

CIBERSEGURIDAD

APLICADA A PYMES Y AUTÓNOMOS



Nuevos vectores de ataques y evolución de métodos de protección

Raul Sanchez Rubio – System Engineer Fortinet

FORTINET



JUNTA DE EXTREMADURA





ZERODIUM Payouts for Desktops/Servers*

Up to \$1,000,000												1.001 Win RCE Zero Click Win
Up to \$500,000								3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win		
Up to \$250,000							5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux		
Up to \$200,000	6.001 VMware ESXi VME Win/Linux	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux			
Up to \$100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux			
Up to \$80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win			
Up to \$50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	8.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD			
Up to \$10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux			

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com



Los atacantes tienen una ventaja injusta



- ✓ Fácil acceso a conocimiento
- ✓ Pocas barreras para entrar
 - ✓ Enfocados a objetivos
- ✓ Pocas consecuencias en fallos

- ✗ Recursos limitados
- ✗ Muchos puntos a proteger
- ✗ Muchas responsabilidades
- ✗ Gran impacto ante fallos

TECH CULTURE SECURITY RANSOMWARE LOCKBIT

Fastest ransomware found to encrypt 53GB of data in just over four minutes

A sample from the LockBit ransomware family is really quick at locking up files

By [Humza Aamir](#) March 28, 2022, 7:37 AM | [9 comments](#)



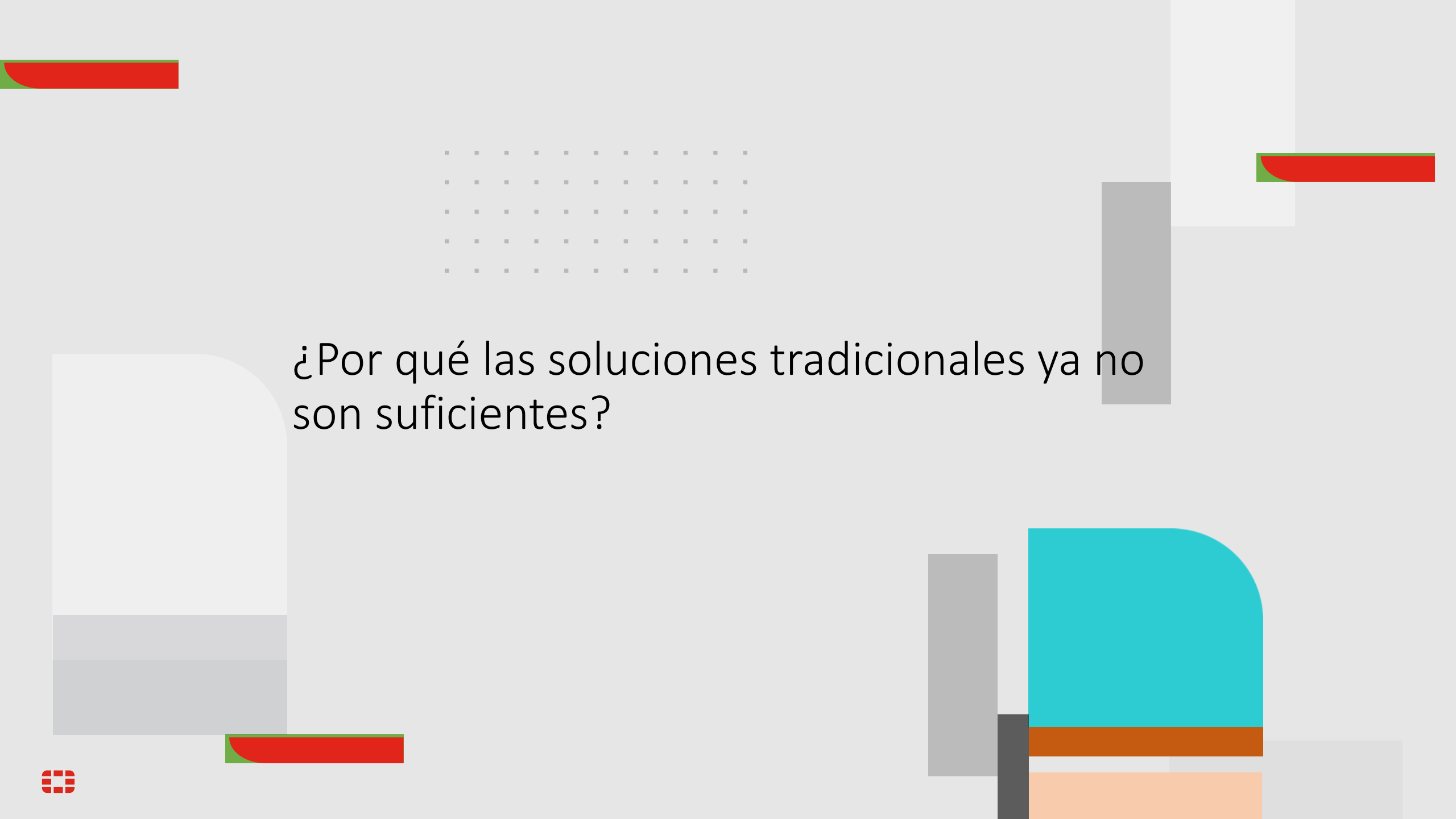
Why it matters: For IT admins and cybersecurity teams, a ransomware attack is a crucial race against time to detect and contain damage while salvaging what's left of a company's data assets. But how much reaction time is there when such an incident occurs? Not a lot it seems, as revealed by ransomware testing of ten candidates, where LockBit led the pack by encrypting nearly 100,000 files on a Windows Server machine in just over four minutes.



MOST READ



It took 37 years to find this Easter egg in Windows 1.0



¿Por qué las soluciones tradicionales ya no son suficientes?

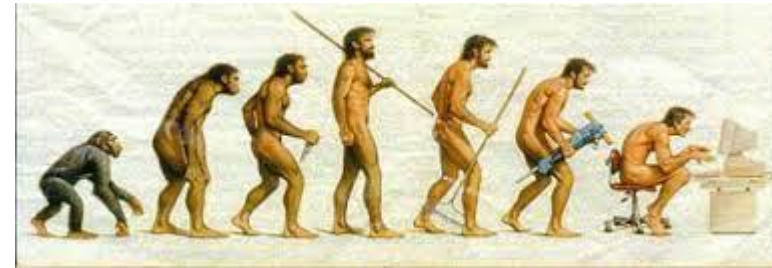


Evolución de las Tecnologías de Detección de Malware



Evolución de las soluciones de Antivirus

- **1987 Nace la industria del AV:** *“todo es bueno a menos que digamos que es malo”*
- **Años 90’s, empiezan a aparecer numerosos fabricantes de AV**
- **Principio de los 2000’s – Listas blancas:** *“Defino todo lo que es bueno, todo lo demás es malo”*
- **Primera década de los 2000’s – Antivirus perimetral:** *“Lo capturo en movimiento en la red”*
- **Principios de 2010 – Sandboxing:** *“Déjalo correr, vamos a ver qué hace”*
- **2014 – Principios del EDR:** *“Necesitamos toda la evidencia”*
- **En 2015 se incorpora la Inteligencia Artificial (IA)**
- **Actualmente tenemos soluciones de EDR de última generación:** recolección de evidencias, utilización de IA, automatización de la respuesta, etc.



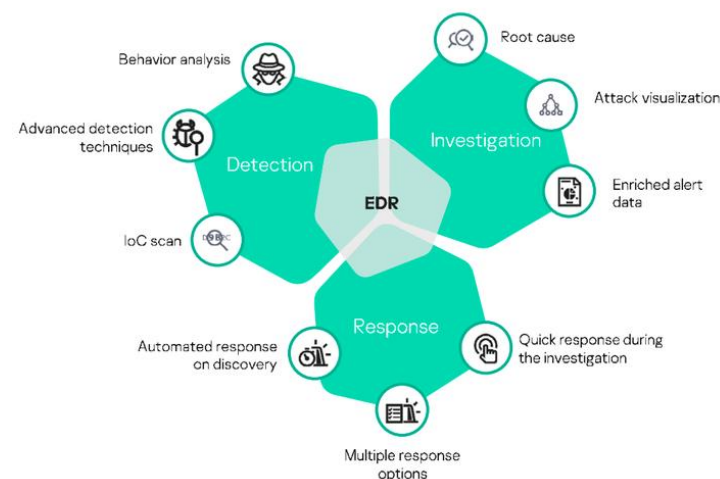
Razones por las que evolucionar un AV Tradicional

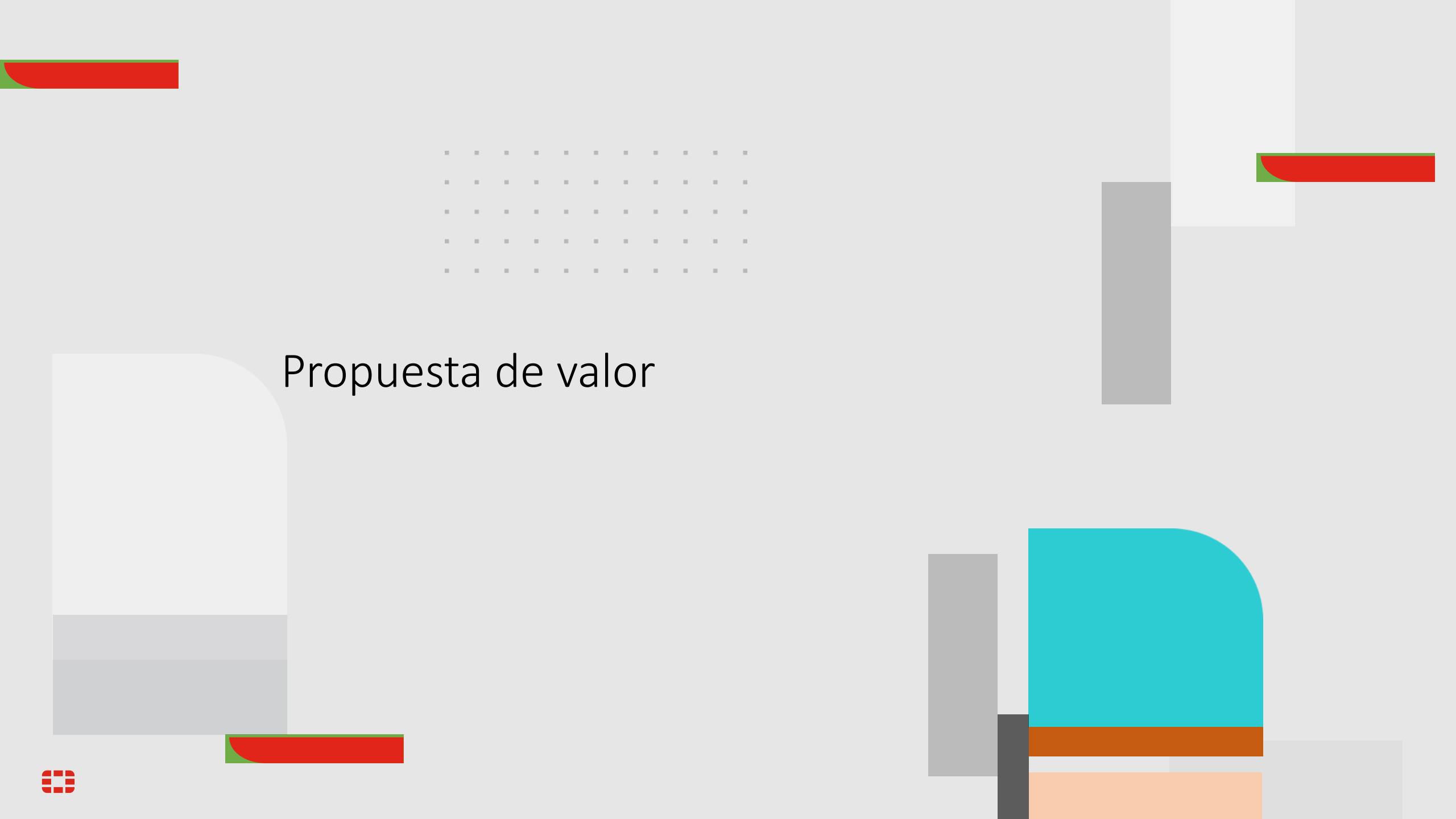
- **Ataques más sofisticados** (APT / Zero Day / Low & Slow)
- **Disminuye la productividad / Entornos Legacy**
- **Necesitan de soluciones adicionales en el endpoint** (FW, Sandboxing, etc.)
- **Constantes actualizaciones de los patrones de firma** (inteligencia adquirida)
- **Dificultad de proteger ante malware polimórfico** (>94% del malware)
- **Incapacidad de proteger ante ataques desconocidos** (Zero Day)
- **Archivos comprimidos** (no se analizan, zip de la muerte, etc.)
- **Ataques fileless** (Living off the Land)
- **El 95% de las filtraciones son causadas por errores humanos** (el eslabón más débil)
- **Transformación Digital**, ¿Dónde quedó el perímetro? (work from Everywhere)
- **Nuevos vectores de ataque**



¿Por qué ir hacia una solución EDR?

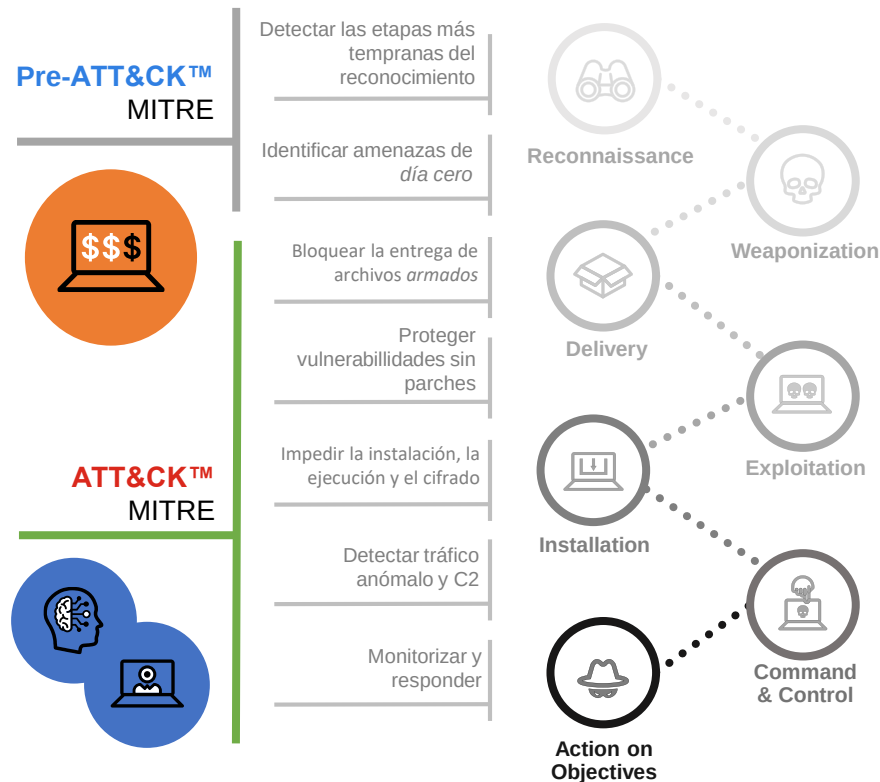
- **Mayor anticipación a los ataques dirigidos:** *se analizan patrones de comportamiento y es posible anticipar amenazas*
- **Detección Avanzada:** *detección tanto de amenazas conocidas como desconocidas gracias al análisis por comportamiento, IA, movimientos laterales, etc.*
- **Visión Global:** proporciona una visión global de la organización en todas sus plataformas o sistemas operativos desde un punto central (nube), incluso para entornos legacy
- **Analítica de Datos:** monitorización/telemetría continua del Endpoint (en línea y fuera de banda). Facilidad para la investigación. Visualización de la cadena de ataque, causa raíz
- **Enfoque Proactivo:** reducción del tiempo de Detección y Respuesta automatizada
- **Disminución de falsos positivos** (fatiga del analista)
- **Contención:** bloqueo a nivel de Endpoint evitando que se propague en la red interna





Propuesta de valor

Cuál es la vision de la seguridad de Fortinet



Ganamos o perdemos por TIEMPO

Para romper la secuencia de ataque, debemos poder **ajustar rápidamente la *postura* de seguridad** para defendernos de manera coherente contra ataques recién descubiertos en una superficie de ataque en constante expansión.

Detectar

Detección temprana para **minimizar impacto y coste**.

Proteger

Estrechar/**minimizar la ventana de oportunidad** del atacante.

Responder

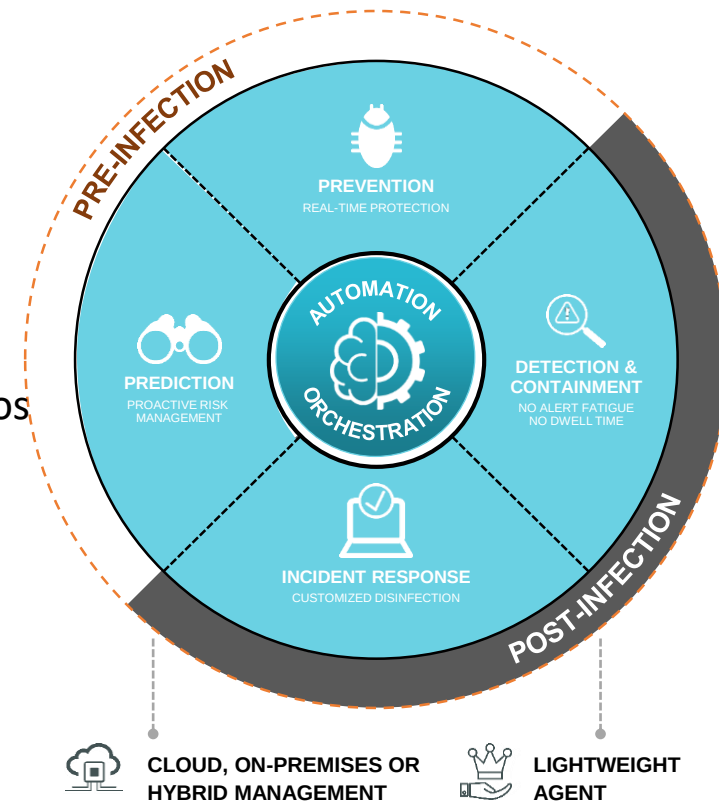
Moviéndonos **más rápido que el ataque** (inteligencia compartida y respuesta automatizada)

FortiEDR

Endpoint Protection, Detection & Response



- ✓ Agente Unificado “by design”. Uno de los más ligeros del mercado
- ✓ ML y Behavior-based protection
- ✓ Clasificación continua a través de nuestra AI alojada en la nube
- ✓ Soporte para entornos y SO legacy (XP, 2003, ...) y entornos híbridos (Airgap)
- ✓ Solución integrada y automatizada



AV Comparatives. Business Security Tests. March / June 2020 and Aug/Nov 2020