Bitdefender GravityZone Endpoint Security HD

The Layered Next-gen Endpoint Security Platform

Bitdefender

EVOLUCIÓN DEL MERCADO DE SEGURIDAD…
LA PRÓXIMA GENERACIÓN

VISION GENERAL DEL MERCADO

Puntos Críticos: Endpoints Comprometidos

62% de ataques que han tenido éxito

51% de ataques incluían Malware

Las amenazas llegaron a través de Endpoint

66% de malware fue instalado a través de Archivos malisiosos adjuntos en correos electrónicos

92% de los ataques de phishing que llevaron a una violación fueron seguidos por algún tipo de instalación de software

Fuente: Verizon 2017 Data Breach Investigations Report

Mercado inundado con Productos de Seguridad para Endpoint

Prevención	Protección especializada	Detección y respuesta Endpoint (EDR)
Protección altamente efectiva con con el número mas bajo de falso positivos.	• Detección de malware sin firmas (detección agresiva con administración falsa) • Endurecimiento basado en políticas.	Detección basada en datos, análisis forense, investigación, respuesta y remediación.

Jugadores Tradicionales
3.5b , 5% CAGR

Jugadores Emergentes
350m , 50% CAGR

Permutaciones de Seguridad

Los clientes responden combinando múltiples soluciones

Repensar la ejecución de múltiples productos de Seguridad Endpoint

"La combinación de tecnologías de múltiples proveedores pone en riesgo la proliferación de agentes y conflictos de software, lo que da como resultado características de protección deshabilitadas y configuraciones poco óptimas."

* Make Sense of Endpoint Malware Protection Technology by Ian McShane, Gartner
Published on 25 April 2017

Bitdefender

DESAFÍOS DE SEGURIDAD INFORMÁTICA

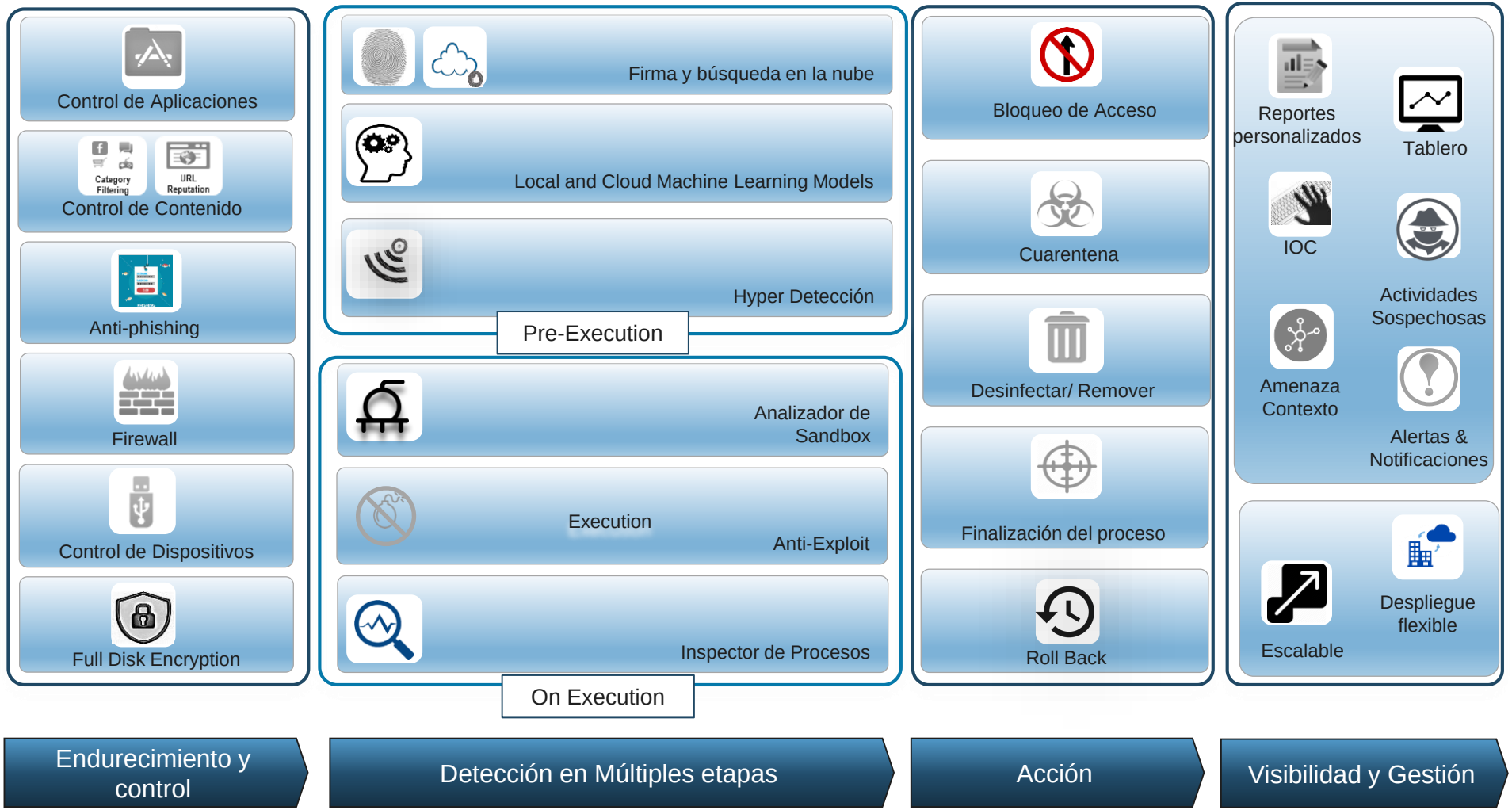
- Las amenazas avanzadas omiten la seguridad en el Endpoint.
- Aumentar las soluciones incrementa la complejidad.
- Los llamados AV de próxima generación ocasionan cantidad de falsos positivos.
- Falta de experiencia en Seguridad Informática.

SOLUCIONES BITDEFENDER

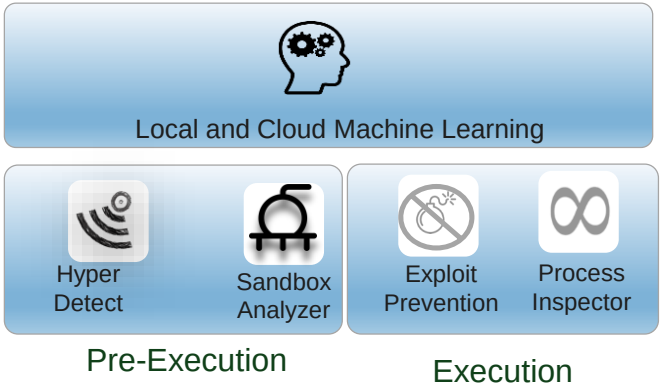
GRAVITYZONE ENDPOINT HD

La plataforma de seguridad de la próxima generación.

Bitdefender


Control de Aplicaciones
Category Filtering
URL Reputation
Control de Contenido
Anti-phishing
Firewall
Control de Dispositivos
Full Disk Encryption
Firma y búsqueda en la nube
Local and Cloud Machine Learning Models
Hyper Detección
Pre-Execution
Analizador de Sandbox
Execution
Anti-Exploit
Inspector de Procesos
On Execution
Bloqueo de Acceso
Cuarentena
Desinfectar/ Remover
Finalización del proceso
Roll Back
Reportes personalizados
Tablero
IOC
Actividades Sospechosas
Amenaza Contexto
Alertas & Notificaciones
Escalable
Despliegue flexible
Endurecimiento y control
Detección en Múltiples etapas
Acción
Visibilidad y Gestión

Powered by Signature-less Layers



Machine Learning

* Algoritmos complejos probados durante más de 8 años en el tamaño de muestra más grande: 500 M de Endpoints-sensores.
* Trillones de muestras.
* Altamente eficiente en detección,
* Nivel bajo de falso positivos

Prevención de Exploit

Tecnología de prevención proactiva contra los exploits de día cero, que
reduce la superficie de ataque, capturando APT en tiempo real.

Inspector de Procesos(ATC)

Tecnología de detección proactiva y dinámica, basada en el monitoreo continuo de procesos y eventos del sistema, y etiquetado de actividades sospechosas.
Diseñado para actuar contra amenazas desconocidas basadas en su comportamiento.

Hyper Detect* NEW!

Un nuevo conjunto de ML y modelos de análisis de comportamiento entrenados para detectar amenazas avanzadas y sofisticadas en pre-ejecución

Sandbox Analyzer* NEW!

Envío automático de archivos sospechosos desde
Endpoints a Sandbox para la detonación y análisis de comportamiento

* In GravityZone Cloud first

Bitdefender

LO NUEVO!!!

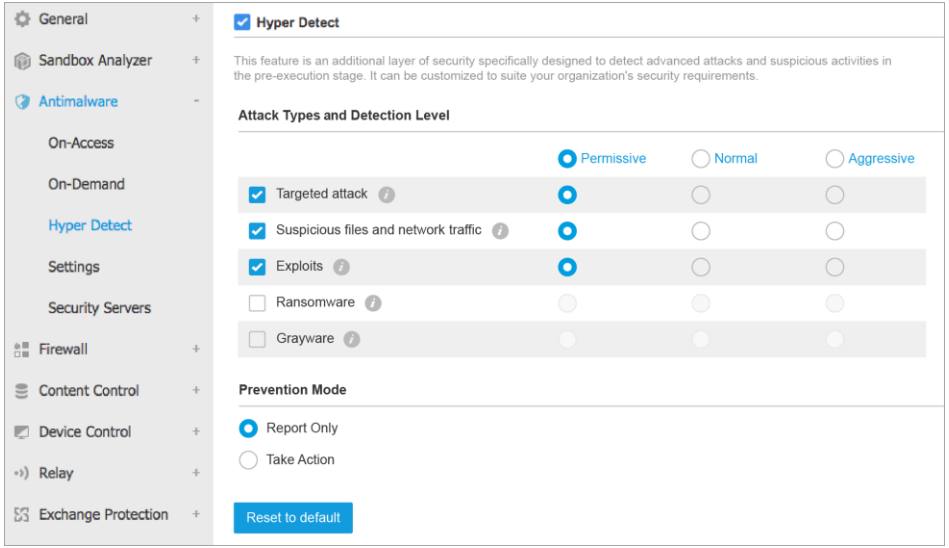
HyperDetect:
* La capa adicional de detección en la etapa previa a la ejecución presenta nuevos modelos de aprendizaje automático y tecnología de comportamiento.
* Entrenado para bloquear malware desconocido y amenazas avanzadas.

Sandbox Analyzer:
Análisis automático en espacio aislado.
* Detona archivos sospechosos en un entorno aislado.
* Realiza un análisis profundo y dinámico del comportamiento del archivo.
* Devuelve resultado de muestra y resumen de análisis detallado

Machine Learning on Steroids

Característica destacada - HyperDetect

- Prevención en pre-ejecución.
- Ninguno basado en firmas – Machine Learning + heurística avanzada.
- Detiene las amenazas sofisticadas (PowerShell, ataques sin archivos, ataques al refugio, ransomware desconocido)
- Ataque dirigido, herramientas de pirateo, anti-exploit, ransomware, PUA, tráfico web sospechoso.
- Configuraciones flexibles para optimizar la protección agresiva con bajos falsos positivos.
- Visibilidad de amenaza potencial.



General +
Antimalware -
On-Access
On-Demand
Hyper Detect
Settings
Security Servers
Sandbox Analyzer +
Firewall +
Content Control +
Device Control +
Relay +
Exchange Protection +
Encryption +

Hyper Detect

This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.

Reset to default

Protection Level

	Permissive	Normal	Aggressive
Targeted Attack	○	●	○
Suspicious files and network traffic	○	●	○
Exploits	○	●	○
Ransomware	○	●	○
Grayware	○	●	○

Actions

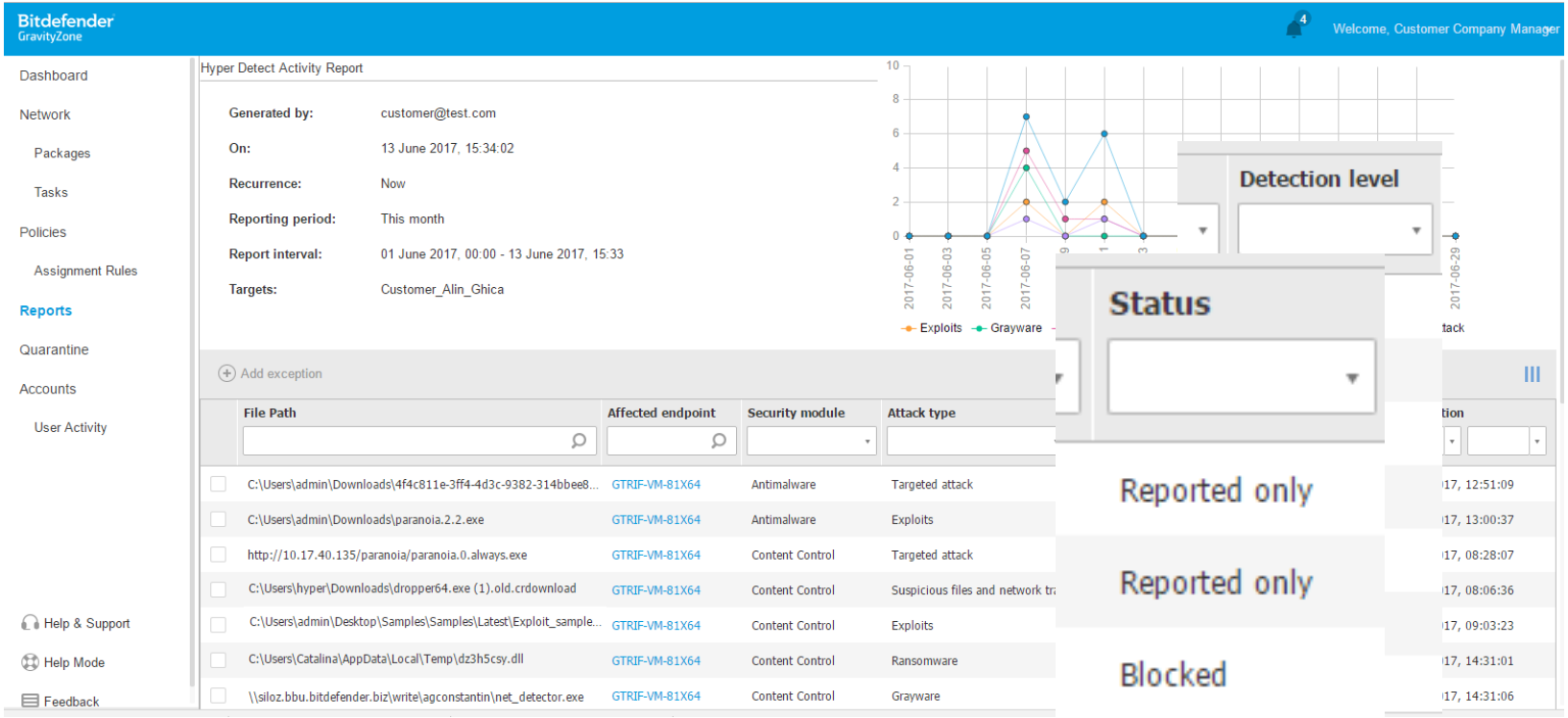
Files: Report Only — Extend reporting on higher levels

Network traffic: Block — Extend reporting on higher levels

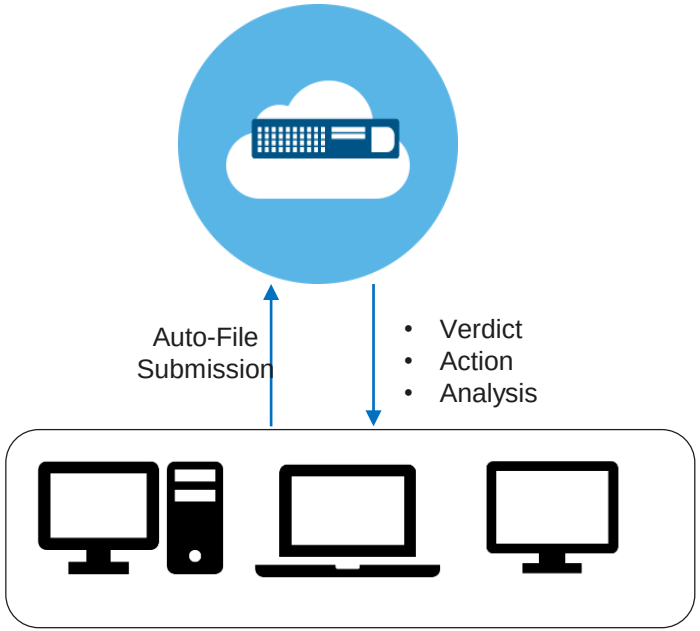
Save Cancel

INFORME HD

BLOQUEA E INFORMA EN DIFERENTES NIVELES



SANDBOZ ANALYZER:
PROTEGE CONTRA ATAQUES DIRIGIDOS Y AMENAZAS DESCONOCIDAS



Envío automático de archivos sospechosos desde los Endpoint para el análisis de Sandbox.

Opciones para bloqueo y monitoreo.

Resultados en tiempo real.

Percepción del comportamiento de archivos desconocidos.

Analice una vez, protección para toda la empresa.

Reporte Sandbox

Analysis Result

Behaviour Summary

The sample may perform certain actions over the network. This may include connecting to remote hosts or sending and reading data from different domains. Furthermore, the sample will write additional files on the system which may be used in various ways, including ensuring persistence. The sample may try to modify internet settings, DNS settings, or browser settings which may include home page or search provider settings.

%userprofile%\downloads\maria4.txt, %userprofile%\downloads\maria5.txt, %userprofile%\downloads\maria6.txt, %userprofile%\downloads\maria7.txt, %userprofile%\downloads\maria8.txt, %userprofile%\downloads\maria9.txt, %userprofile%\downloads\test.

Attempts to connect to a remote host. Malware can connect to a remote host to do any of the following: check for internet connection, report a new infection to its author, receive configuration or other data, receive instructions, search for your location, upload information etc. The original file sampledetest-infected.exe attemps to connect to the domains 90.130.70.73,

the infected system from accessing the internet. In
er pages. The original file sampledetest-infected.exe
on\internet settings\wpad, hkcu\software\microsoft
wpaddecision : 0, hkcu\software\microsoft\windows
isionreason : 1, hkcu\software\microsoft\windows
isiontime, hkcu\software\microsoft\windows
cf82418a2}\ -> wpaddecision : 0, hkcu\software
170-4272-9b13-64bcf82418a2}\ ->
n\internet settings\wpad\{6ede5dc4-
microsoft\windows\currentversion\internet
tworkname : network 9, hkcu\software\microsoft
-9b13-64bcf82418a2}\82-00-00-00-00-08.

registry keys: the original file sampledetest-
s hkcu\software\microsoft\windows\currentversion
on\internet settings\wpad\82-00-00-00-00-08,
l\{6ede5dc4-d170-4272-9b13-64bcf82418a2},
l\{6ede5dc4-d170-4272-9b13-64bcf82418a2}

keys: hkcu\software\microsoft\windows
ectedurl, hkcu\software\microsoft\windows
cf82418a2}\ -> wpaddetectedurl.

%userprofile%\downloads\maria2.txt:56907396339ca2b099bd12245f936ddc

%userprofile%\downloads\maria2.txt: 56907396339ca2b099bd12245f936ddc

Sandbox Analyzer Results Report

Generated by:

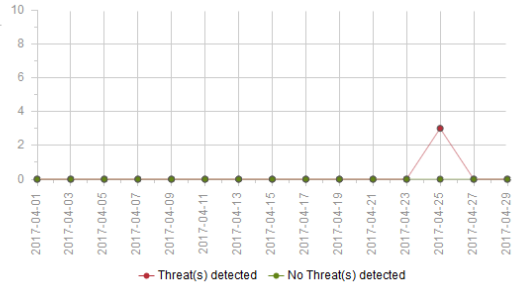
On: 10 May 2017, 10:00:32

Recurrence: Now

Reporting period: Last month

Report interval: 01 April 2017, 00:00 - 01 May 2017, 00:00

Targets: customer1



Verdict	Threat Type	Detection Timestamp	Host name/IP	Submission	Remediation	Company	Analysis Result
Threat detected	Trojan	26 Apr 2017, 09:26:14	PC / 10.17.22.76	sampleDeTest-infected.exe	Reported Only	customer1	Read more
Threat detected	Trojan	26 Apr 2017, 09:35:20	PC / 10.17.22.76	電買開.exe	Reported Only	customer1	Read more
Threat detected	Trojan	26 Apr 2017, 15:31:34	PC / 10.17.22.76	電買開.exe	Reported Only	customer1	Read more

PREVENCIÓN AVANZADA DE EXPLOITS
Protección para vulnerabilidades de día cero y sin parche.

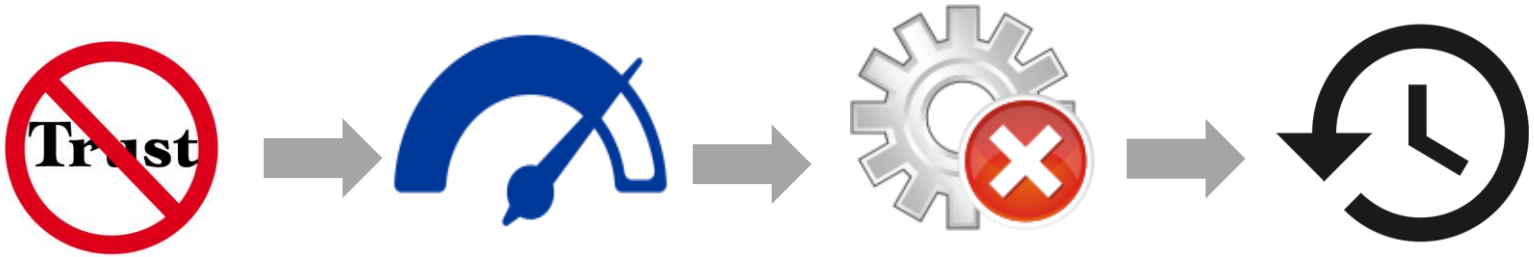
Protege aplicaciones comúnmente usadas de Microsoft y de terceros.

Se centra en herramientas y técnicas de ataque.

Sirve como una capa adicional de seguridad para las vulnerabilidades conocidas sin parches y de día cero.

Diseñado para la precisión.

INSPECTOR DE PROCESOS (ATC)
Protección contra Ataques sin Archivos



* Confianza Cero
* Controle siempre los procesos en ejecución

* Mantener el proceso basado en el comportamiento

* Emite un fallo cuando el proceso alcanza el umbral determinado.
* Finalización del proceso

* Revierte los cambios realizados por procesos maliciosos


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
Anti-Exploit
Processor Inspector
On Execution
Block Access
Quarantine
Disinfect/ Remove
Process Termination
Roll Back
Reports
Dashboard
IOC
Suspicious Activities
Threat Context
Alerts & Notifications
Scalable
Flexible Deployment
Hardening & Control
Multi-Stage Detection
Action
Visibility and Management

Beneficios para el cliente

- Eficacia de seguridad: detectar amenazas sofisticadas.
- Bajo nivel de falso positivos.
- Acciones automáticas para limitar los daños
- Mejor visibilidad.
- Ligero, agente integrado, panel único.

Protección contra amenazas avanzadas

"La eficacia de detección de mi solución Endpoint actual no es adecuada para bloquear amenazas avanzadas"

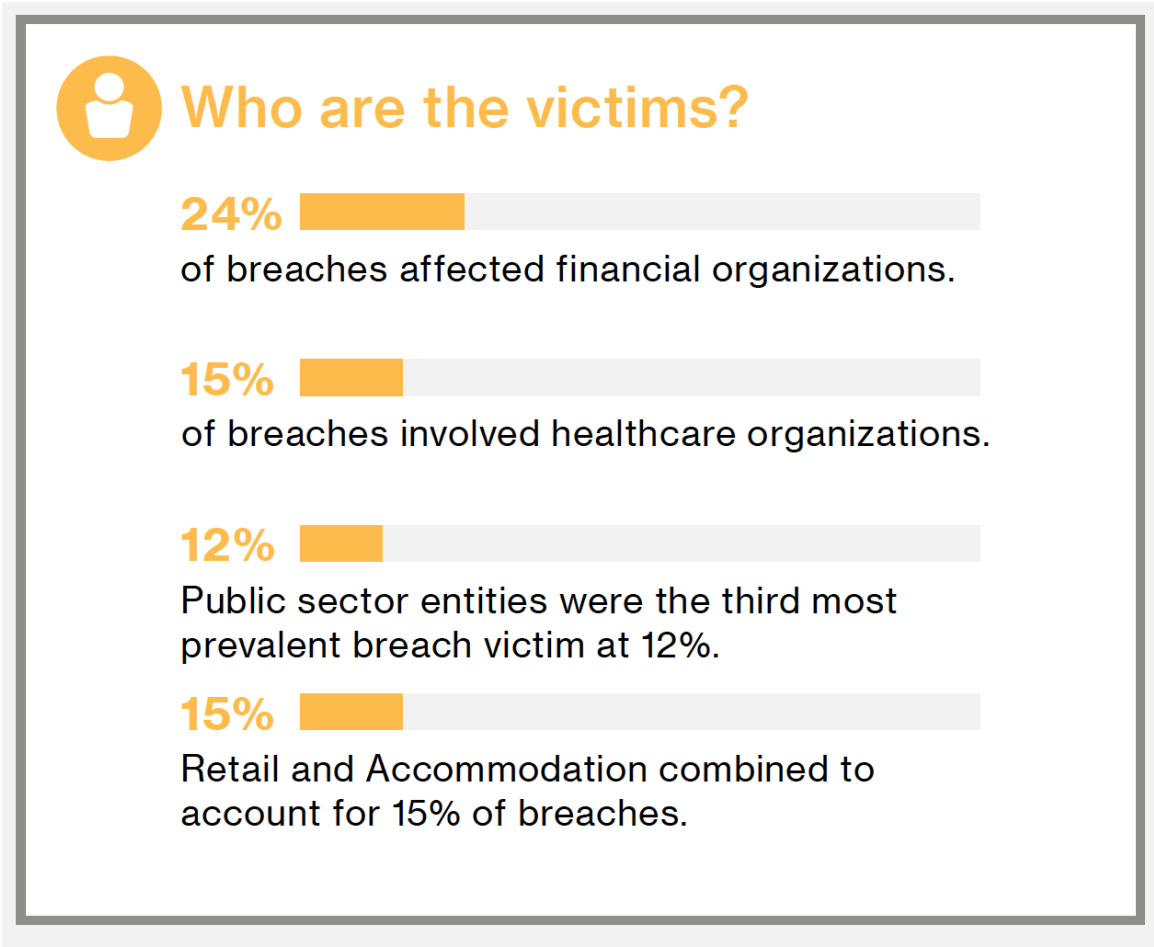
Consolidación del Endpoint/ Reducción de complejidad

"No quiero instalar varios agentes para prevención, detección y respuesta"

OPINIONES

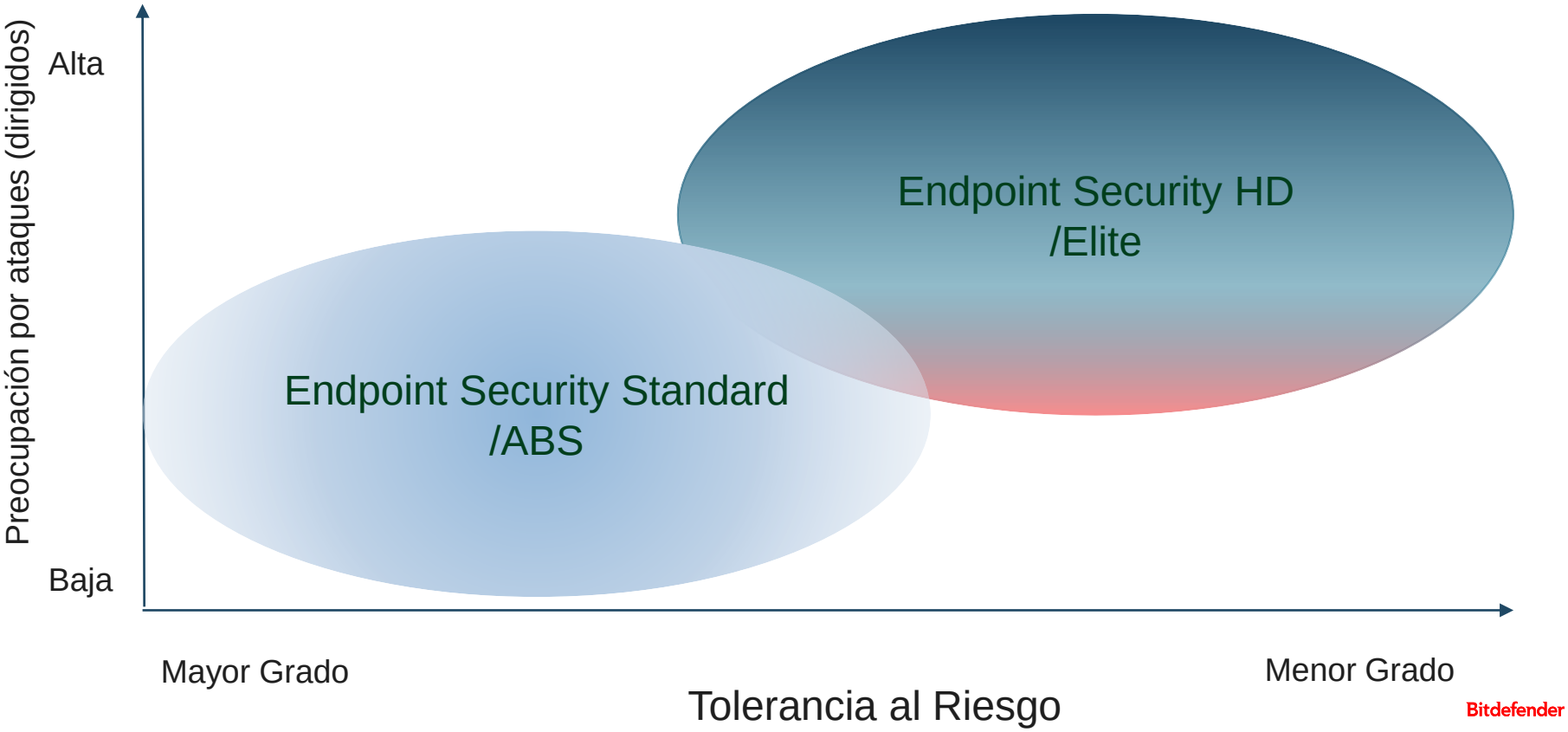
Optimizar los recursos de seguridad de TI

“Tengo un pequeño equipo y no puedo realizar inversiones adicionales en la gestión de seguridad de mis Endpoint”



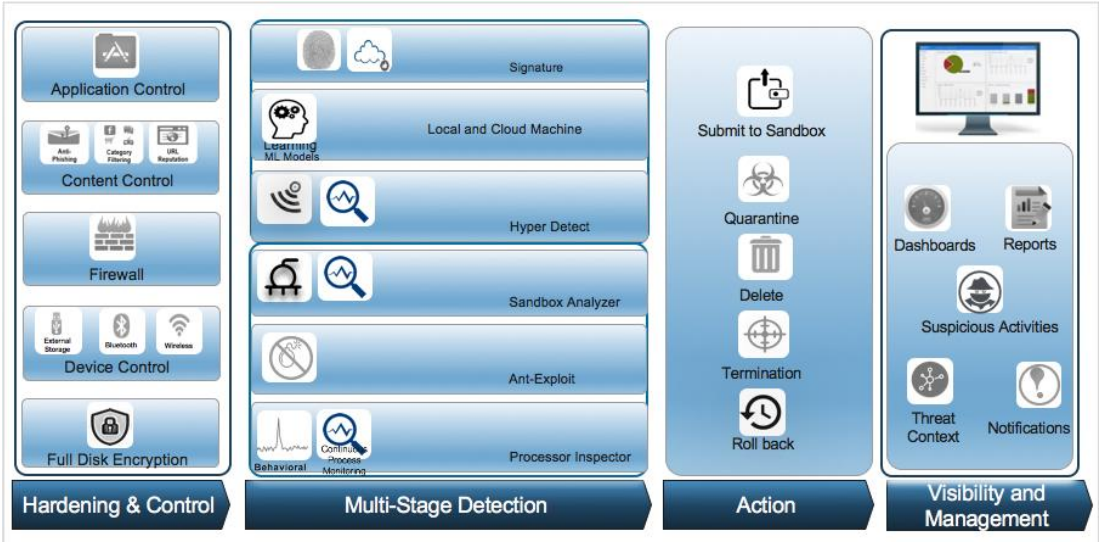
Source: 2017 Verizon Data breach investigation report

DIFERENCIAS ENTRE UN ENDPOINT STANDARD Y HD



Bitdefender

VENTAJAS COMPETITIVAS



Bitdefender Endpoint HD	●	●	●	◑
So called Next-Gen AV	◔	◕	◑	◕
Traditional EPP	●	◑	◑	◑

Bitdefender

VENTAJAS COMPETITIVAS

Bitdefender Endpoint HD VS. y los llamados Next-Gen AV

Endpoint HD

- ✓ Aprendizaje automático probado / AI
- ✓ Precisión, bajo nivel de FP.
- ✓ Detección de etapas múltiples
- ✓ FPP de próxima generación en capas.
- ✓ Un solo agente y una sola consola.
- ✓ Actuación.
- ✓ Optimizado para plataformas virtualizadas.

Los Next Gen AV

- ✓ Aprendizaje automático / sin firma.
- ✓ Alto nivel de falso positive.
- ✓ AV solo - capa única
- ✓ Agregar a Epp.

GRACIAS