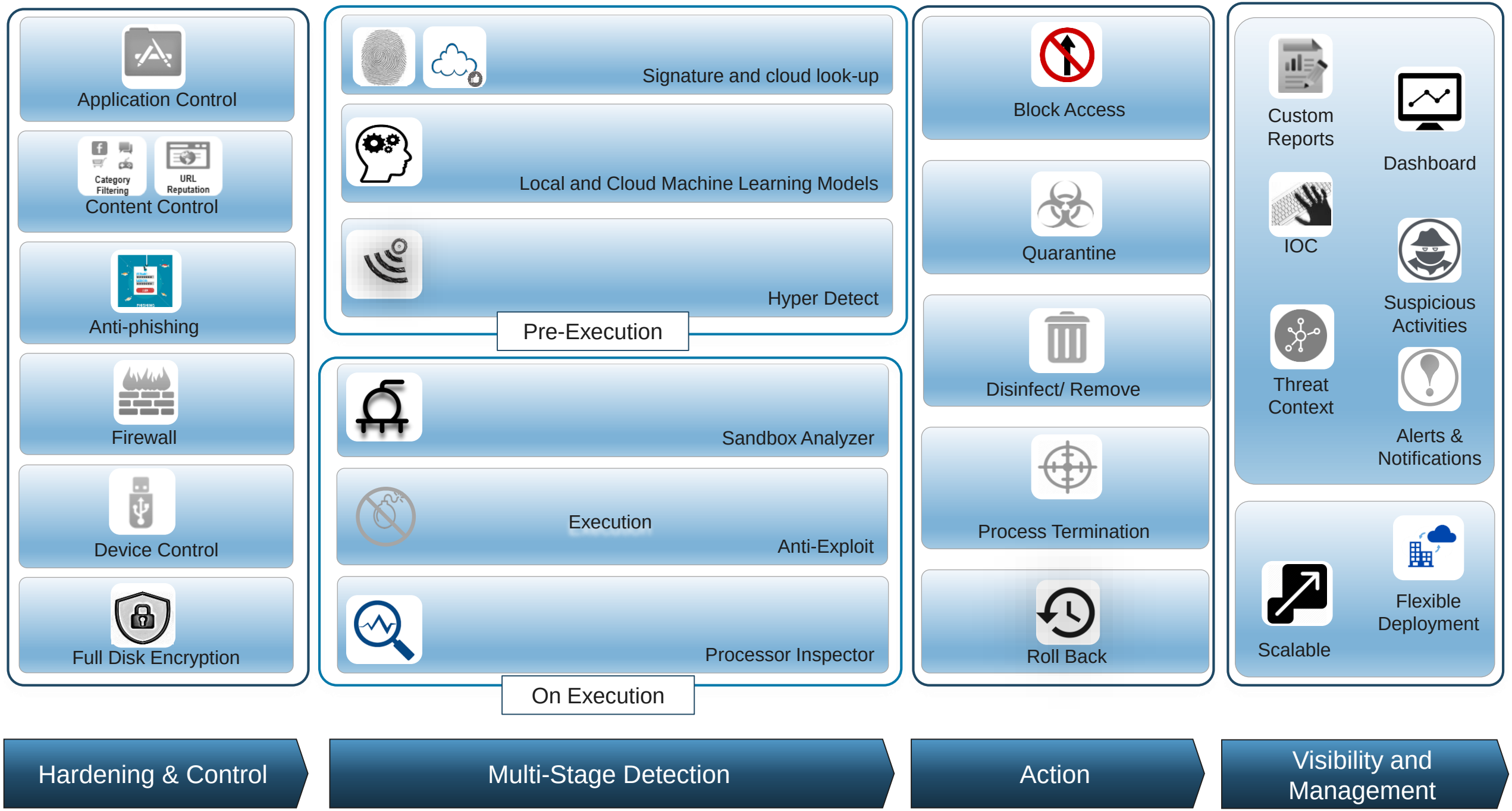
Costo della protezione:

- Costo nuove licenze software
- Soluzioni Multiple – introduzione di Anti-exploit, next-gen AV, etc.
- Regole manuali di configurazione
- Elevato numero Falsi Positivi.



Bitdefender

HYPERDETECT


Application Control
Category Filtering
URL Reputation
Content Control
Anti-phishing
Firewall
Device Control
Full Disk Encryption
Signature and cloud look-up
Local and Cloud Machine Learning Models
Hyper Detect
Pre-Execution
Sandbox Analyzer
Execution
Anti-Exploit
Processor Inspector
On Execution
Block Access
Quarantine
Disinfect/ Remove
Process Termination
Roll Back
Custom Reports
Dashboard
IOC
Suspicious Activities
Threat Context
Alerts & Notifications
Scalable
Flexible Deployment
Hardening & Control
Multi-Stage Detection
Action
Visibility and Management

DATA CENTER SECURITY: IL CUORE DELLA SECURITY
HYPERVISOR AGNOSTIC

25% Di tutto il **Malware** è **V**irtual **M**achine **A**ware.

ORACLE VM

NUTANIX READY • AHV •

vmware READY NETWORKING AND SECURITY

vmware NSX

vmware

CITRIX ready

CITRIX XenServer

Microsoft Hyper-V

KVM

RED HAT ENTERPRISE VIRTUALIZATION 3
It's your virtualization. Not theirs.

Bitdefender “Next Gen Endpoint” :

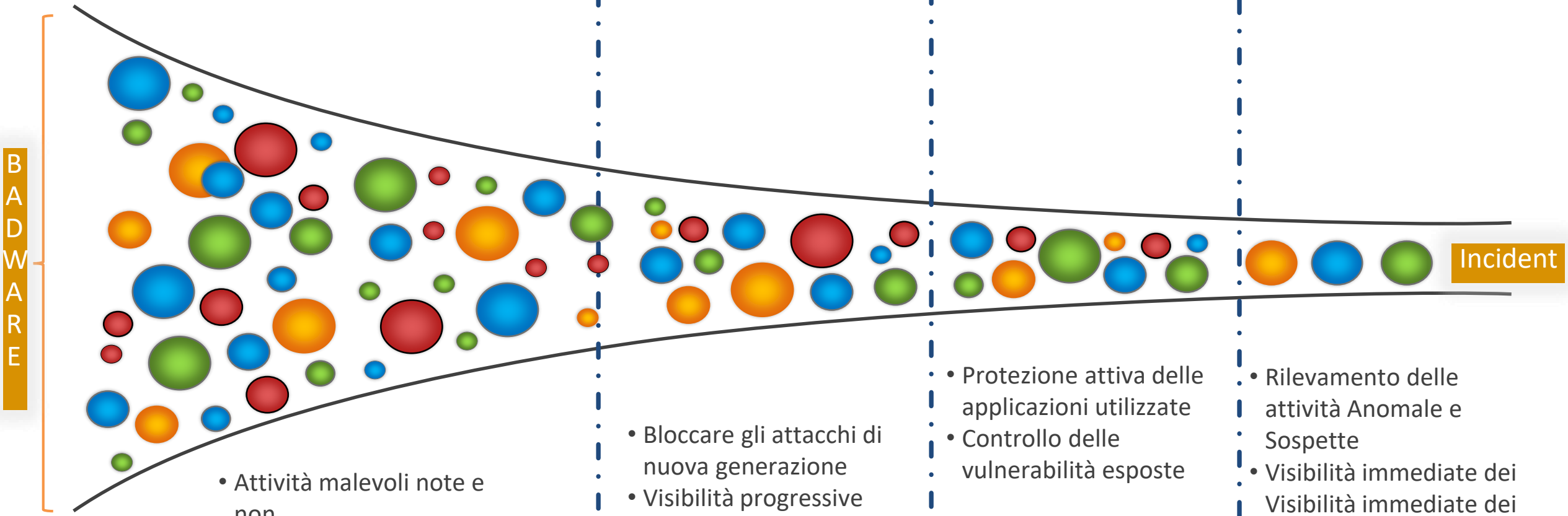
Riduce progressivamente la “Superficie di Attacco”

Anti-Malware (Pre-execution & Behavioral): Step 1

Hyper-Detect : Step 2

Hardening : Step 3

Detect & Respond: Step 4



- Attività malevoli note e non
- Nessun Falso Positivo

- Bloccare gli attacchi di nuova generazione
- Visibilità progressive degli IOC (In funzione delle policy)
- Visibiltà delle attività “sospette”

- Protezione attiva delle applicazioni utilizzate
- Controllo delle vulnerabilità esposte

- Rilevamento delle attività Anomale e Sospette
- Visibilità immediate dei Visibilità immediate dei tentative di attacco mirato
- Bloccare e contenere gli Attacchi

Bitdefender

Bitdefender

MEMORY INTROSPECTION

UNA SOLUZIONE RITENUTA **IMPOSSIBILE DA RAGGIUNGERE**

Estrarre il significato semantico dale **righe di "raw memory "**

Una caratteristica **mai raggiunta sino ad ora**

```
ookhopping      proc near               ; CODE XREF: sub_A0C41E2+72↑p
                                        ; sub_A0C41E2+A9↑p
                cmp     byte ptr [eax], 0E8h
                jz      short loc_A0C42B1
                cmp     byte ptr [eax], 0E9h
                jz      short loc_A0C42B1
                cmp     byte ptr [eax], 0EBh
                jnz     short loc_A0C42C2

loc_A0C42B1:                            ; CODE XREF: hookhopping+3↑j
                                        ; hookhopping+8↑j
                cmp     dword ptr [eax+5], 90909090h
                jz      short loc_A0C42C2
                mov     edi, edi
                push    ebp
                mov     ebp, esp
                lea     eax, [eax+5]

loc_A0C42C2:                            ; CODE XREF: hookhopping+D↑j
                                        ; hookhopping+16↑j
                jmp     eax
```

Controlla **SOLO** a livello di **Raw Memory,** l'unica fonte affidabile di informazione

Dove gli attaccanti, indipendente mente dale tecniche avanzate utilizzate, non possono nascondere le loro tracce

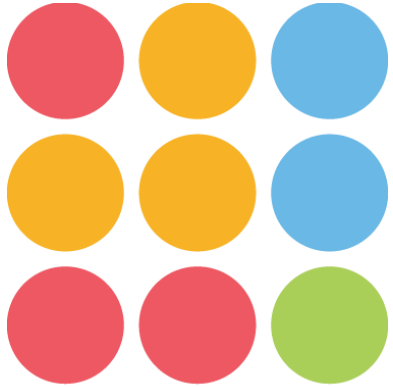
Bitdefender

ENDPOINT SECURITY

CENTINAIA DI MILIONI
MALWARE CONOSCIUTI E NON

RAW MEMORY @ HYPERVISOR LEVEL

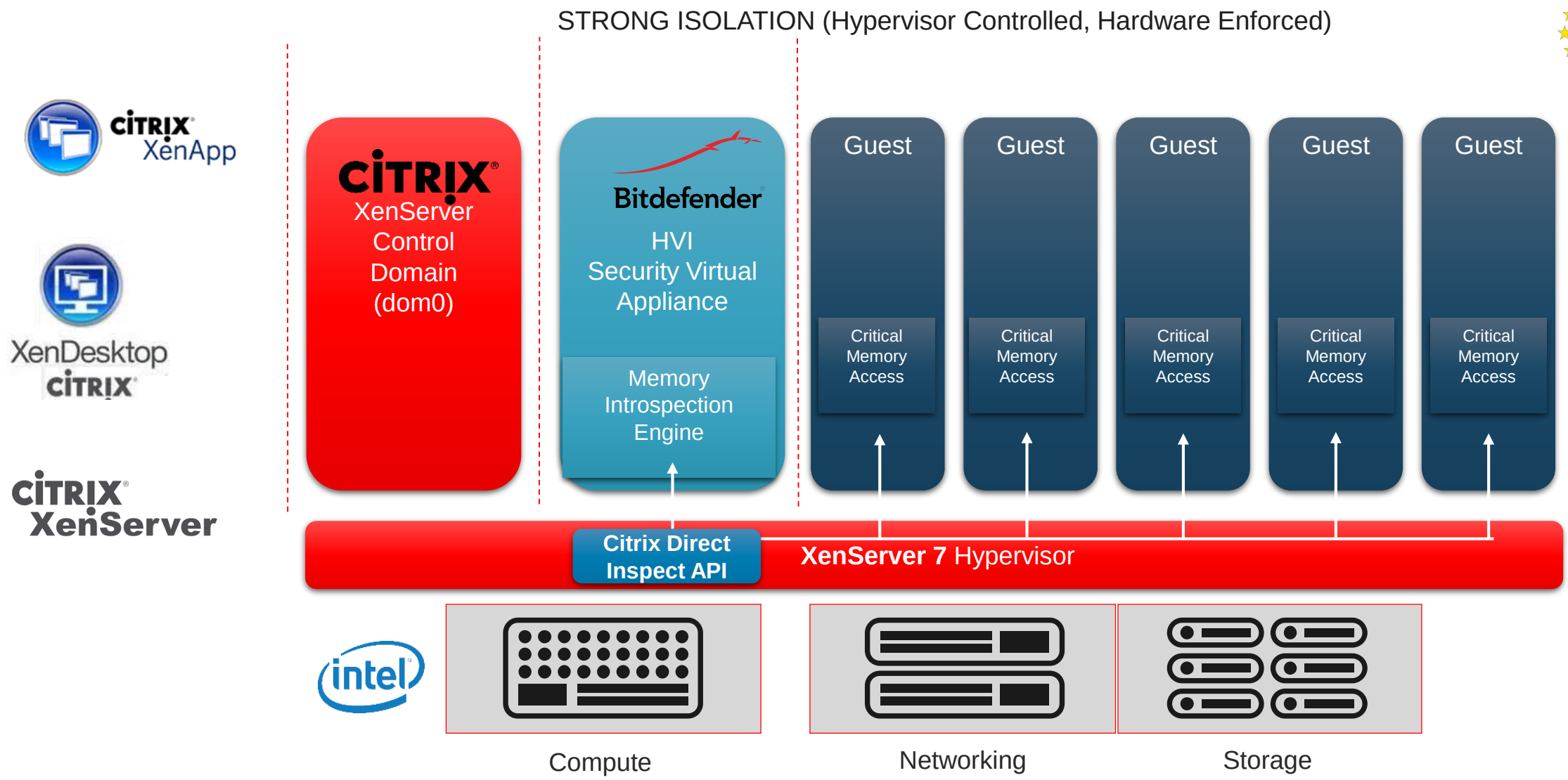
UNA SERIE LIMITATA
DI TECNICHE DI ATTACCO



HEAP SPRAY
CODE INJECTION
FUNCTION DETOURING
API HOOKING

Bitdefender

UNA ARCHITETTURA RIVOLUZIONARIA



APT PROTECTION Investimenti previsti x3 NEI PROSSIMI ANNI

Bitdefender

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica

Bitdefender

CITRIX

intel

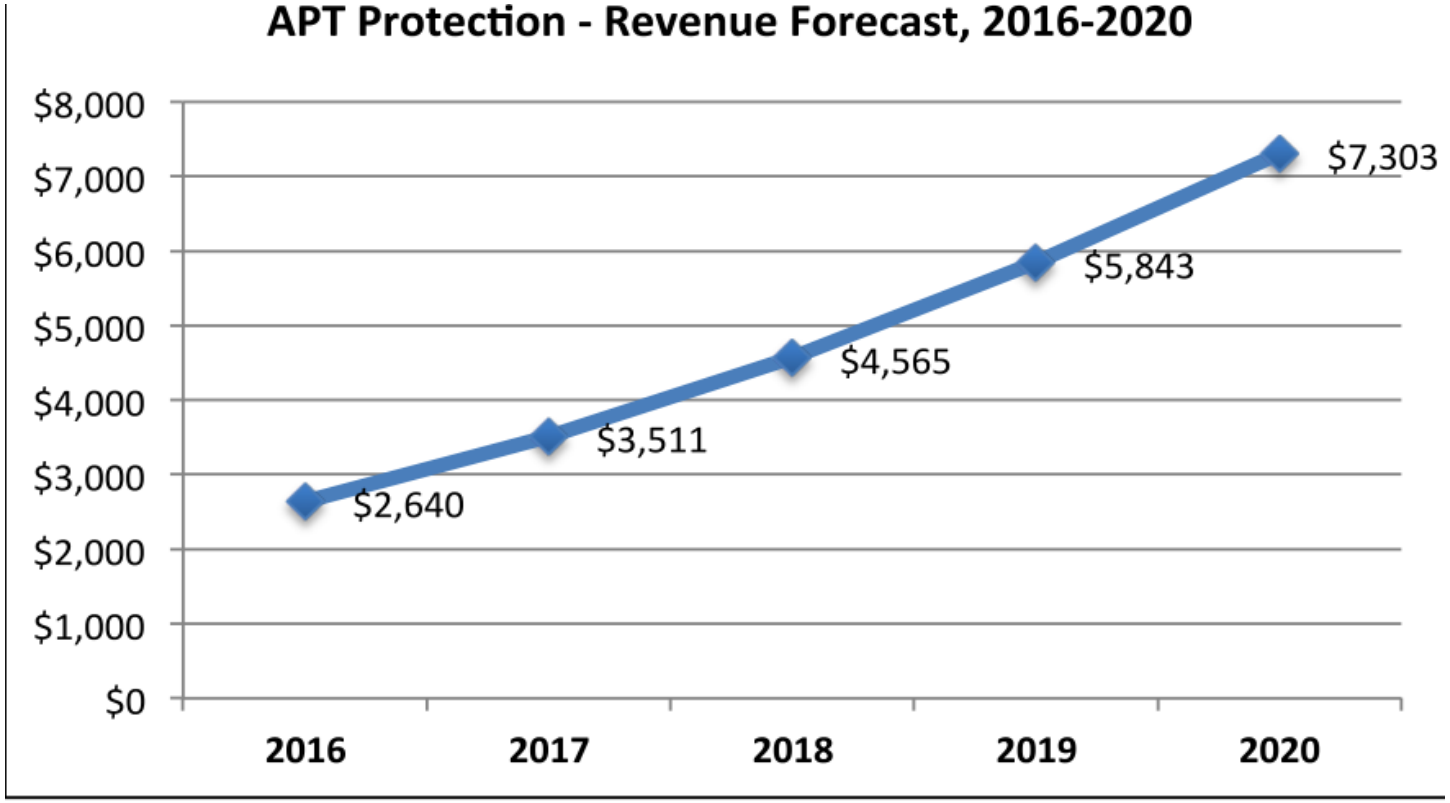


Figure 2: APT Protection Market Revenue Forecast, 2016 – 2020


B
PROTECTING 500 MILLION USERS WORLWIDE