Zero Trust: relevancia e implicaciones en seguridad end point y gestión de identidad_

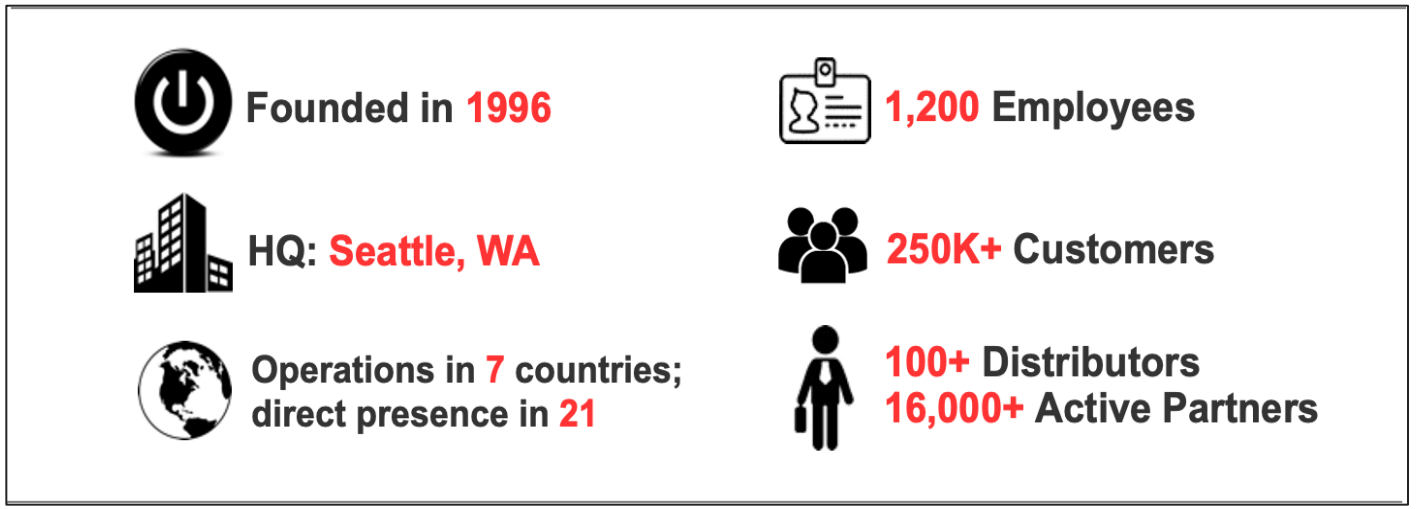
Miguel Carrero

VicePresidente, Proveedores de Servicios de Seguridad

y Cuentas Estratégicas


panda
WatchGuard
One Giant Leap for Integrated Security

Quien es WatchGuard y sus pilares estratégicos_



- Ciberseguridad efectiva (funcionalidad y simplicidad)
- Seguridad consumida como servicio
- Fabricantes participando de un ecosistema de colaboradores

WatchGuard | CYTOMIC

Que es Zero Trust_

~~"Trust but verify"~~

Enter zero trust

The term "zero trust" is widely abused in security product marketing. However, it is useful as a shorthand way of describing an approach where implicit trust is removed from all computing infrastructure. Instead, trust levels are explicitly and continuously calculated and adapted to allow just-in-time, just-enough access to enterprise resources.

"Zero trust is a way of thinking, not a specific technology or architecture," says Gartner Distinguished VP Analyst **Neil MacDonald.** "It's really about zero implicit trust, as that's what we want to get rid of."

WatchGuard | CYTOMIC

Modelo de protección Zero Trust para end point_

Modelo Zero-Trust: protección por capas

ENDPOINT LAYERS

Layer 1 / Signature files and heuristic technologies

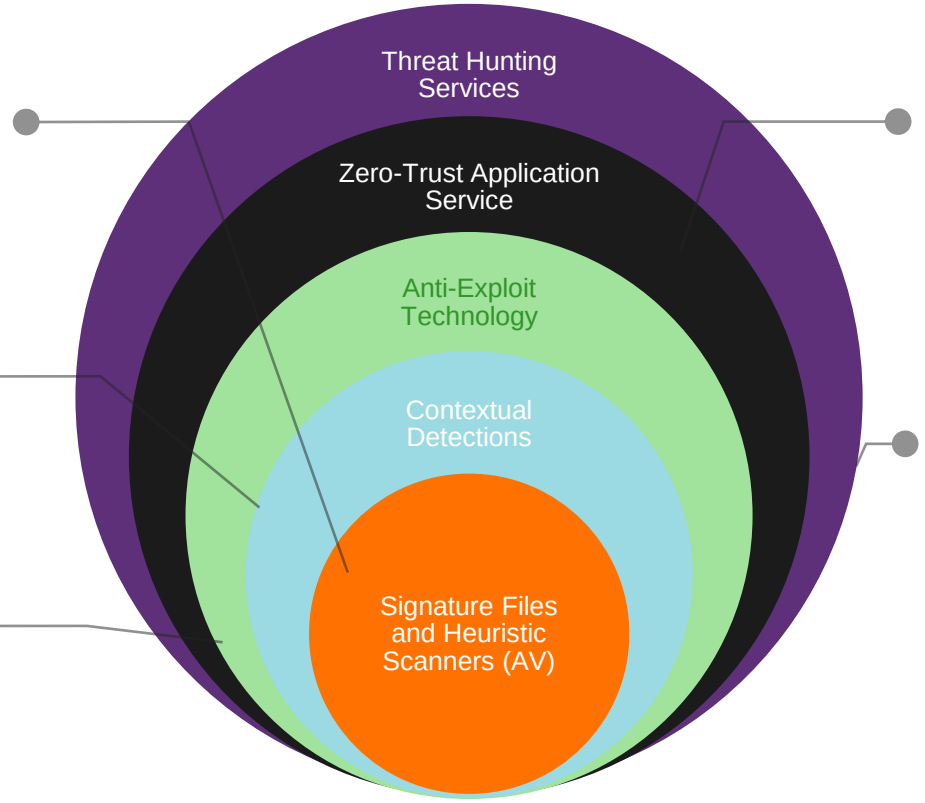
Tecnología eficaz y optimizada para detectar ataques conocidos

Layer 2 / Contextual detections

Permite detectar ataques sin malware y sin archivos

Layer 3 / Anti-exploit technology

Permite detectar ataques sin archivo diseñados para explotar vulnerabilidades



CLOUD-NATIVE LAYERS

Layer 4 / Zero-Trust App Service

Proporciona protección en caso de que se produzca una brecha en la capa anterior, detiene los ataques a equipos ya infectados y frena los ataques de movimiento lateral dentro de la red

Layer 5 / Threat Hunting services

Capacidad proactiva detectar ataques en fase inicial y actividades sospechosas

WatchGuard | CYTOMIC

Modelo de protección Zero Trust para end point_

- Complementa las capas anteriores
- Esencial para organizaciones ya infectadas y para detener ataques de movimiento lateral dentro de la red
- Muy importante también para proteger ordenadores/servidores con protección parcial o con otras soluciones con lagunas de detección de malware

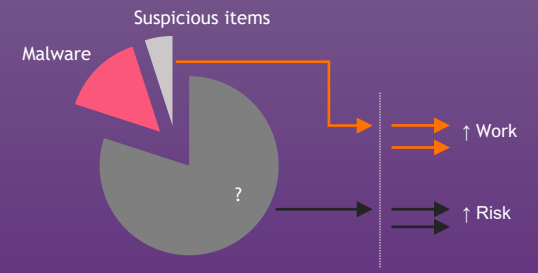
Clasifica el 100% de los procesos en ejecución

Sólo se permite la ejecución de elementos de confianza

AV tradicionales y otras soluciones EDR

Puede identificar el malware y algunos elementos sospechosos, pero nada más.

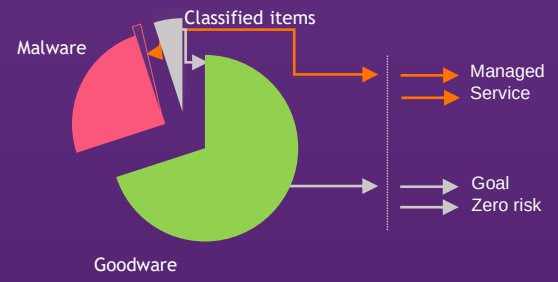
- Mayor tasa de éxito en los ataques de malware
- Brecha de detección



WatchGuard End Point security

Monitoriza todos los procesos en ejecución, permitiendo ejecutar sólo aquellos procesos clasificados como de confianza por Panda.

Servicio gestionado. Máxima protección sin delegar las decisiones en los clientes.



WatchGuard | CYTOMIC

Seguridad endpoint Zero Trust: Maximiza la protección, minimiza el esfuerzo_

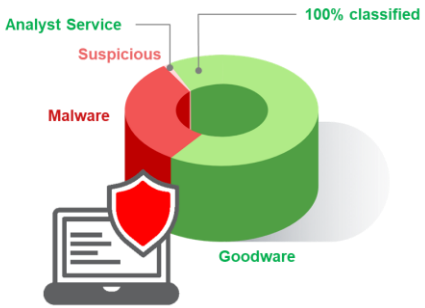
WatchGuard EPDR, combina la tecnología antivirus tradicional con el modelo de protección avanzada de detección y respuesta endpoint en una única solución para defenderse de las amenazas conocidas y desconocidas.

Tres niveles de seguridad endpoint:

- WatchGuard **EPP**
  (Endpoint Protection Platform)
- WatchGuard **EDR**
  (Endpoint Detection and Response)
- WatchGuard **EPDR**
  (Endpoint Protection Detection and Response)

Zero-Trust Application Service

- **100% of running processes** on your endpoints classified
- Only applications, process, or DLLs **classified as Goodware will execute**
- **Real-time activity monitoring and analysis of all programs**
- All behaviors are **verified by Panda analysts**
- **Higher level of protection with less effort**

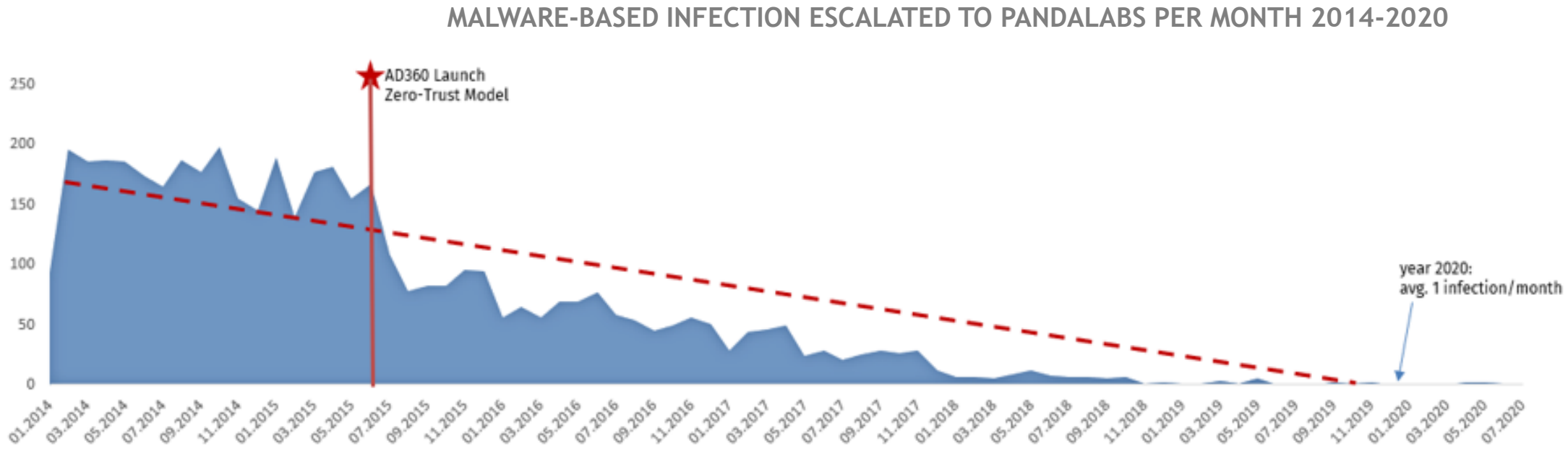


Threat Hunting Service

- **Leverage our team** of cybersecurity experts!
- **Reduce the MTTD and MTTR** (Mean Time To Detect and Mean Time To Respond)
- Create new rules that can be delivered to the endpoints to rapidly protect them against new attacks.
- Get recommendations on how to mitigate the attack and reduce the attack surface to avoid falling victim to future attacks.

WatchGuard | CYTOMIC

Eficacia de la aproximación Zero Trust: resultados_



"Analysts move from reactively responding to compromised customers to proactively notifying them about suspicious activity in their endpoints"

"The Zero-Trust Application service can drastically reduce the threat surface of endpoints."
Gartner Magic Quadrant for EPP, 2018.

WatchGuard | CYTOMIC

Zero Trust: La identidad es fundamental_

Los nuevos enfoques de seguridad, como zero trust, asumen que **cada dispositivo y usuario, dentro o fuera de la red, representa un riesgo para la seguridad.**

Al exigir una base sólida de identidad, estos enfoques hacen hincapié en:

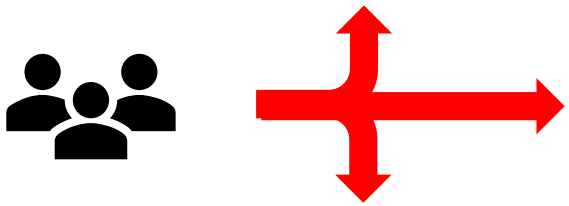
- Saber siempre quién y qué se conecta a la red y los servicios.
- Limitar el acceso a los sistemas y aplicaciones críticos para la empresa sólo a los dispositivos y perfiles que tienen permiso explícito para acceder a ellos.

Transformación de la red que traslada el núcleo a la nube

- Seguridad ofrecida como un servicio desde un núcleo gestionado
- Arquitectura centrada en la identidad
- Clave para la capacitación segura del trabajo desde casa
- Eficiencia y facilidad de gestión

SASE

(Secure Access Service Edge)



XDR

(Extended Detection and Response)

Telemetría & correlación en todo el portfolio

- Protección, detección y respuesta
- Consolidación de múltiples productos de seguridad en una plataforma
- Normalizar los datos de telemetría en la red, endpoint y cloud
- Mejora de la eficacia
- Mejora de la eficiencia
- Menor TCO

Zero Trust

Nunca confíes, siempre verifica

- Fuerte protección de la identidad de los usuarios y de los dispositivos
- Acceso simplificado con las principales plataformas IAM
- Mayor seguridad en las VPN
- Aislamiento de host
- Integraciones de terceros

WatchGuard | CYTOMIC

Zero Trust_ Conclusiones

1. Una aproximación al mundo de la ciberseguridad
2. Implicaciones fuertes en el mundo del endpoint
3. Gestion de Identidad es critica
4. Mejoras significativas en eficacia y eficiencia

WatchGuard | CYTOMIC

WatchGuard | CYTOMIC

Gracias_

¿Hablamos?

+34 900 840 407

sales@cytomic.ai