

¿Qué hacer para estar más protegidos?

Gustavo Carvalho – Solutions Engineer – gcarvalho@malwarebytes.com

Riesgos emergentes



¿Cómo ocurren los ataques?

Comienza el ataque

- Phishing emails
- Fake websites
- Whatsapp/SMS
- Promociones (Black Friday/Navidad/Madres)
- Acceso remoto (RDP/VNC/TeamViewer/etc)

El objetivo es la curiosidad humana

- Miedo a reportar el problema para área de seguridad
- Nuevo software = nuevos problemas = nuevas vulnerabilidades
- Aplicar parches ya no es suficiente



Mr. Robot – Amazon Prime Video

¿Cómo protegerse?

Pero, ¿cómo protegerse de la curiosidad humana?

- Conciencia interna
- Políticas eficientes
- Herramientas eficientes
 - Solución rápida de problemas (1, 10, 60)
 - Tiempo ganado es dedicado a otras actividades



Regla 1, 10, 60

Al detectar un malware, los expertos recomiendan...

1 minuto

Detectar el problema

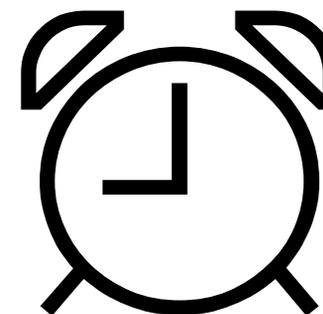
10 minutos

Investigar el problema

60 minutos

Resolver el problema

Realidad



287 días

212 días para detectar
75 días para resolver

Tiempo promedio para solucionar un
problema

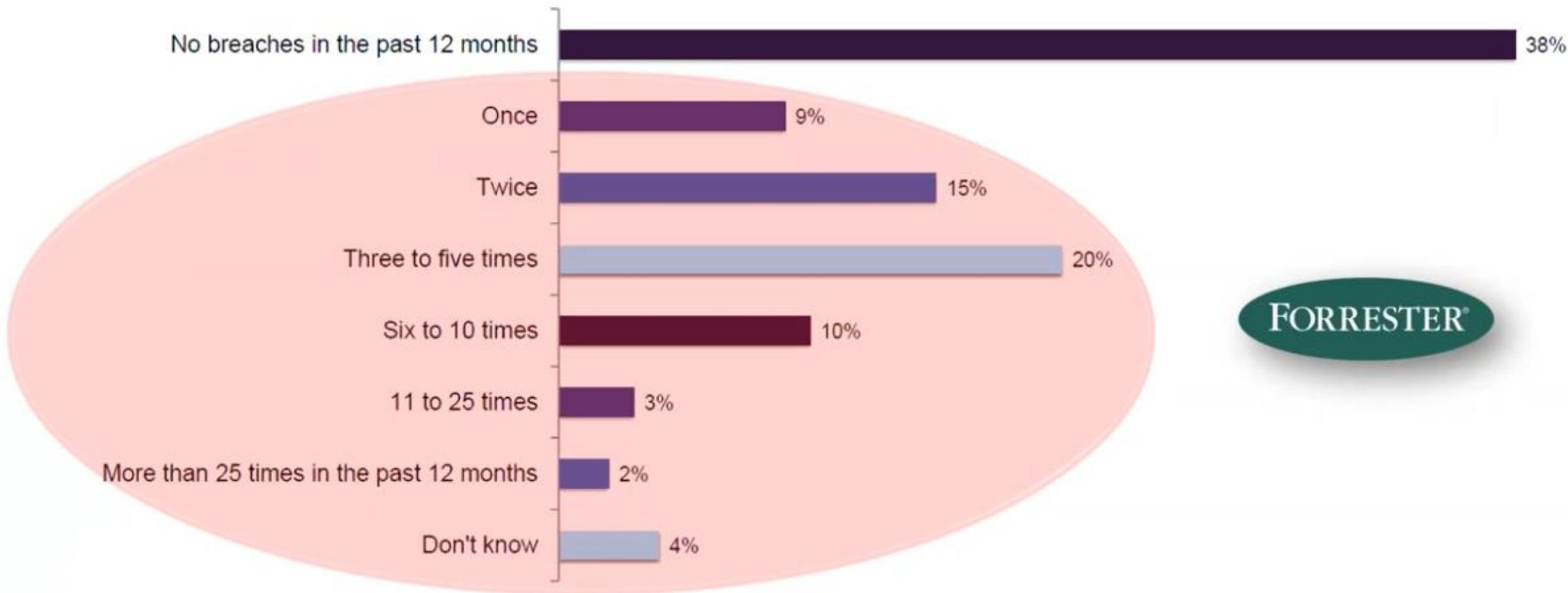
Fuente: [IBM](#)

Los ataques están aumentando

- Los ataques de ransomware han dejado de ser un juego de niños y se han convertido en negocios rentables, con grupos de atacantes que actúan como empresas (ex. ReVil Corp.)
- Los ejecutores de amenazas se centran en las vulnerabilidades a explotar
- Cada 11 segundos, se realiza un nuevo ataque
- El pago promedio de rescate es US\$ 250.000,00
- Después de un ataque, el 60% de las pequeñas y medianas empresas cierran sus puertas



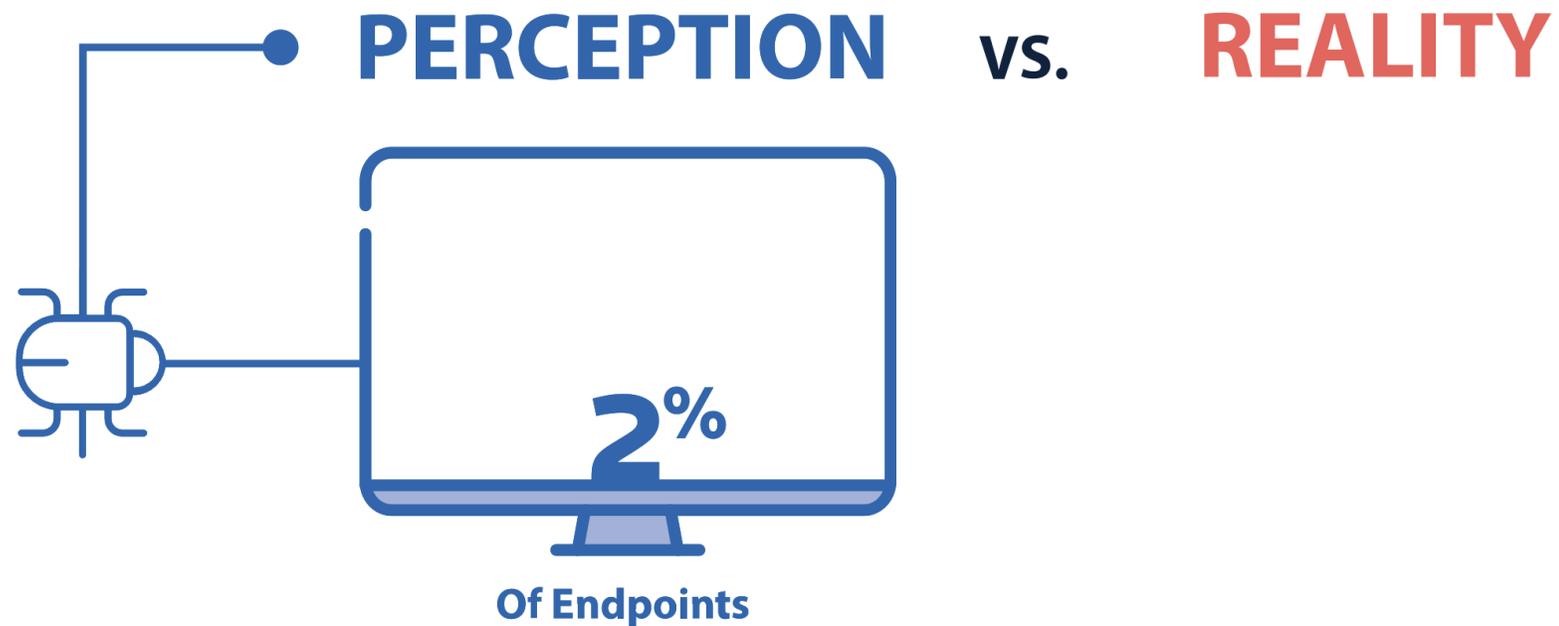
Casi dos tercios de las empresas han tenido algún ataque



Base: 1,195 security decision-makers with network, data center, app security, or security ops responsibilities; Source: Forrester Analytics Business Technographics® Security Survey, 2020



Percepción x Realidad



Anatomía de un ataque

Vertical movement



Phish



RDP



Gap

Lateral movement



Malware APT



Malware spread



Malware spread



Malware spread



Ransomware



Ransom

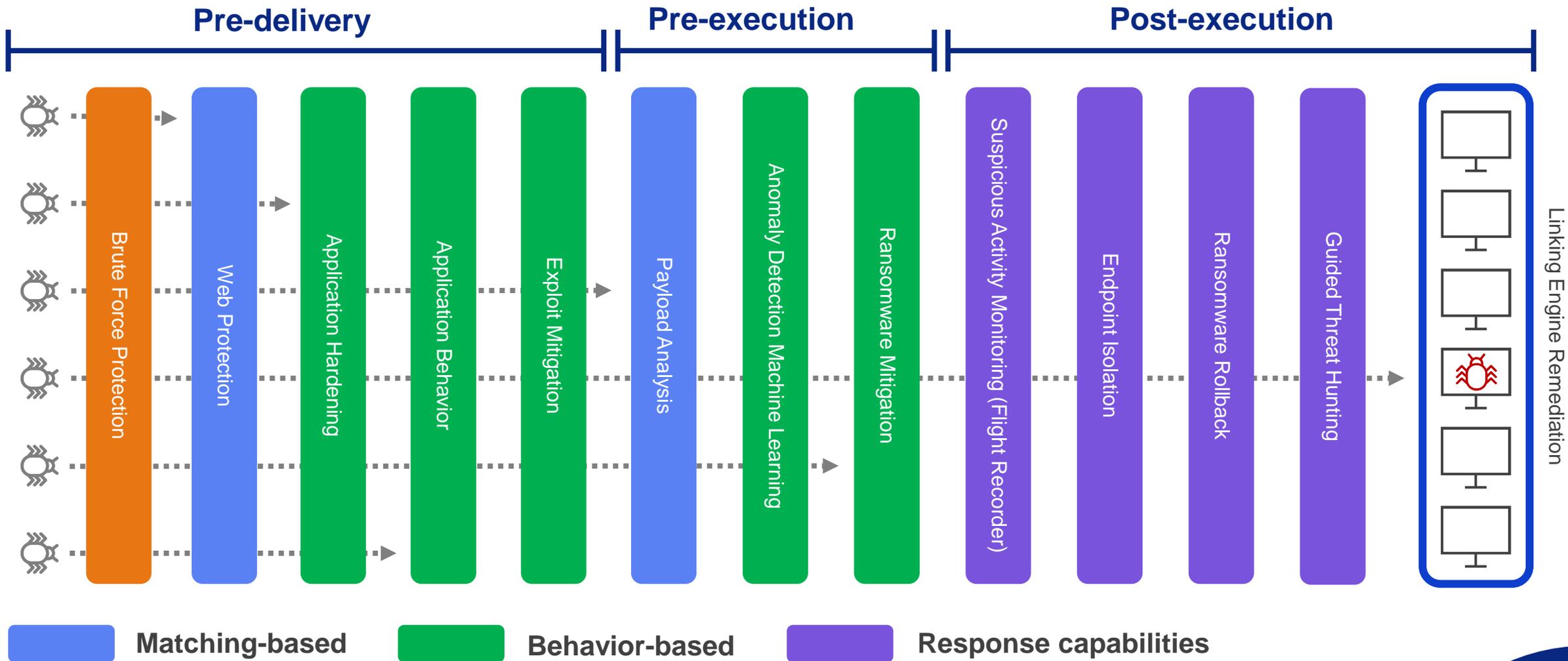


Damage



APT = Advanced Persistent Threat

Detección, protección y respuesta Multi-Vectorial



Evaluación de Vulnerabilidades

- Identificar vulnerabilidades críticas
- Evalúe aplicaciones heredadas y modernas
- Comprender la prioridad en su ecosistema
- Conocimiento para actuar
- Actualizamos su aplicación

Malwarebytes Nebula | Gustavo Carvalho Super Admin

Displaying records for Vulnerabilities

Export [icon] [icon]

Critical	High	Medium	Low	Unknown	CISA Recommended
204 3 endpoints affected	603 36 endpoints affected	954 34 endpoints affected	119 6 endpoints affected	0	1880

Showing 1880 of 1880.

Drag column headers here to group results

<input type="checkbox"/>	CVE	Application	OS platform	Identified Date	Severity	CISA Recommended	Endpoint
<input type="checkbox"/>	CVE-2016-0940	Adobe Reader	Windows	23/04/2022 04:02:22	High	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0941	Adobe Reader	Windows	23/04/2022 04:02:22	Medium	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0942	Adobe Reader	Windows	23/04/2022 04:02:22	Critical	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0943	Adobe Reader	Windows	23/04/2022 04:02:22	Medium	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0944	Adobe Reader	Windows	23/04/2022 04:02:22	High	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0945	Adobe Reader	Windows	23/04/2022 04:02:22	High	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0946	Adobe Reader	Windows	23/04/2022 04:02:22	Critical	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-0947	Adobe Reader	Windows	23/04/2022 04:02:22	Medium	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-1007	Adobe Reader	Windows	23/04/2022 04:02:22	Critical	CISA Recommended	DI
<input type="checkbox"/>	CVE-2016-1008	Adobe Reader	Windows	23/04/2022 04:02:22	High	CISA Recommended	DI

Gestión de Parches

- Simplificar el proceso de aplicación de parches
- Ordenar y priorizar la implementación
- Catálogo continuamente actualizado
- Parches simultâneos, inmediatos y programados

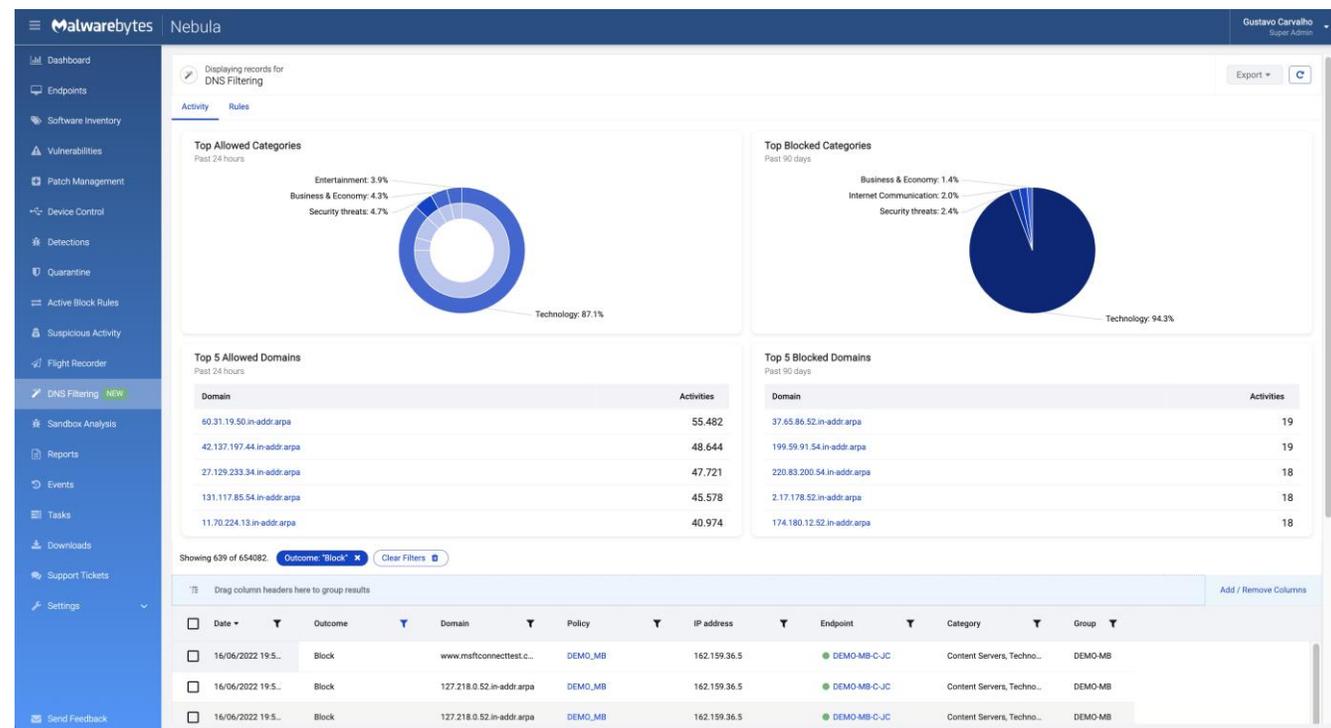
The screenshot displays the Malwarebytes Nebula Patch Management interface. The top navigation bar includes the Malwarebytes logo, the name 'Nebula', and the user 'Gustavo Carvalho .ORG Super Admin'. The left sidebar contains various system management options like Dashboard, Endpoints, Software Inventory, Vulnerabilities, Patch Management, Device Control, Detections, Quarantine, Active Block Rules, Suspicious Activity, Flight Recorder, DNS Filtering (NEW), Sandbox Analysis, Reports, Events, Tasks, Downloads, and Send Feedback.

The main content area is titled 'Patch Management' and is split into 'OS Patches' and 'Software Updates'. It shows a summary of patch records for OS Patches, categorized by severity: Critical (3, 2 endpoints affected), Important (110, 29 endpoints affected), Moderate (0), Low (0), and Unknown (19, 16 endpoints affected). Below this, a table lists 132 records, with the first three visible:

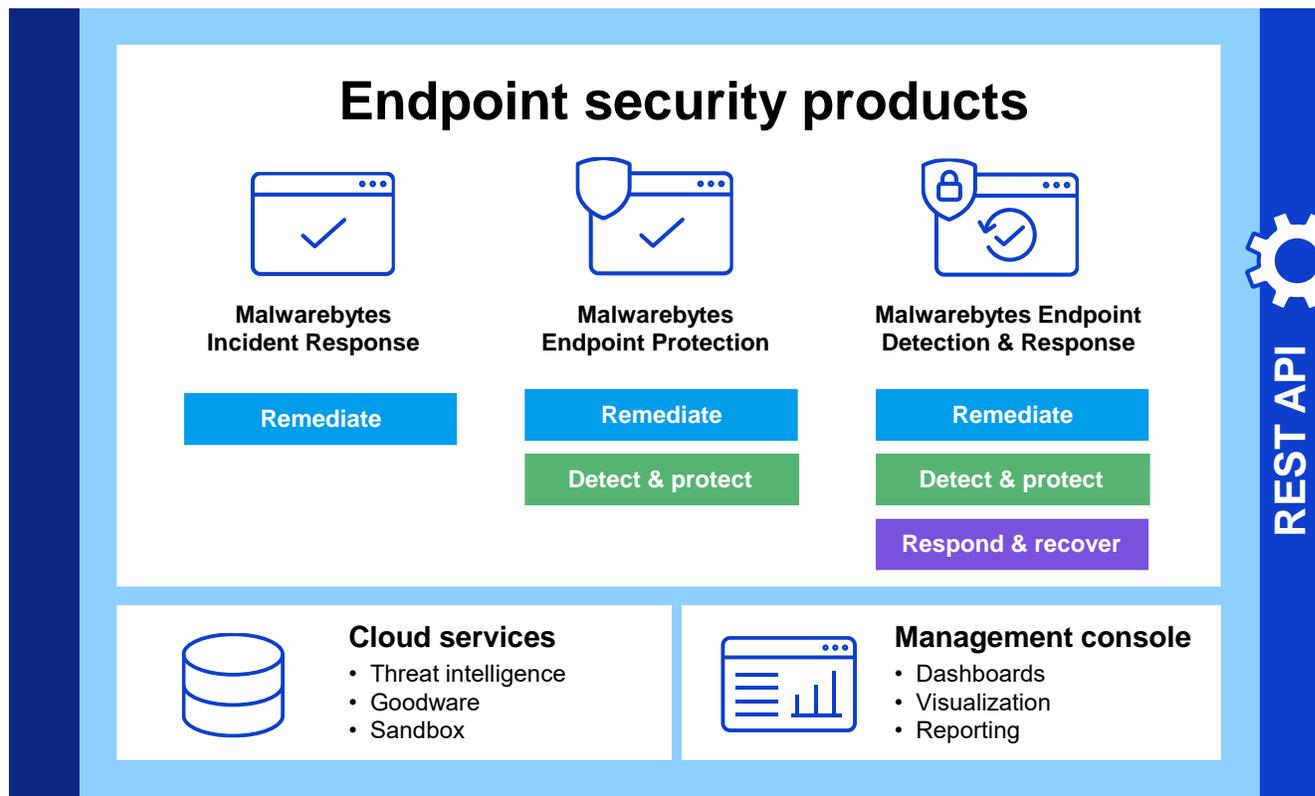
Severity	Endpoint	Patch	Category	KB ID
Critical	RE-TEST-2016S	2022-03 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5011570)	Security update	501157
	RE-TEST-2016S	2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5012596)	Security update	501259
	VA-SERVER-201	2022-03 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5011570)	Security update	501157

Filtrado de DNS

- Cifre el tráfico DNS para protegerse contra la información de dominio filtrada, utilizando DNS a través de HTTPS (DoH)
- Protección contra actores de amenazas que crean dominios web falsos
- Aísle las interacciones del navegador y las aplicaciones web contra las amenazas
- Bloqueos y permisos configurables



¿Cómo podemos ayudar?





Gracias

gcarvalho@malwarebytes.com

csantana@malwarebytes.com