Construyendo un plan de ciberdefensa más allá de los límites para el sector educativo

.

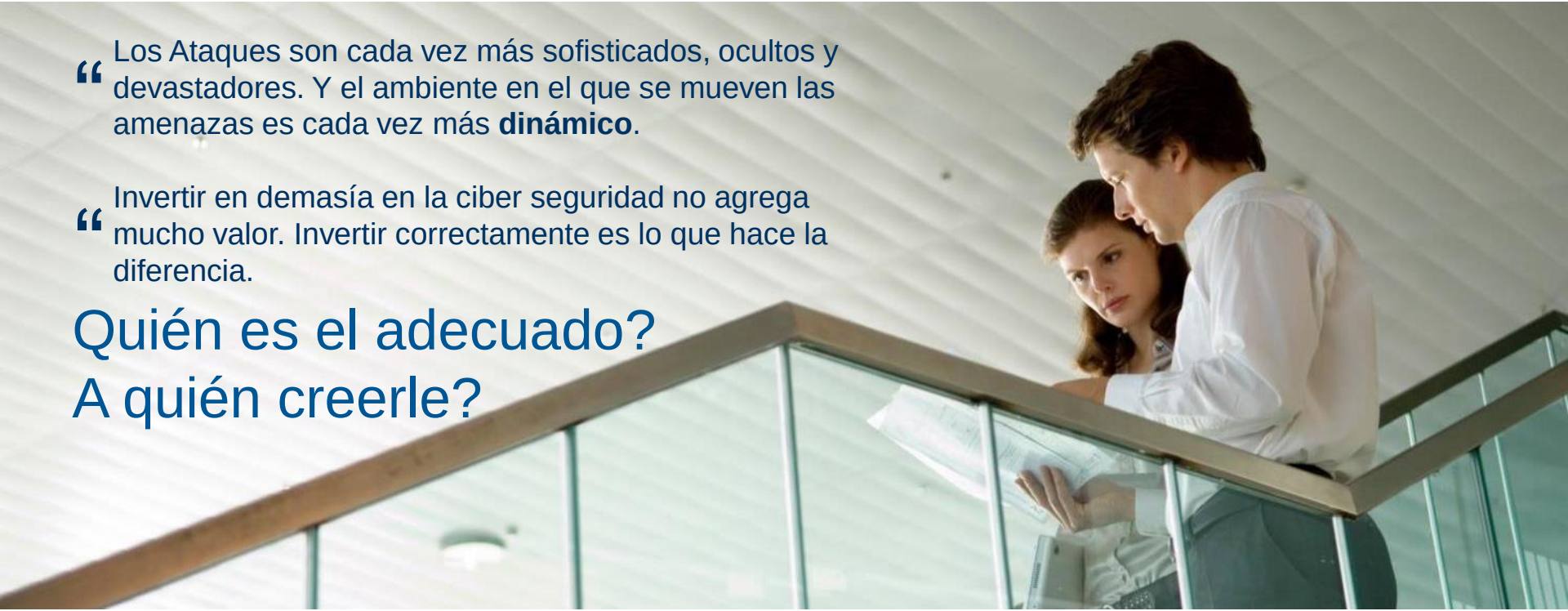
MTIA Jorge Antonio Claret Cisneros Diego de Arribas

Senior Sales Engineer NGFW

McAfee México

Intel & McAfee Confidential

Un Día Normal para un CISO y Su Equipo a Cargo de la Seguridad de la Red



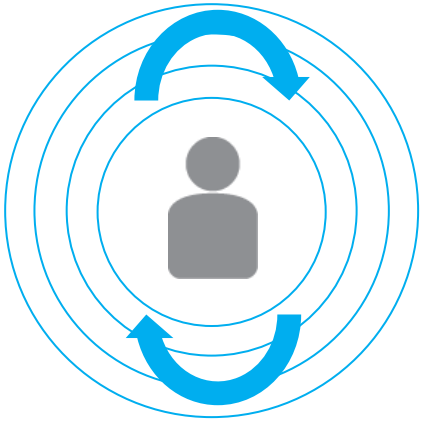
> Los Ataques son cada vez más sofisticados, ocultos y devastadores. Y el ambiente en el que se mueven las amenazas es cada vez más **dinámico**.

> Invertir en demasía en la ciber seguridad no agrega mucho valor. Invertir correctamente es lo que hace la diferencia.

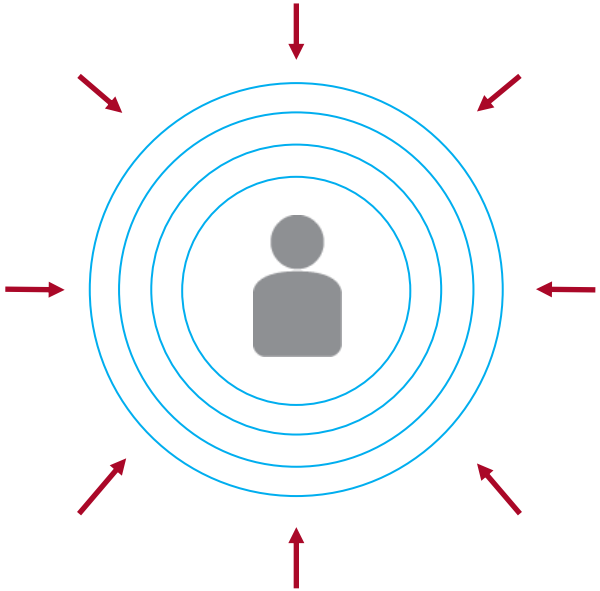
Quién es el adecuado?
A quién creerle?

Prólogo

La ley de la seguridad de red



TODO esta conectado con direcciones IP y digitalmente en red…



..Y **TODO** lo conectado y en red se encuentra vulnerable.

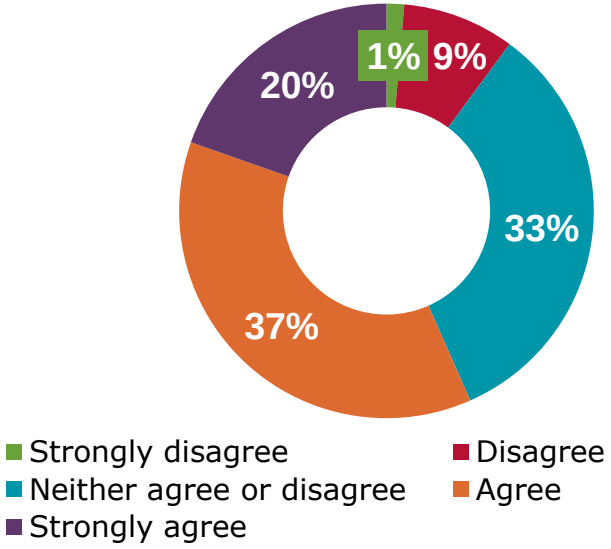
Por lo tanto **TODO** puede ser hackeado!

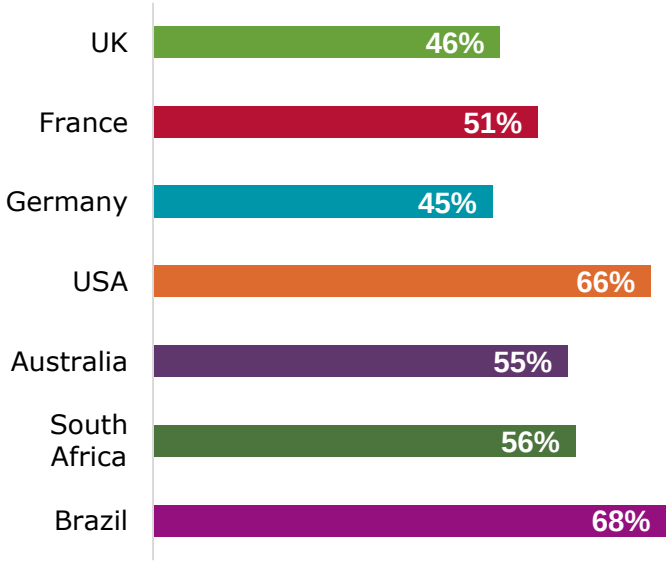
El extraño Ciber Mundo de hoy

El surgimiento de ciber ataques **AVANZADOS** y **EVASIVOS**.

Observando el Nacimiento

De Técnicas Avanzadas de Evasión



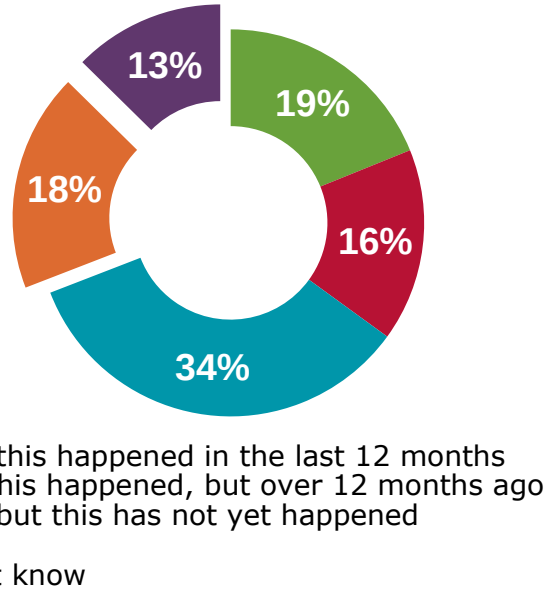


"Por favor indique que tan de acuerdo está con lo siguiente"
AETs representan una amenaza inmediata a mi negocio
De una muestra de empresas corporativas (800)

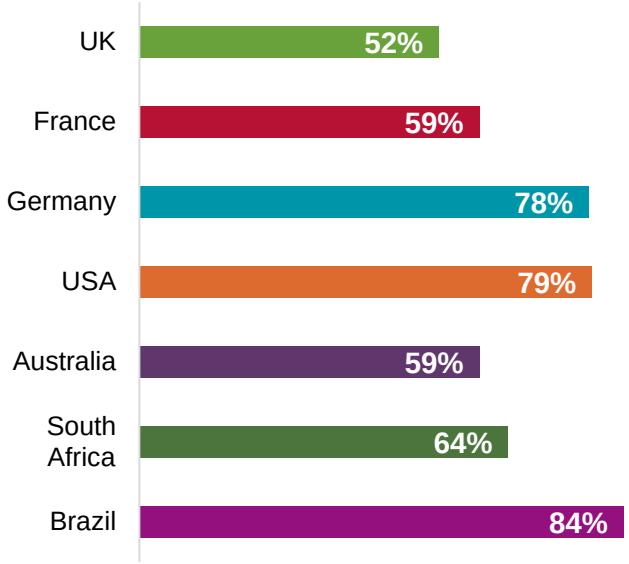
Análisis de aquellos que estuvieron de acuerdo que los AETs representan una amenaza actualmente – por país
De una muestra de empresas corporativas (800)

El Mundo Real

de las Técnicas Avanzadas de Evasión



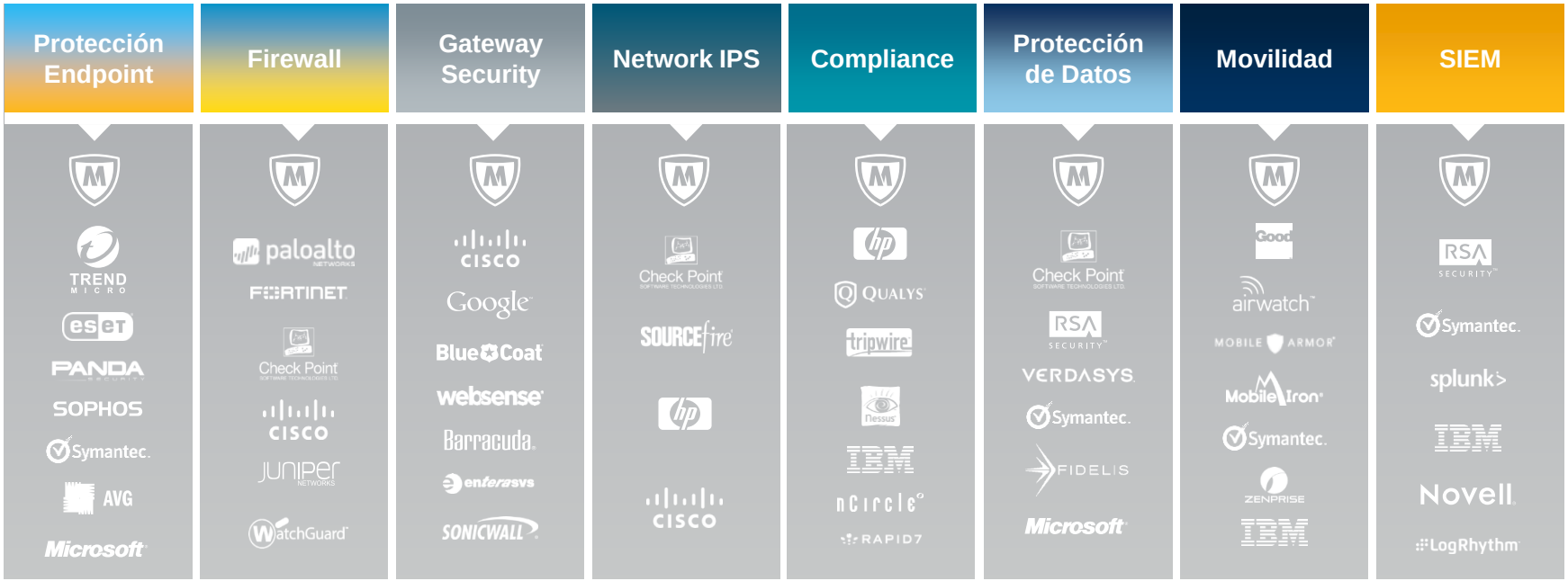
"Los AETs han permitido redescubrir y explotar vulnerabilidades conocidas en su ambiente actual?"
De una muestra corporativa (800)



Análsis de las organizaciones que piensan que las AETs pueden redescubrir vulnerabilidades conocidas en sus ambientes
De una muestra corporativa (800)

Construyendo Seguridad basado en Silo

El proceso de adquisición de la Tecnología ha generado caos en el ámbito de la seguridad

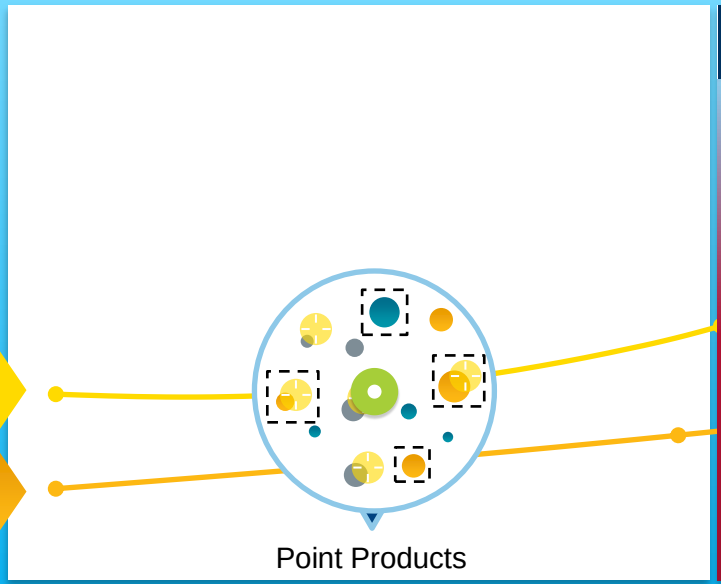


Construyendo Seguridad basado en Silos

Creando una Falsa Sensación de Seguridad

TCO
CapEx + OpEx

Security Posture



Lecciones Aprendidas

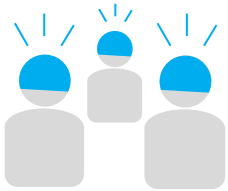
- Organizaciones con presupuesto no significa organizaciones bien protegidas
- Cumplir el compliance no deriva en protección
- Alertas Masivas en un mar de ruido no permite acción inmediata
- La Defensa operando en silos esta destinada a fallar

Parity → TIME → Advancement

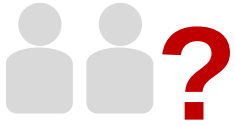
Es Responsabilidad de Todos!

El Flujo del Ciber Sufrimiento

USUARIO(S)
Baja Productividad

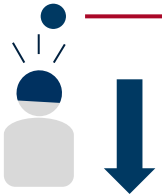


ADMINS
Extra Trabajo, Presión en el tiempo



GESTIÓN DE LA RED Y LA SEGURIDAD
- Trabajo de Gestión
- Presión Profesional
- Necesidad de Cambio

CYBER SHOCK



CEO
Valor de las Acciones

VENTAS & MARKETING
Confianza del Cliente

CFO
Impacto Económico

CIO
Falla en Habilitar el negocio y la estrategia

Ataques Dirigidos

Existen dos Tipos de Víctimas:

AQUELLOS CON ALGO DE VALOR

AQUELLOS QUE SON VICTIMAS OBVIAS.

Definiciones

ADVANCED PERSISTENT THREAT

"**Un atacante altamente motivado** implementando un ataque enfocado. Utiliza múltiples metodos de hacking y malware avanzado con el objetivo de penetrar y mantenerse oculto por un periodo largo de tiempo. Con frecuencia utiliza AETs para mejorar su porcentaje de éxito al intentar penetrar la red."

MALWARE AVANZADO Y EVASIVO PARA ATAQUES BASADOS EN HOST

"**Cualquier tipo de malware** diseñado y desarrollado para operar y no poder ser detectado mientras penetra en puntos de acceso y hosts objetivo."

TECNICAS AVANZADAS DE EVASION EN AMBIENTES DE RED

"**Son Técnicas especificas de hacking** que han sido desarrolladas para burlar los dispositivos de seguridad y entregar código malicioso o un exploit a un objetivo sin ser detectado. Los AETs pueden ser utilizados para entregar exploits y contenido malicioso conocido y no tan conocido..

Porque preocuparnos HOY?

Que tal les va a los AETs en contra de los productos líderes de nueva generación?

7 CASO DE PRUEBA (Conficker worm)	ATAQUES DE AET EXITOSOS (NO detectados)
Divide exploit in IP fragments	70%
Divide exploit in TCP segments	90%
Using grey areas of protocols to hide the exploit	90%
Change byte encoding methods	40%
TCP segmentation and re-ordering	80%
TCP segmentation and re-ordering + urgent data	90%
Sending TCP payload with old timestamps (PAWS)	80%

CISCO

TippingPoint

paloalto NETWORKS

JUNIPER NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

SOURCEfire®

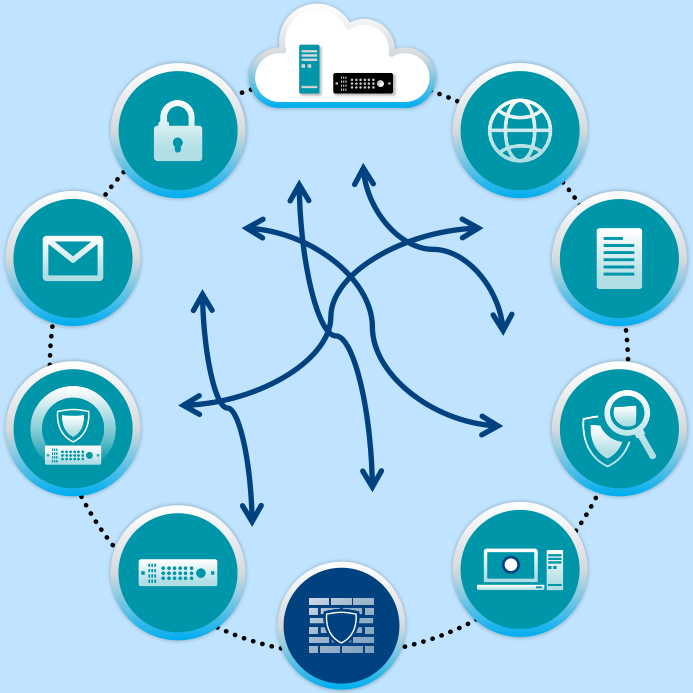
FORTINET

Evolución de la Seguridad Conectada

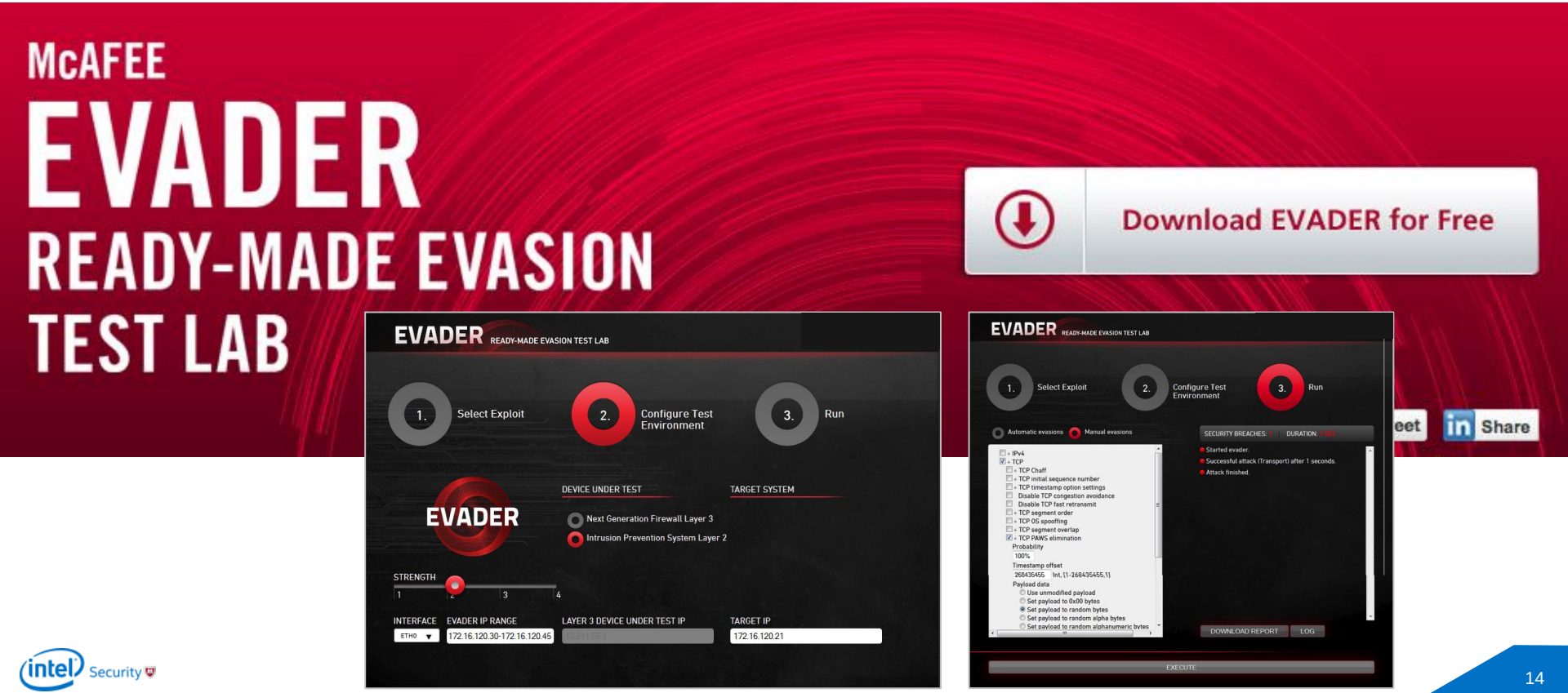
Eliminando Obstaculos Comunes

Una Arquitectura Conectada NO es…

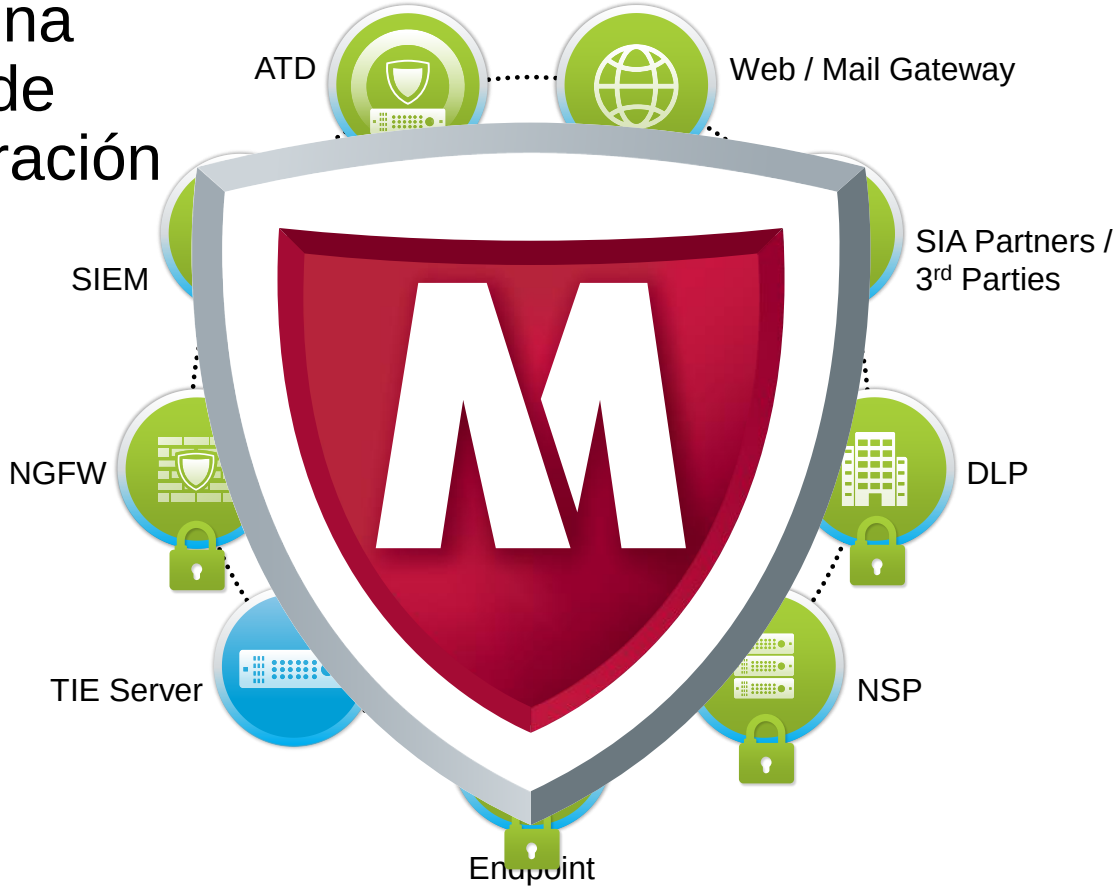
- Soluciones de una sola marca
- Una Arquitectura Monolítica
- Agregar Continuamente Nuevas Tecnologías
- Un entorno nuevo con más recursos que gestionar
- Reemplazo Masivo de la Infraestructura de Seguridad



McAfee Evader



Habilitando una arquitectura de Nueva Generación



Una plataforma completa con Protección entregada lista para implementar

Analíticos	RA TOMA DE DECISIONES EFECTIVAS
Inteligencia de Amenazas	BLE PROPORCIONA PROTECCION ROBUSTA
Contramedidas	COBE ENSIVA AMPLIA DESDE EL ENDPOINT HASTA LA RED
Gestión de Seguridad	GESTION SIMPLIFICADA REDUCE EL ESFUERZO Y EL COSTO
Contexto y Orquestación	INTERCAMBIO DE DATOS INTEGRADO OFRECE UNA DEFENSA CON MENOS HUECOS

Servicios Profesionales Foundstone

McAfee Security Services

*"With a worldwide presence across the **Americas**, Europe, the Middle East, Africa, and Asia Pacific, our teams are skilled experts in all **McAfee products and McAfee Foundstone services**. McAfee Professional Services also collaborates with key partners and alliance organizations to deliver our services, enabling customization to meet your business requirements."*

Solution Services
- Products Deployments
- Preventive Maintenance
- Products Health Checks
- Assisted Operation

Education Services
- McAfee Product Education
- McAfee Foundstone Security Education
- McAfee Certification

Foundstone Practice
- Strategic Consulting
- Technology Consulting

Seguridad Conectada de McAfee Ha sido Probada Exitosamente

NOTE: The NSS Labs evasion test consists of approx. 60 static, recorded AETs that can be easily fingerprinted.

Lo Recomenado para Malware y Ataques de Evasión

…que sus tecnologías de seguridad de red tengan la capacidad de **detectar, detener, correlacionar y generar reportes** de **APT y AET**.

…adquiera únicamente capacidad real de APT y AET.

…y verifique el estatus de protección contra AET y APT.
No confie solo en la palabra de su fabricante.

Intel & McAfee Confidential