Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT : MAS ALLA DEL FIREWALL

Cyber Kill Chain , Check Point Defense

Daniel Gonzalez / TAM BAJIO.

Agenda

- Check Point
- Ciberseguridad en la actualidad
- Attack Modeling
- Zero Trust
- Preguntas

Check Point: "pure play" de ciberseguridad mas grande del mundo

- Líder Global – 100,000+ Clientes, 88+ Países, 6,200+ Socios
- Más de 29 años de tecnologías de punta, altamente reconocido por su visión
- Liderazgo en innovación: mayor cantidad de desarrolladores
- Operando en Nasdaq desde 1996 - CHKP
- 5,200+ Empleados a nivel mundial con gran talento

ELEGIDO POR LAS COMPAÑIAS DE FORTUNE 500

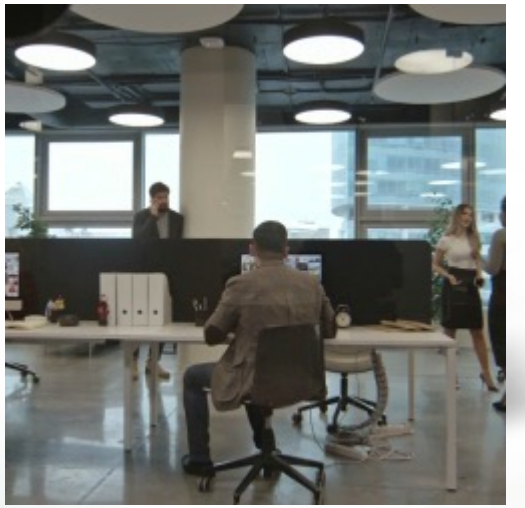
CIBERSEGURIDAD EN LA ACTUALIDAD

¿Se define el alcance de las amenazas correctamente?


Superficie ampliada
Amenazas no contempladas
Nuevos vectores

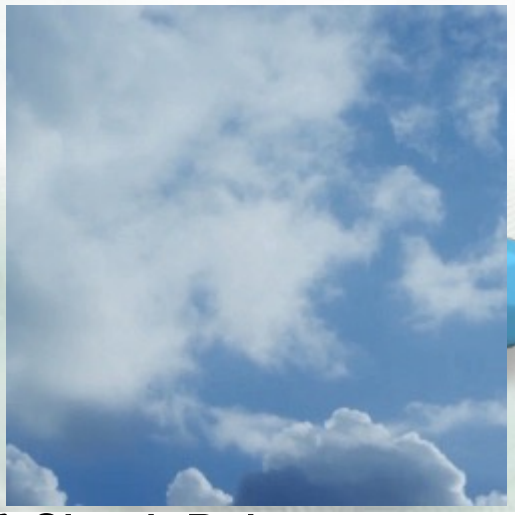
LAS SUPERFICIES DE ATAQUE SE AMPLIARON

Los empleados pueden ser atacados mientras:

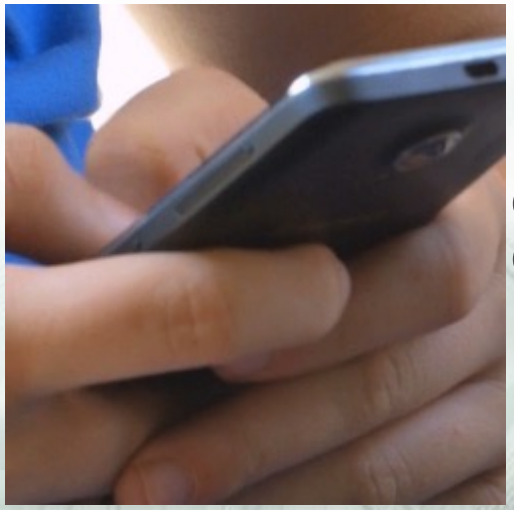


Se encuentran trabajando en la **red** corporativa

Se conectan de forma remota utilizando sus **computadoras**



Utilizan aplicaciones o estructura en **nube**



Utilizan servicios corporativos accediendo con sus **celulares**

Amenazas actuales

Actores de amenaza motivados y bien financiados

MALICIOUS INSIDERS

TERRORISTAS

CRIMEN ORGANIZADO

HACKTIVISTS

NATION STATES

Ataques sofisticados y evasivos

ATAQUES FILELESS

MALWARE

ATAQUES WEB

ZERO-DAY EXPLOITS

RANSOMWARE

Factor humano

ERROR DE CONFIGURACION

COMPROMISO FÍSICO (ROBO O PÉRDIDA)

INGENIERÍA SOCIAL

CREDENCIALES COMPROMETIDAS

CORREOS MALICIOSOS

Vectores de ataque mas comunes

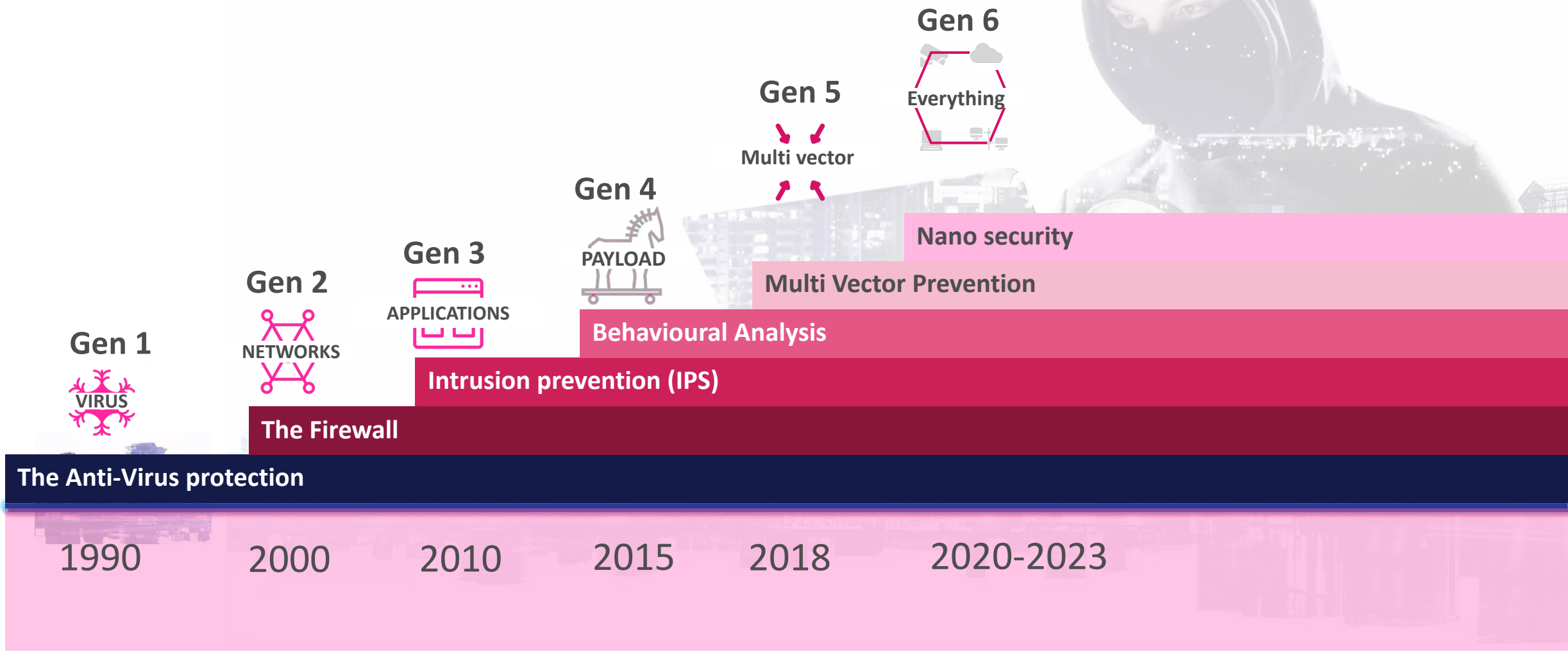
SUPERFICIES → / VECTORES ↓	 Red	 Endpoint	 Nube	 Mobile
E-mail		Exchange	Exchange	Exchange
Web				
File Sharing				
Phishing				
Man in the Middle		Redes Vulneradas		Redes Vulneradas
Apps Maliciosas				


POR QUE
TANTO IMPACTO?

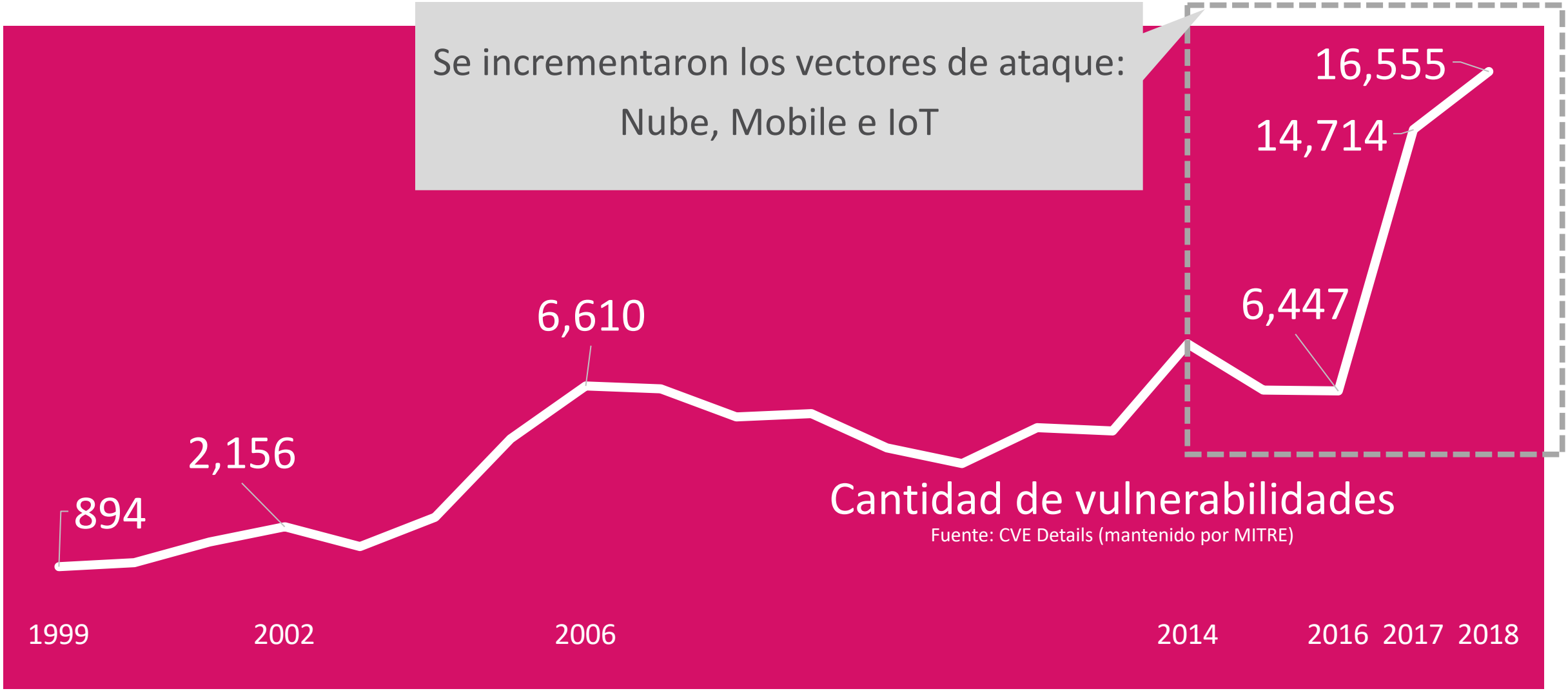
#1 Mentalidad en reacción.

Sí se acepta la Reaccción
ya se está perdido

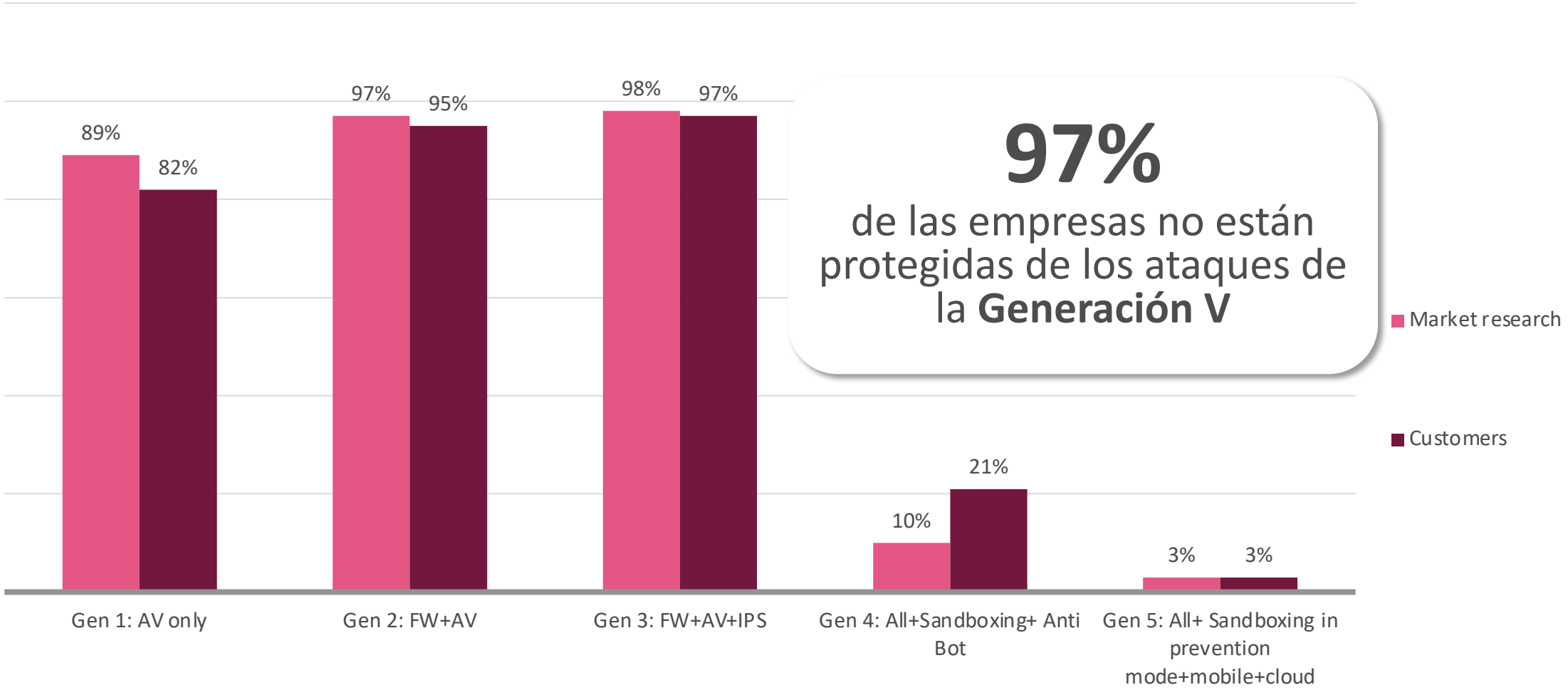
#2 – Sin protección contra los ataques actuales (Contexto , AI. Big Data.)



Incremento de vulnerabilidades en los últimos años…



Generaciones de seguridad VS Clientes

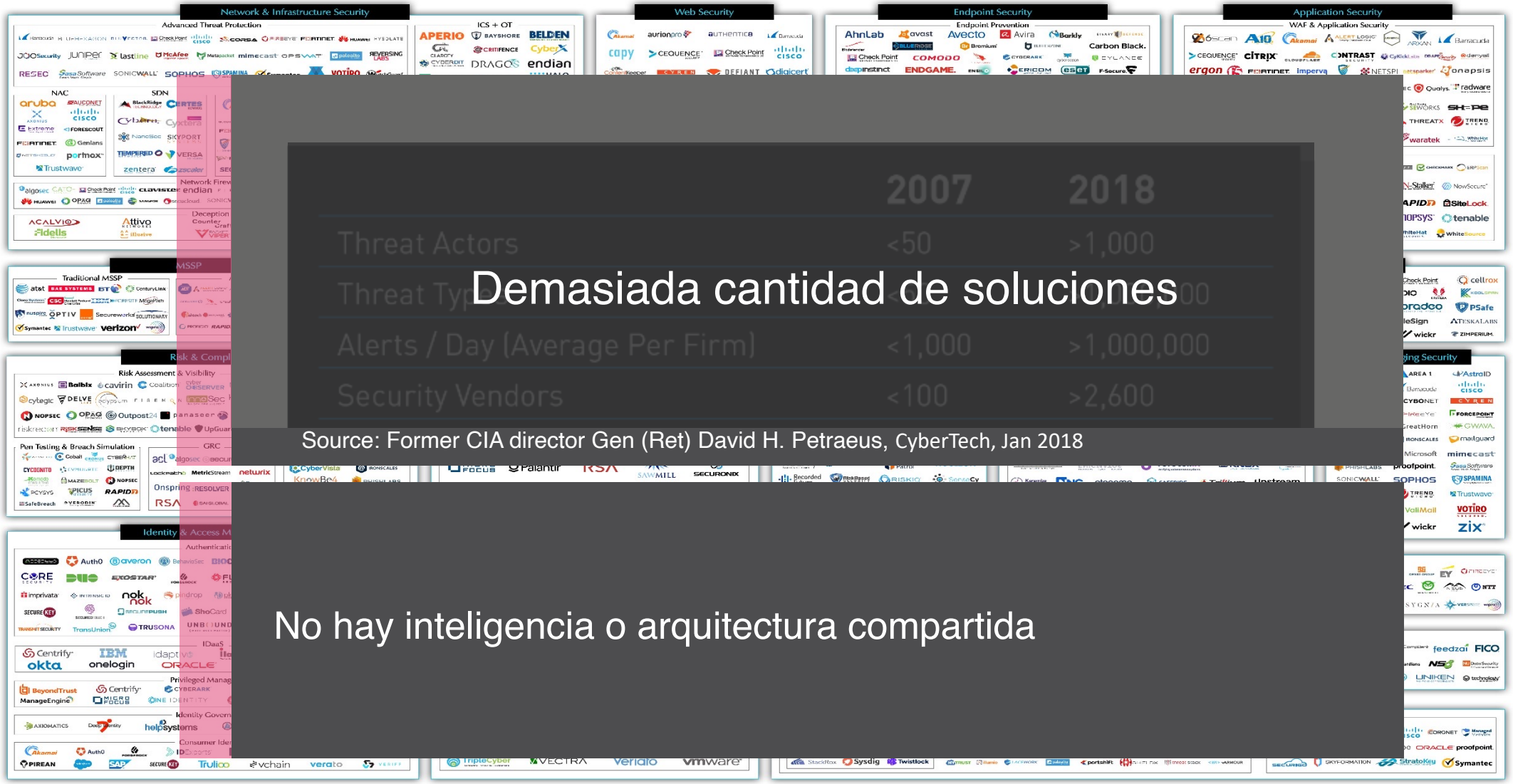


97%

de las empresas no están protegidas de los ataques de la **Generación V**

Source: Cyber Security Generations Survey among IT Professionals, March 2018, N=300 and Check Point Customer Generations Research, February-March 2018, N=443

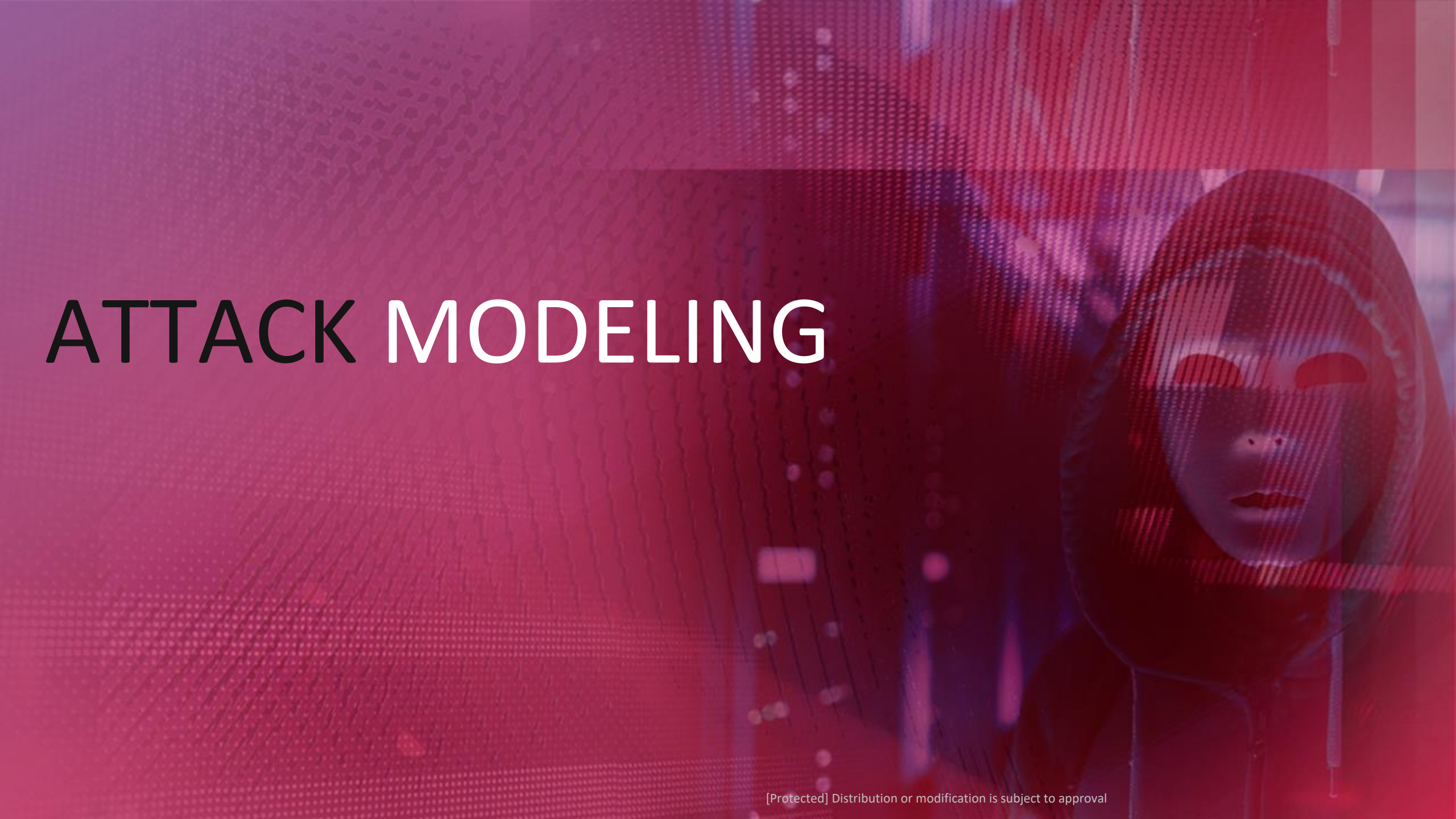
#3 – Demasiada complejidad



Source: Former CIA director Gen (Ret) David H. Petraeus, CyberTech, Jan 2018

Source: David DeWalt/General Petraeus

ATTACK MODELING



Que es el CYBER KILL CHAIN?

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Adaptación de un modelo militar
- Desarrollada por Lockheed Martin
- Pensar como un atacante
- Los ataques siguen una secuencia de fases

Cyber Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identificar el objetivo y las debilidades explotables.	Crear / seleccionar vector de ataque	Entregue el payload malicioso a la víctima	Obtenga privilegios de ejecución	Instale el malware en el host infectado	Establecer un canal de comunicación	Recolección de datos o corrupción, movimiento lateral y exfiltración

Planificación y ejecución de un ciberataque

Planificación del ataque

Semanas de antelación

- *Busque posibles víctimas*
- *Recopile datos sociales relevantes*
- *Construye, encuentra o compra tu arma preferida*
- *Kit de explotación (exploit kit), paquete de malware*
- *Adáptese a sus necesidades específicas*
- *Paquete listo para entrega*

Ingresando

En segundos

- *Detección de bypass*
- *Convence a la víctima para que abra su archivo creado*
- *Bypass del control de seguridad del sistema*
- *Instale su malware*

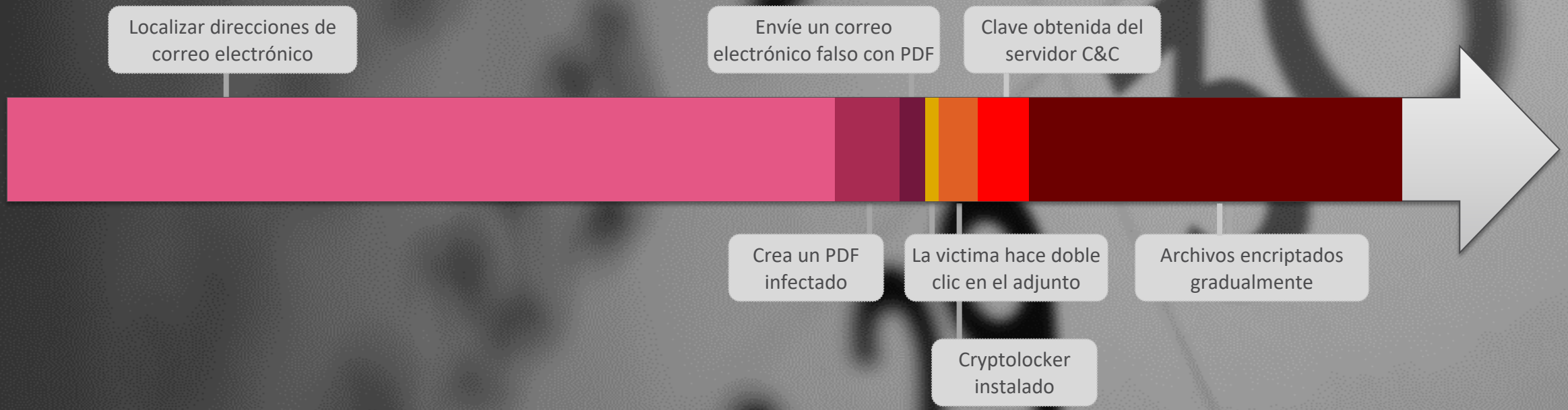
Ejecución del ataque

A partir de aquí...

- *Espere a que su malware "llame a casa"*
- *Indíquele qué hacer en la computadora de la víctima*
- *Monitorear continuamente su progreso*

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identificar el objetivo y las debilidades explotables.	Crear / seleccionar vector de ataque	Entregue el “payload” malicioso a la víctima	Obtenga privilegios de ejecución	Instale el malware en el host infectado	Establecer un canal de comunicación	Recolección de datos o corrupción, movimiento lateral y exfiltración

Ejemplo de una línea de tiempo
Ataque de ransomware a compañía australiana



Algunos pasos tardan horas o incluso semanas, mientras que otros tardan unos segundos.

Recon Weapon Delivery Exploit Install C&C Act On

Que es MITRE ATT&CK?

ATT&CK = Adversaries Tactics Techniques & Common Knowwldge
(Tácticas, Técnicas y Conocimiento Común de Adversarios)

- Base de conocimientos de las técnicas del adversario
- Basado en observaciones del mundo real
- Tácticas, técnicas y procedimientos
- Ya cuenta con 3 matrices: Enterprise, Mobile, ICS

Lanzamiento: 2017

Promocionada: 2018-2023

https://attack.mitre.org/matrices/enterprise/

Evolución: Cyber Kill Chain ➔ ATT&CK

2011: **Cyber Kill Chain**

LOCKHEED MARTIN THE CYBER KILL CHAIN®

2017: **MITRE ATT&CK**

MITRE ATT&CK™

Tácticas, técnicas y procedimientos en su lanzamiento

Los ataques se dividen en grupos de tácticas

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
Los vectores que usan los adversarios para ganar terreno	Técnicas que dan como resultado la ejecución de código controlado por adversarios en un sistema local o remoto.	Cualquier cambio de acceso, acción o configuración a un sistema que le dé a un adversario una presencia persistente en ese sistema.	Acciones que permiten a un adversario obtener un mayor nivel de permisos en un sistema o red	Técnicas que un adversario puede utilizar para evadir la detección o evitar otras defensas	Técnicas que dan como resultado acceso o control sobre el sistema, dominio o credenciales de servicio que se utilizan en un entorno empresarial.	Técnicas que permiten al adversario adquirir conocimientos sobre el sistema y la red interna	Técnicas que permiten a un adversario acceder y controlar sistemas remotos en una red.	Técnicas utilizadas para identificar y recopilar información, como archivos confidenciales, de una red objetivo antes de la exfiltración.	Técnicas y atributos que dan como resultado o ayudan al adversario a eliminar archivos e información de una red objetivo.	Cómo se comunican los adversarios con los sistemas bajo su control dentro de una red objetivo

THE MOST COMPLETE SECURITY

CloudGuard — SECURE THE CLOUD

CloudGuard Posture Management
Posture Management & Visibility

CloudGuard Intelligence
Network Traffic Analysis

CloudGuard Workload
Runtime Workload Protection

CloudGuard Network
Cloud Access Control & Prevention

CloudGuard AppSec
Web and API Protection

Multi & Hybrid Cloud

SD-WAN

Quantum — SECURE THE NETWORK

Quantum Security Gateway	Quantum Maestro	Quantum Lightspeed	Quantum R81 Secure OS
Enterprise Firewalls	Hyperscale	Hyper-Fast Firewall	
Quantum SMB	**Quantum Rugged**	**Quantum IoT Protect**	**Quantum Smart-1 Cloud**
SMB Suite	ICS Security	IoT Security	Security Management

- Access Control
- Advanced Threat Prevention
- Data Protection

- Wide Range of Firewalls
- Up to 3 Tbps Throughput
- 1, 10, 25, 40, 100 GbE ports
- Wi-Fi, DSL, 3G/4G/ LTE

- Unified Policy
- Autonomous Security
- Event Management
- Compliance

Horizon — UNIFIED MANAGEMENT & SECURITY OPERATIONS

Horizon MDR/MPR
Managed Prevention & Response

Horizon XDR/XPR
Extended Prevention & Response

Horizon Events
Unified Events

INFINITY PORTAL
Management & Unified Visibility

THREATCLOUD
Threat Intelligence

Harmony — SECURE USERS & ACCESS

SECURE ACCESS SERVICE EDGE (SASE)

Harmony Connect (SASE)

- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Branch FWaaS

EMAIL AND COLLABORATION

Harmony Email & Collaboration

- Account Takeover Protection
- Data Loss Prevention
- Threat Prevention
- Zero Phishing

ENDPOINT AND MOBILE

Harmony Endpoint

- Threat Prevention
- Anti-Ransomware Forensics
- Secure Media
- Access Control

Harmony Browse

- Zero Day Browser Protection
- Threat Prevention
- Zero Phishing

Harmony Mobile

- App Protection
- Network Protection
- Device Protection

ThreatCloud: The brain behind Check Point's power

AI TECHNOLOGY

BIG DATA THREAT INTELLIGENCE

MITRE ATT&CK: Casos de uso

Threat Intelligence

Detectar y Analizar

Emulación de adversario

Evaluación y respuesta

MITRE ATT&CK
integrado en el informe de Threat Emulation (AgentTesla)

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL	IMPACT
	Windows Management Instrumentation	Registry Run Keys Startup Folder	Bypass User Account Control	Process Hollowing	Credentials In Files	Security Software Discovery		Email Collection			
	Execution Through API	Change Default File Association	Process Injection	Bypass User Account Control	Credentials from Web Browsers	System Information Discovery		Data from Local System			
	Regsvcs Regasm	AppCert DLLs	AppCert DLLs	Software Packing	Credentials In Registry	Application Window Discovery					
		Windows Management Instrumentation Event Subscription		Process Injection							
				Disabling Security Tools							
				Regsvcs Regasm							

PREGUNTAS

Check Point
SOFTWARE TECHNOLOGIES LTD

GRACIAS!

Daniel González | Territory Account Manager.

joseg@checkpoint.com

Cel. 5554359696