Malwarebytes

¿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

Mr. Robot – Amazon Prime Video

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

¿Cómo protegerse?

Pero, ¿cómo protegerse de la curiosidad humana?

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

Regla 1, 10, 60

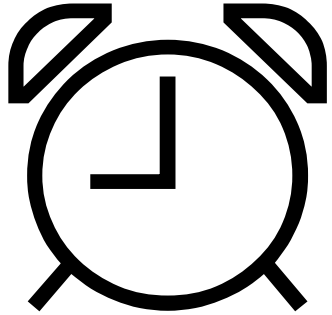
Al detectar un malware, los expertos recomiendan...

1 minuto
Detectar el problema

10 minutos
Investigar el problema

60 minutos
Resolver el problema

Realidad



287 dias

212 dias para detectar
75 dias para resolver

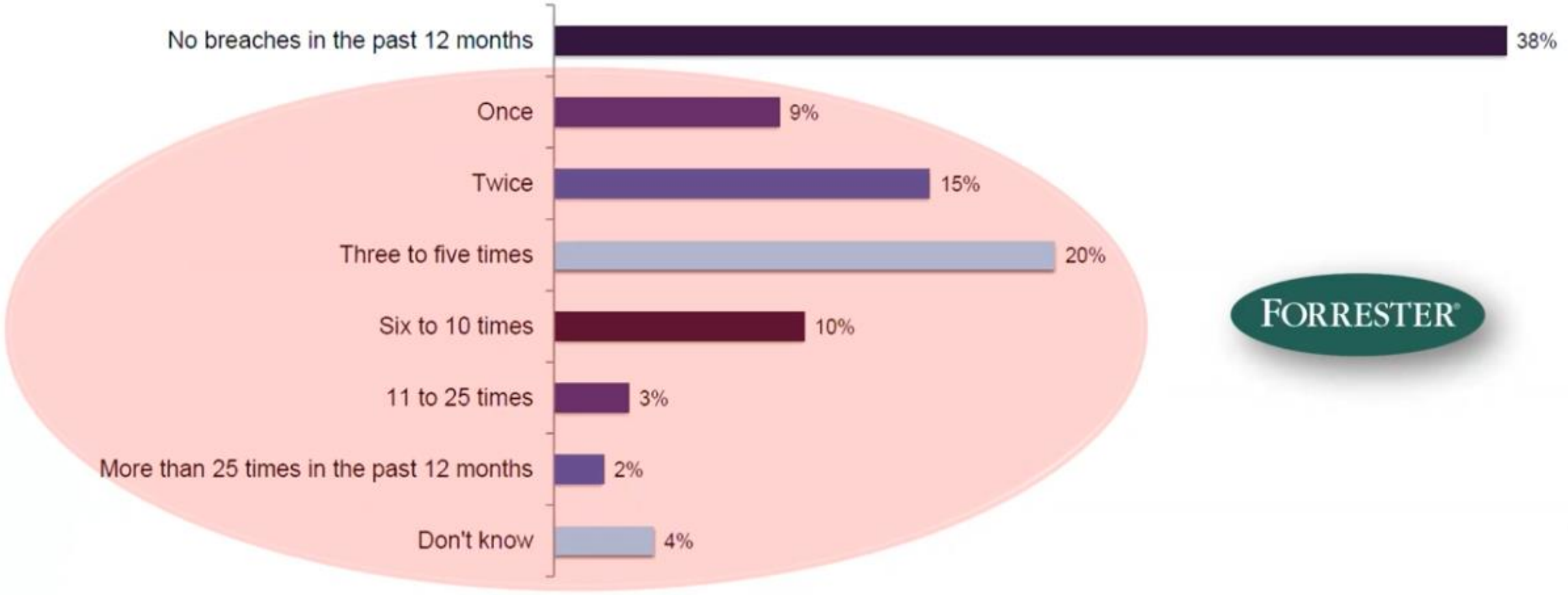
Tiempo promedio para solucionar un problema

Fuente: IBM

Los ataques están aumentando

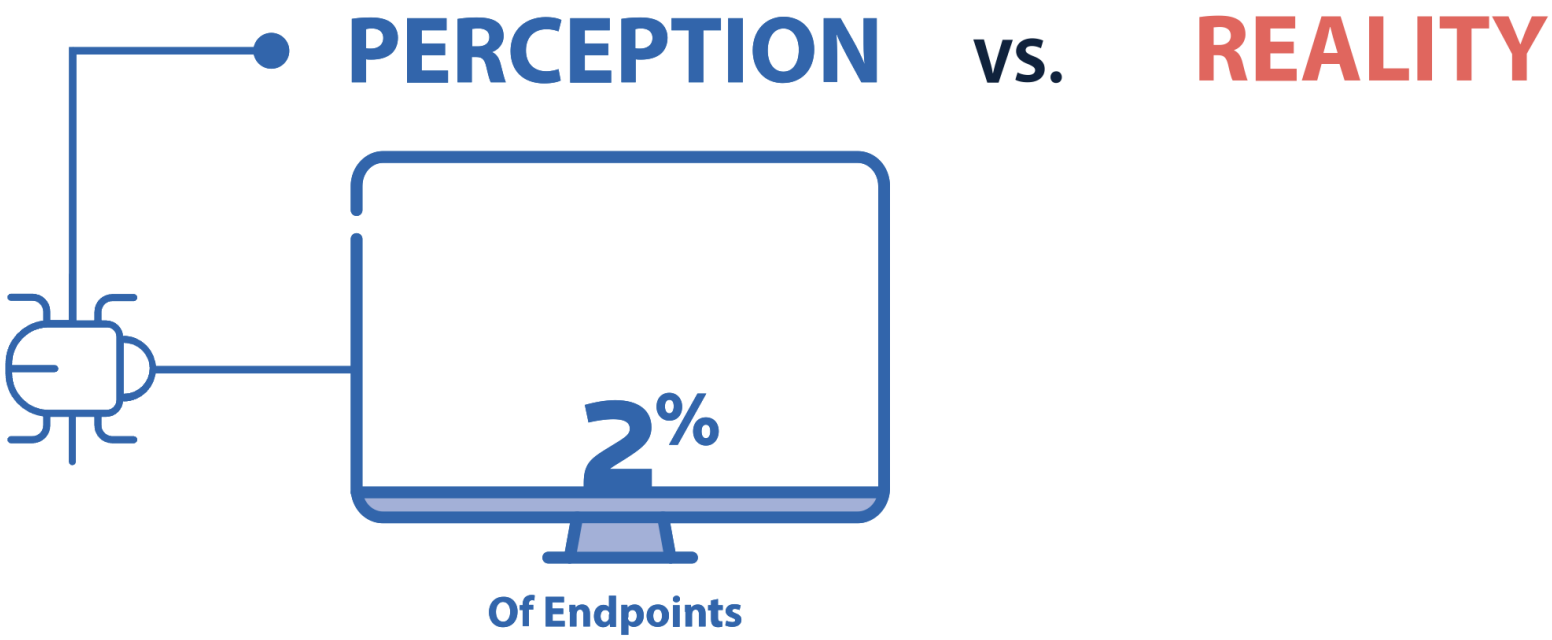
- Los ataques de ransomware han dejado de ser un juego de niños y se han convertido en negocios rentables, con grupos de atacantes que actúan como empresas (ex. ReVil Corp.)
- Los ejecutores de amenazas se centran en las vulnerabilidades a explotar
- Cada 11 segundos, se realiza un nuevo ataque
- El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

Casi dos tercios de las empresas han tenido algún ataque

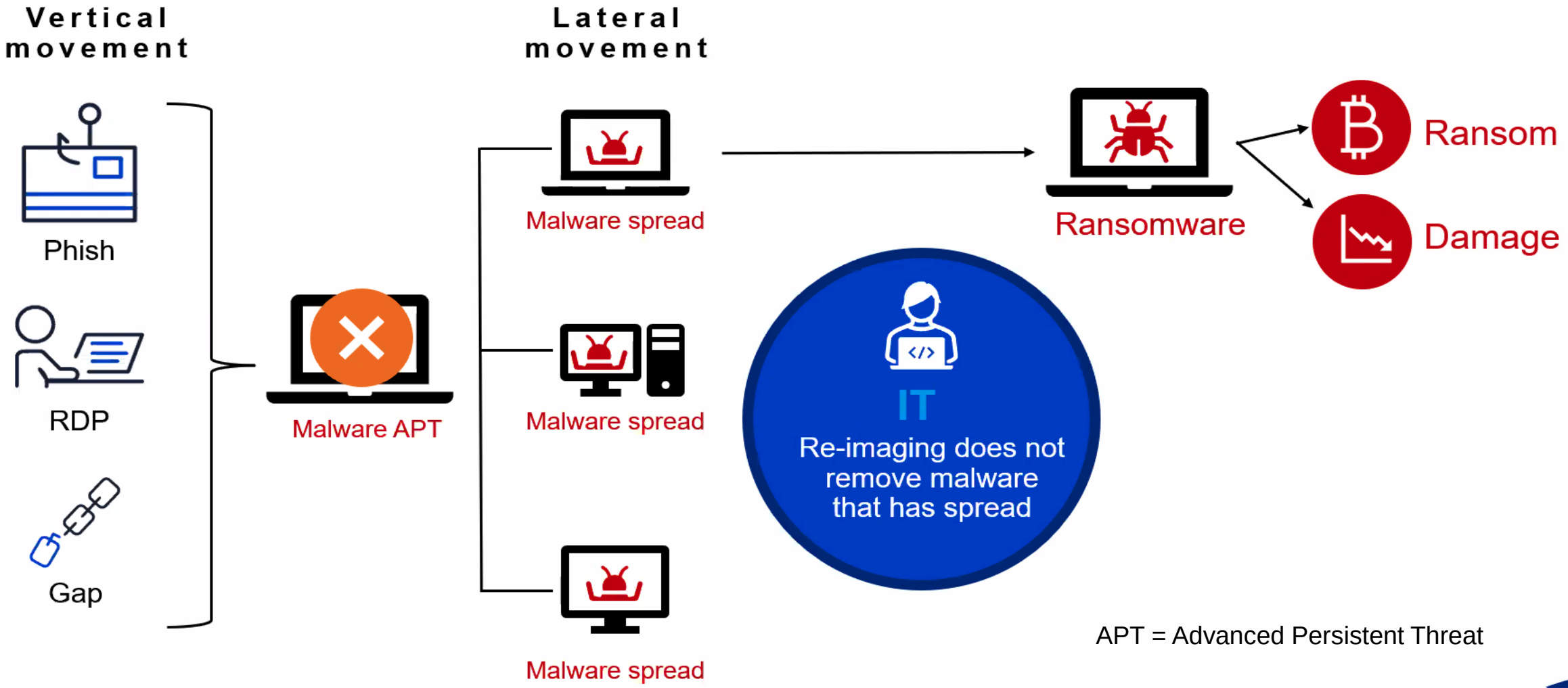


Base: 1,195 security decision-makers with network, data center, app security, or security ops responsibilities; Source: Forrester Analytics Business Technographics® Security Survey, 2020

Percepción x Realidad

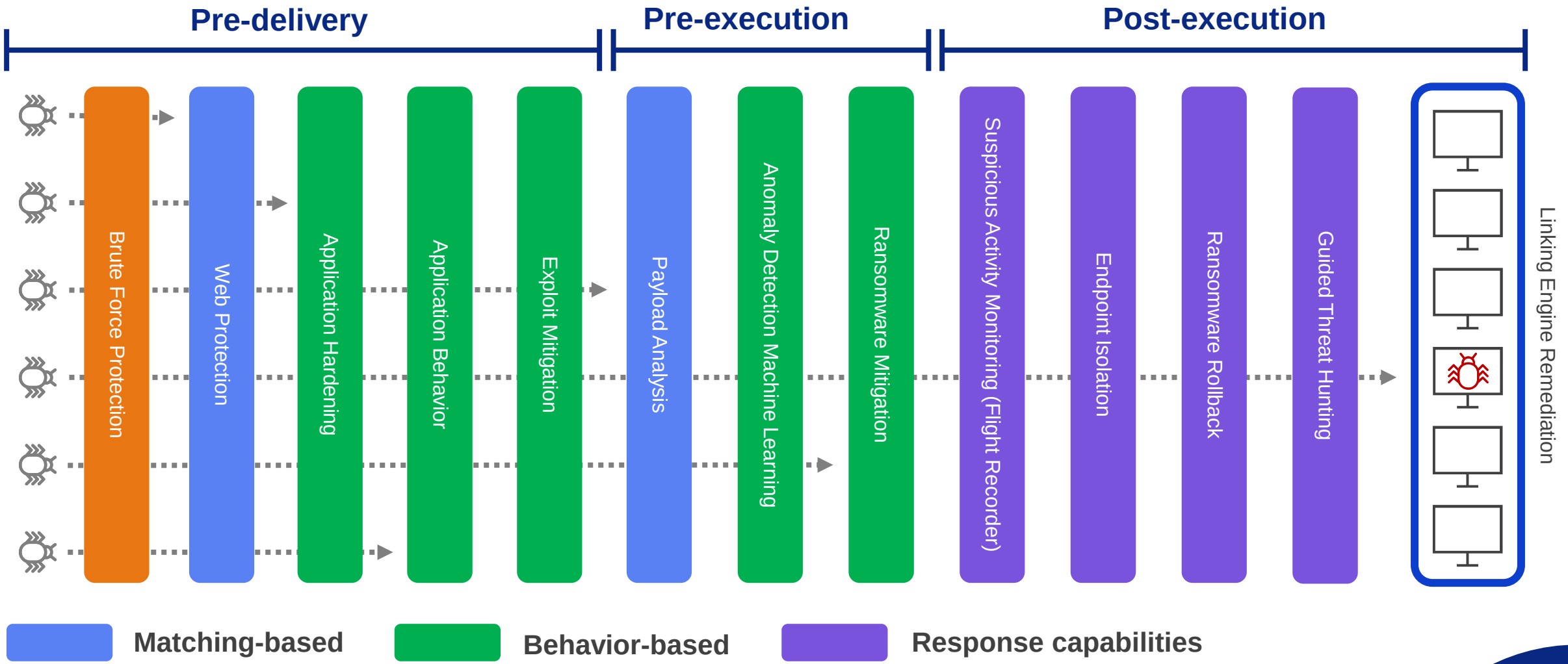


Anatomía de un ataque



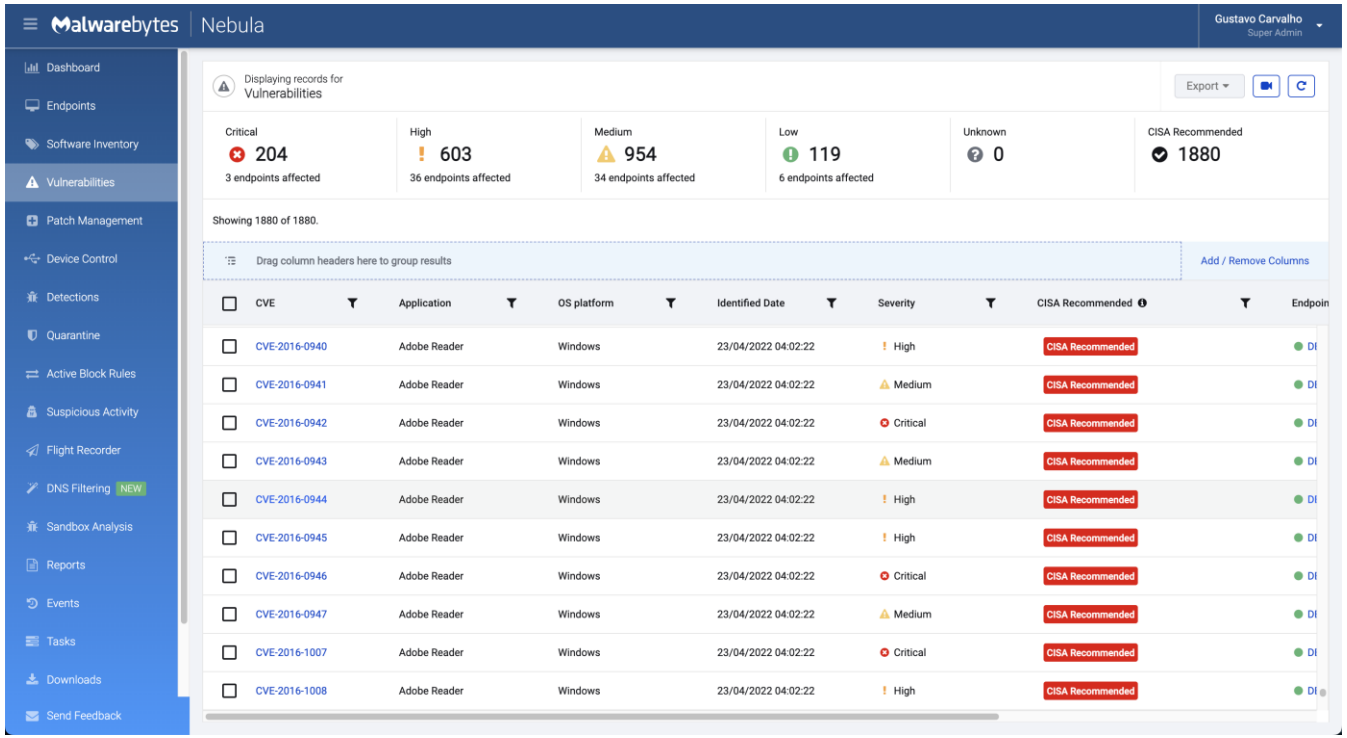
APT = Advanced Persistent Threat

Detección, proteccion y respuesta Multi-Vectorial



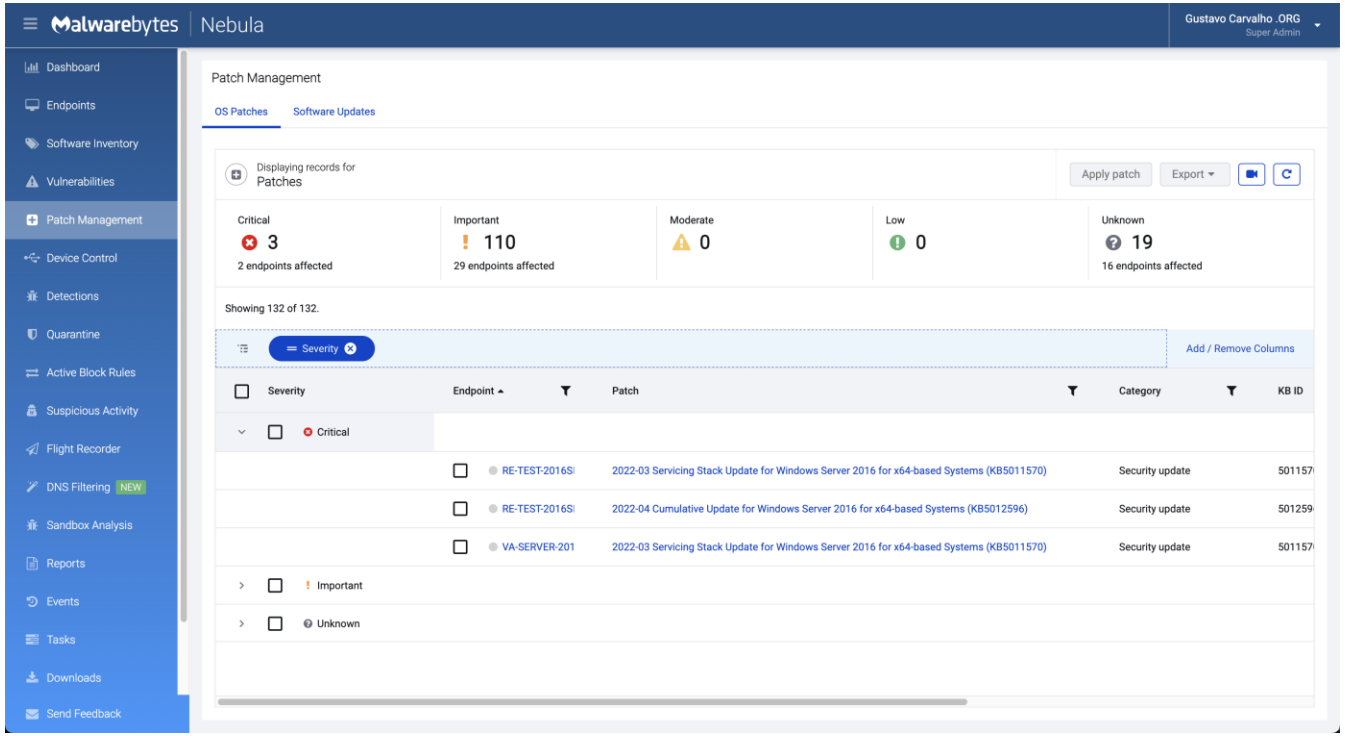
Evaluación de Vulnerabilidades

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



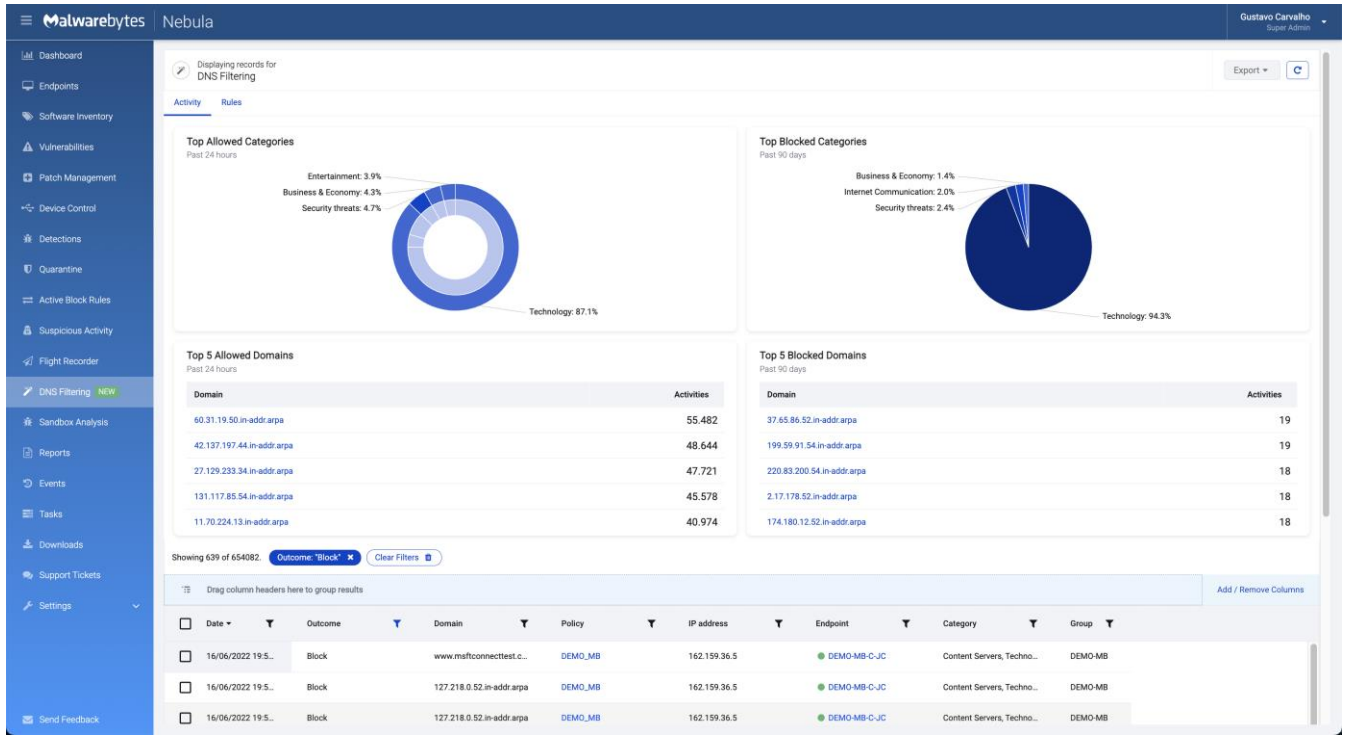
Gestión de Parches

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



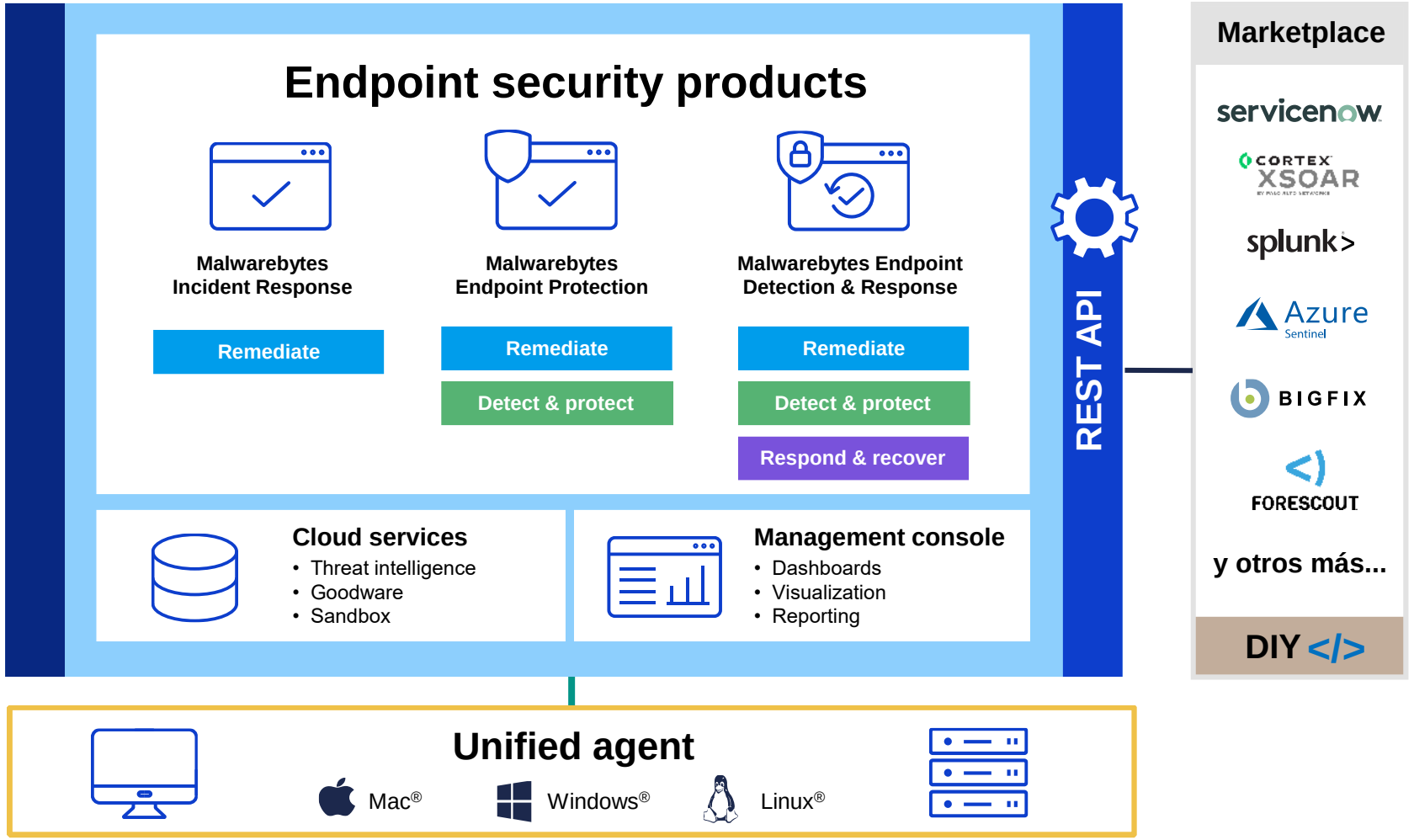
Filtrado de DNS

- 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?

NEBULA
CLOUD PLATFORM



Malwarebytes

Gracias

gcarvalho@malwarebytes.com
csantana@malwarebytes.com