Pon fin a las ciber amenazas

Panda Adaptive Defense 360

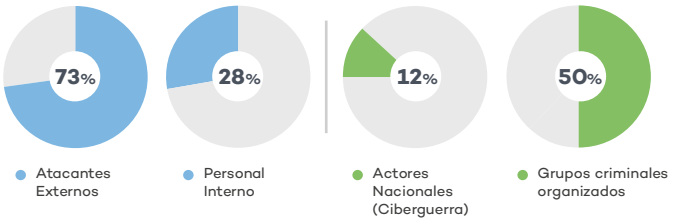
Seguridad Avanzada **automatizada y centralizada**

panda

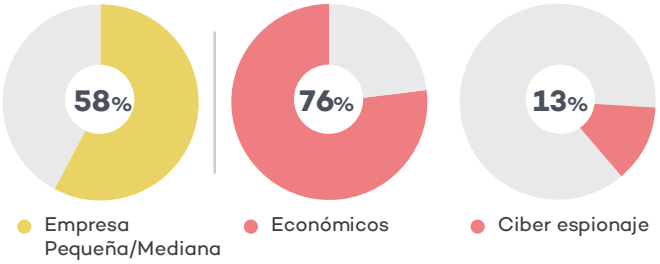
pandasecurity.com

CIBERSEGURIDAD EN LAS EMPRESAS

¿Quién está detrás de las ciber amenazas?[1]



¿Quiénes son sus víctimas y motivos?[1]



El Endpoint es el nuevo perímetro

La movilidad, el procesamiento y el almacenamiento en la nube han revolucionado el entorno empresarial. **Los puestos de trabajo, son el nuevo perímetro.** Las soluciones de seguridad en el endpoint deben ser **avanzadas, adaptativas y automáticas**, con los más altos niveles de prevención y detección al atacante, que antes o después evadirá las medidas preventivas. Deben además, ofrecer herramientas ágiles para una rápida respuesta que minimice el daño y reduzca la superficie de ataque.

La profesionalización de los hackers

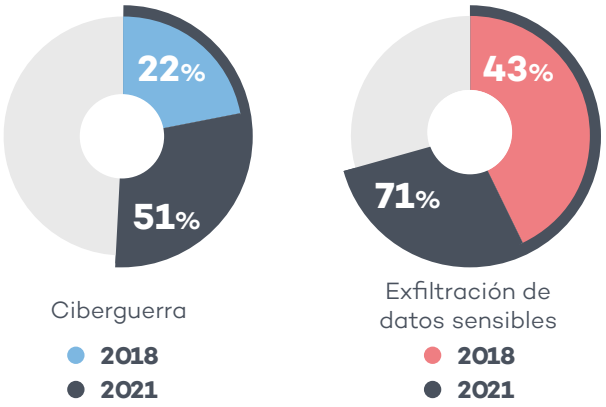
Los **adversarios** son cada vez más **numerosos** y **sofisticados**, resultado de su profesionalización, la democratización de las tecnologías y las filtraciones continúas de ciber inteligencia.

Las **ciber amenazas** de última generación están **diseñadas para evadir** las soluciones de **seguridad tradicionales**.

¿Cuál es el coste para las empresas?

- **Coste global:** $600.000 M[2]
- **Cada brecha de seguridad cuesta** $3.86 M[3]

Empresas y percepción de alto riesgo[4].



Para el 60% de ellas, los ataques Nacionales a gobiernos y empresas desembocarán en **ciberguerra**.

La ciberdefensa en las organizaciones

Mientras los hackers dirigen sus acciones a los equipos y servidores, donde residen los activos más valiosos de las organizaciones y sus **equipos de seguridad tienen grandes dificultades para defenderlas**, las soluciones **EDR** (Endpoint Detection and Response) lejos de ser la solución, **incrementan su carga** de trabajo debido a la ausencia de automatización en la prevención, detección, contención y respuesta.

Mejorar la postura de seguridad de tu organización, **sin incrementar los costes** operativos ilimitadamente, requiere inevitablemente la **automatización de la prevención, detección y respuesta** en los endpoints.

SOLUCIONES ENDPOINT DETECTION AND RESPONSE (EDR)

Las soluciones EDR monitorizan, registran y almacenan la actividad de los endpoints, como por ejemplo eventos del usuario, de los procesos, cambios en el registro, memoria y uso de red. Esta visibilidad, permite descubrir las amenazas que de otra manera pasarían desapercibidas.

¿Qué dificultades se esconden tras las soluciones EDR?

Se utilizan múltiples técnicas y herramientas para buscar en los eventos anomalías de seguridad y validar o descartar las alertas. Todo esto requiere de la intervención humana.

Las soluciones EDR requieren supervisión 24/7, y rapidez en la respuesta de personal altamente calificado.

Sin embargo, estos recursos son costosos y difícil de encontrar. Las organizaciones que se enfrentan a presupuestos escasos y personal reducido no están preparadas para aprovechar y maximizar los beneficios de las soluciones EDR por sí mismas. Sus equipos experimentan más carga de trabajo derivadas de la implantación y operación de estas soluciones en lugar de ser una ayuda para dedicarse a lo que importa: Mejorar la postura de seguridad de sus organizaciones.

1 "2018 Data Breach Investigation report". Verizon
2 "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
3 "2018 Study on Global Megatrends in Cybersecurity". Ponemon Institute
4 "2018 Cost of a Data Breach Study: Global Overview". Ponemon Institute/IBM Security

Panda Adaptive Defense 360

Panda Adaptive Defense 360 es una solución innovadora de ciberseguridad para estaciones, portátiles y servidores, entregada desde la nube, que **automatiza la prevención, detección, contención y respuesta** contra cualquier amenaza avanzada, malware de día cero, ransomware, phishing, exploits en memoria y ataques sin malware, presente y futuro, dentro y fuera de la red corporativa.

Se diferencia del resto de soluciones en que combina el más amplio conjunto de tecnologías de **protección (EPP)** con capacidades de **EDR automatizadas**, gracias a dos **servicios gestionados por expertos en Panda Security**, entregados como características de la solución:

- **Servicio de clasificación del 100% de las Aplicaciones.**
- **Servicio de Threat Hunting e Investigación.**

Gracias a su arquitectura en la nube, su **agente es ligero** y no impacta en el rendimiento de los endpoints, que se gestionan través de **una única consola cloud**, incluso si están aislados del exterior.

Panda Adaptive Defense 360 integra las **Plataformas Cloud de Protección y de Gestión** (*Aether*), que maximizan la prevención, detección y respuesta automatizada, minimizando el esfuerzo.

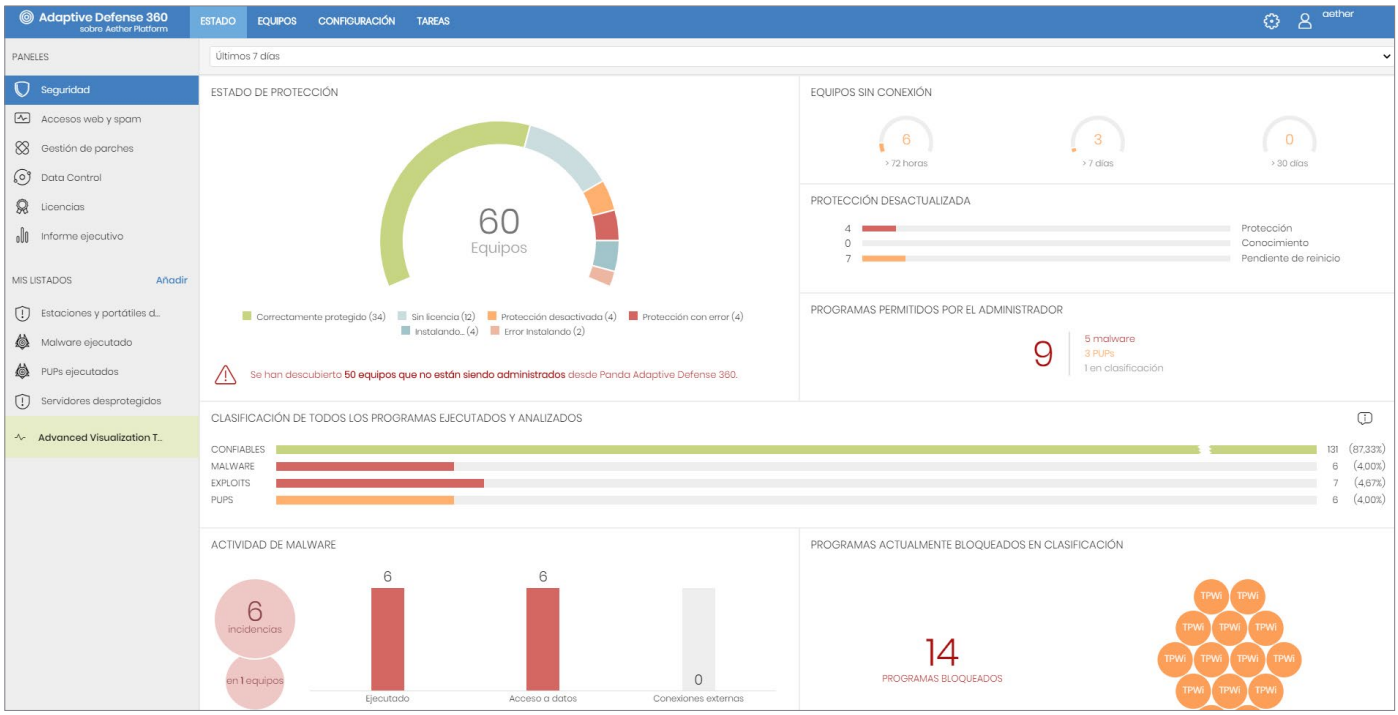


Figura 1: Un único panel ofrece una visión global y una gestión consolidada y priorizada de las amenazas encontradas

BENEFICIOS

Panda Adaptive Defense 360

Simplifica y minimiza los costes de la Seguridad Avanzada y Adaptativa

- Sus servicios gestionados reducen los costes de personal experto. No hay falsas alertas que gestionar, no se delega la responsabilidad.
- Los servicios gestionados autoaprenden de las amenazas. No dediques tiempo a ajustes manuales.
- Prevención máxima en el endpoint. Reduce el coste operativo a valores muy cercanos a cero.
- No hay infraestructura de gestión que instalar, configurar o mantener.
- El rendimiento de los endpoints no se ve impactado al estar basado en un agente ligero y en una arquitectura totalmente en la nube.

Automatiza y reduce el tiempo de detección y exposición (Dwell Time)

- Deniega la ejecución de amenazas, malware de día cero, ransomware y phishing.
- Detecta y bloquea la actividad maliciosa en memoria (Exploits) antes de que cause daños.
- Detecta procesos maliciosos que superaron las medidas preventivas.
- Detecta y bloquea técnicas, tácticas y procedimientos de hacking.

Automatiza y reduce el tiempo de respuesta e investigación

- Remediación automática y transparente.
- Recuperación de la actividad en los endpoints y vuelta inmediata a la operativa habitual.
- Visibilidad accionable del atacante y su actividad, acelerando la investigación forense.
- Facilita la reducción de la superficie de ataque. Ayuda a la mejora de la postura y madurez en seguridad.

PLATAFORMA DE PROTECCIÓN *ADAPTIVE* CLOUD

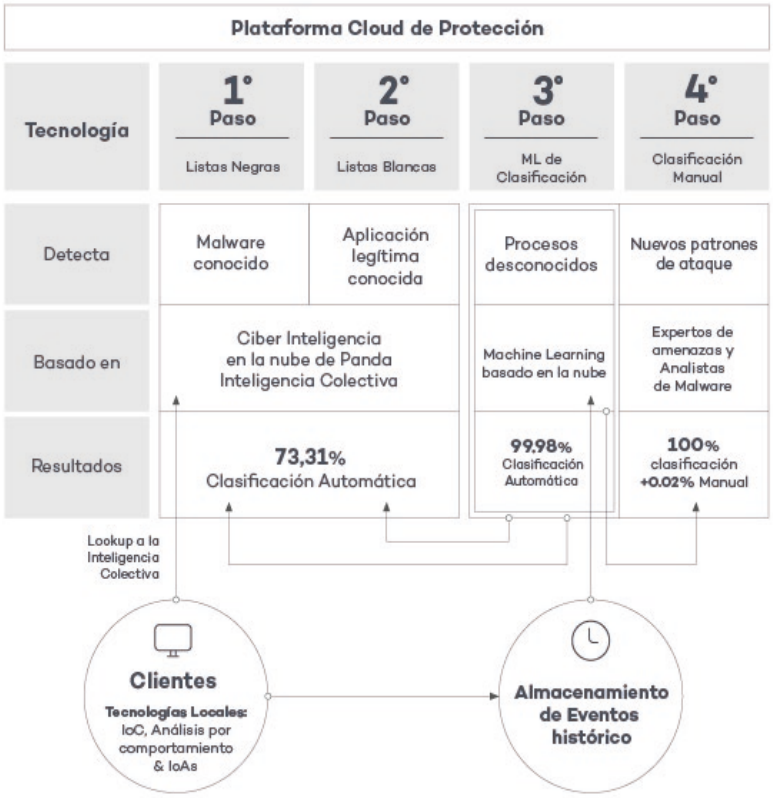
Humanos y Máquinas liderando la Seguridad Avanzada y Adaptativa.

100% ATTESTATION SERVICE

El servicio gestionado de clasificación del 100% de las aplicaciones monitoriza la actividad en el endpoint y deniega la ejecución de aplicaciones y procesos maliciosos. Por cada ejecución, emite en tiempo real un **veredicto de su clasificación, malicioso o legítimo, sin incertidumbre**, sin delegar en el cliente. Todo esto es posible solo por la capacidad, velocidad, adaptación y escalabilidad de la IA y el procesamiento en la nube.
El servicio unifica tecnologías de **Big Data** y técnicas de **Machine Learning** multinivel, incluido **Deep Learning**, resultado de la supervisión continua y automatización de **la experiencia, inteligencia y conocimiento acumulado del equipo** de seguridad y amenazas del Centro de Inteligencia de Panda Security.

El servicio de 100% Attestation Service libera, como ninguna otra solución en el mercado, a las empresa del riesgo que conlleva la ejecución de software malicioso en la organización.

Figura 2: Secuencia del servicio gestionado de clasificación en la nube



* TTPs: tácticas, técnicas y procedimientos utilizados por los atacantes

SERVICIO GESTIONADO DE THREAT HUNTING & INVESTIGATION

Siempre habrá hackers que sean capaces de pasar por alto los sistemas de seguridad. **El Threat Hunting** es el proceso para descubrir nuevas amenazas avanzadas y sus TTP*, más allá de lo que pueden hacer los actuales sistemas de detección, antes de que causen serios daños a la organización.

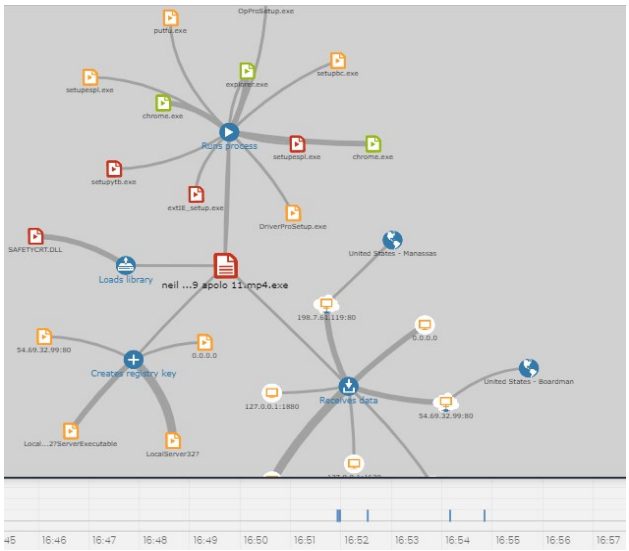
Los hunters trabajan bajo la premisa de que las empresas viven en un **estado de compromiso continuo**.

Entro otros, sus **beneficios** son:

- Crear nuevas detecciones de amenazas.
- Mejorar la respuesta al incidente.
- Reducir la superficie de ataque.

El servicio **Gestionado de Threat Hunting & Investogation** de Panda Security está operado por un equipo de Threat Hunters, expertos en ciberseguridad, altamente cualificado que, dotados de herramientas de profiling, análisis y correlación de eventos en tiempo real y retrospectivo, descubren proactivamente nuevas técnicas y tácticas de evasión y hacking.

Figura 3: Desde la consola de gestión de Panda Adaptive Defense 360, el timeline del incidente permite su investigación forense: fecha en la que se vio por primera vez en la red, el número y nombre de los endpoints afectados, cambios de configuración y con quién se comunicó



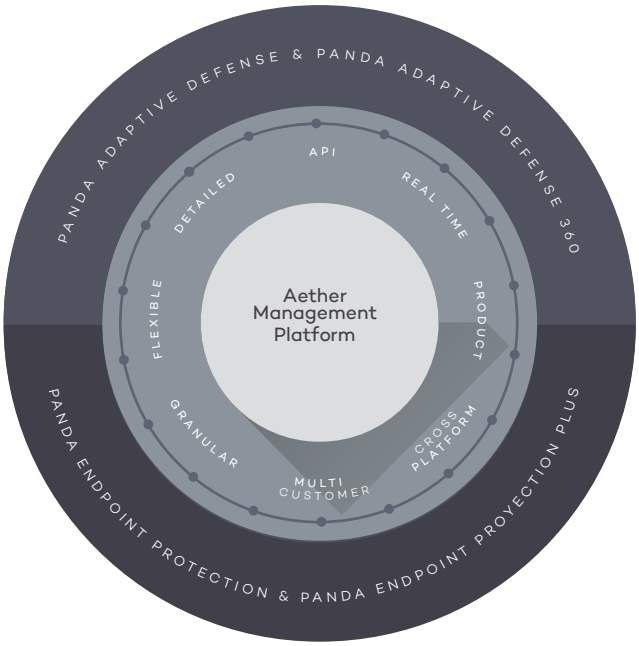
PLATAFORMA CLOUD DE GESTIÓN: *AETHER*

Seguridad, visibilidad y control de última generación. Valor inmediato, escalable e integral desde la nube.

La plataforma cloud Aether y su consola de gestión, común para todas las soluciones endpoint de Panda Security, optimiza la gestión de la seguridad avanzada y adaptativa, dentro y fuera de la red.

Diseñada para que los equipos se focalicen solo en el gobierno de la postura de ciberseguridad de su organización, minimizando la complejidad y maximizando la flexibilidad, granularidad y escalabilidad.

Figura 3: Plataforma cloud de gestión unificada: Aether



BENEFICIOS DE AETHER

Panda Adaptive Defense 360

Genera más valor en menos tiempo. Fácil implementación, visibilidad inmediata

- Despliegue, instalación y configuración en minutos. Comienza a ver el valor desde el primer día.
- Agente ligero multiproducto y multimódulo Panda. Multisistemas (Windows, MAC, Linux, Android).
- Descubrimiento automático de endpoints no protegidos. Instalación remota.
- Tecnología propia Proxy, incluso en equipos sin conexión al exterior.
- Optimización del tráfico, con tecnología propia Repositorio/caché.

Simplifica la operativa, adaptándose a tu organización

- Consola web intuitiva. Gestión flexible y modular.
- Roles predefinidos o personalizados.
- Auditoría detallada de acciones en consola.
- Usuarios con capacidad y visibilidad total o restringida.
- Políticas de seguridad por grupos y endpoint.
- Inventariado hardware, software y changelog.

Facilita la supervisión. Acelera la respuesta

- Paneles de control e Indicadores clave priorizados.
- Alertas confirmadas y priorizadas en tu flujo de trabajo.
- Historial completo y accionable del incidente, procesos involucrados, origen, dwell, prevalencia, etc.
- Actúa en los endpoints con un solo clic: Reiniciar, aislar, parchear y analizar, acelerando la respuesta.

SEGURIDAD AVANZADA Y AUTOMATIZADA EN EL ENDPOINT

Panda Adaptive Defense 360 integra en una única solución, tecnologías preventivas tradicionales con tecnologías innovadoras de prevención, detección y respuesta automatizadas contra las ciber amenazas avanzadas presentes y futuras:

Tecnologías Preventivas Tradicionales

- Firewall personal o gestionado. IDS.
- Control de dispositivos.
- Antimalware permanente multivector y bajo demanda.
- Blacklisting/Whitelisting gestionado. Inteligencia Colectiva.
- Heurística pre-ejecución.
- Filtrado en navegación web.
- Antispam & Antiphishing.
- Anti-tampering.
- Filtrado de contenidos en correo.
- Remediación y rollback.

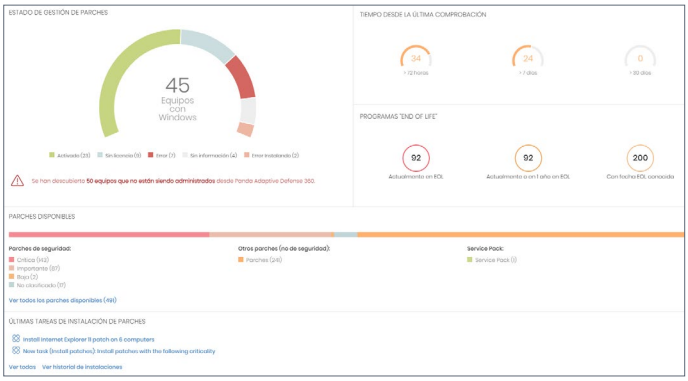
Tecnologías de Seguridad Avanzada

- EDR: monitorización continúa de actividad en el endpoint.
- Denegación de la ejecución de procesos desconocidos.
- Machine Learning de comportamiento en la nube que clasifica el 100% de los procesos (APTs, ransomware, Rootkits, etc.).
- Sandboxing en la nube en entornos reales.
- Análisis por comportamiento y detección de IoAs (scripts, macros, etc.).
- Detección y respuesta automática de exploits en memoria.
- Threat Hunting gestionado de ataques malwareless.

MÓDULOS ADICIONALES

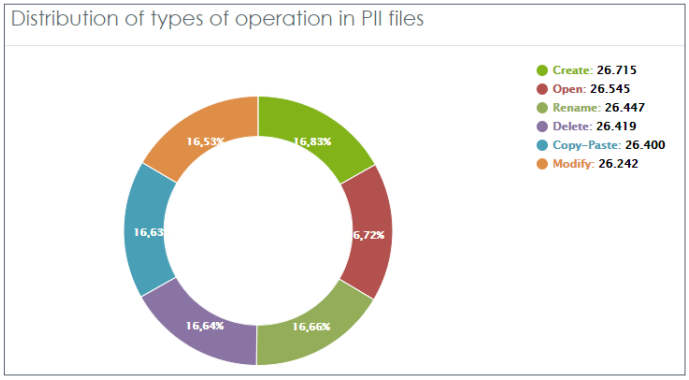
Panda Patch Management

Panda Patch Management es una solución intuitiva de gestión de las vulnerabilidades de los sistemas operativos y aplicaciones de terceros, en estaciones y servidores Windows. El resultado es una reducción de la superficie de ataque, fortaleciendo las capacidades preventivas, y de contención ante incidentes de seguridad



Panda Data Control

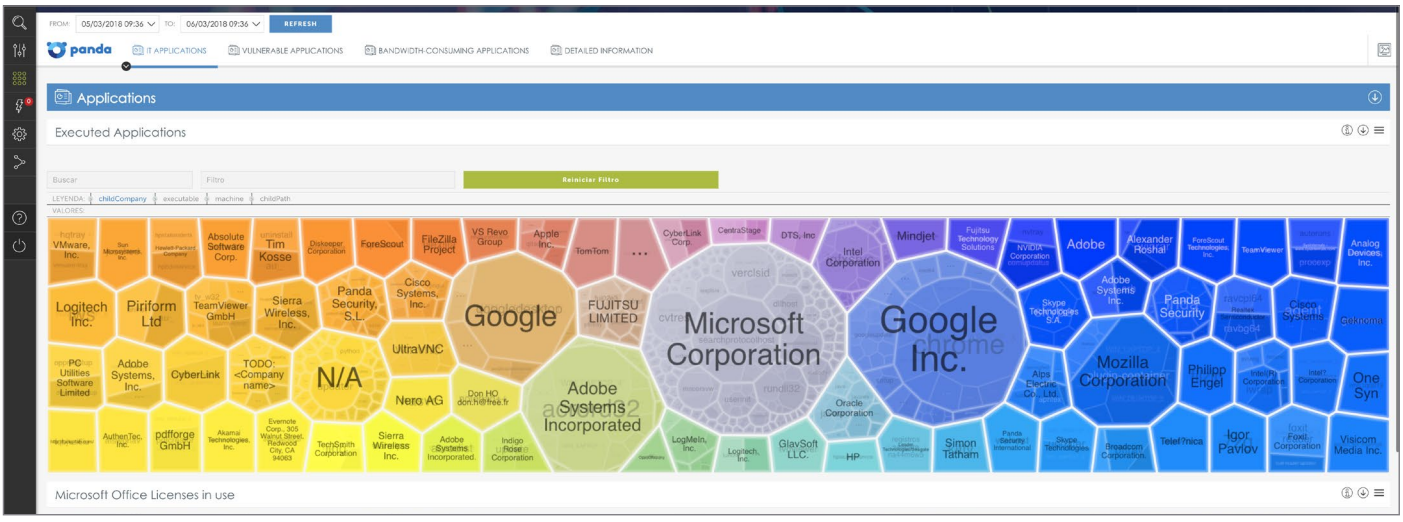
Panda Data Control Descubre, audita y monitoriza los datos de carácter personal y sensible desestructurados en los endpoints: desde el dato en reposo (data at rest), hasta las operaciones sobre ellos (data in use) y su tránsito (data in motion).



Panda Advanced Reporting Tool

La plataforma de **Panda Advanced Reporting** retiene y automatiza la correlación de la información generada por la ejecución de procesos y aplicaciones en los endpoints protegidos con su contexto, que Panda Adaptive Defense 360 recoge y los enriquece en la Plataforma Cloud de Protección.

Panda Advanced Reporting Tool genera automáticamente inteligencia de la actividad en la organización y permite buscar, correlacionar y configurar alertas sobre los eventos.



El módulo **SIEMFeeder** envía a la organización, en tiempo real, los eventos recogidos del endpoint y enriquecidos en la Plataforma Cloud de Protección con Inteligencia de seguridad, para su integración en el SIEM corporativo.

Conoce más en www.pandasecurity.com/business/solutions

CERTIFICACIONES Y RECONOCIMIENTOS

Panda Security participa regularmente y obtiene premios en protección y rendimiento de Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs

Panda Adaptive Defense logró la certificación EAL2 + en su evaluación para el estándar Common Criteria

Panda Security reconocido como visionario en el Cuadrante Mágico de Gartner de Endpoint Protection Platforms (EPP) 2018.

AV-Comparatives test Adaptive Defense 360 "Esta solución clasifica todos los procesos ejecutados, registra cualquier tipo de malware"

"La anticipación es nuestra mejor aliada a la hora de definir nuestras necesidades futuras y prevenir los riesgos. Adaptive Defense 360 nos da la visibilidad necesaria para lograr esa anticipación"

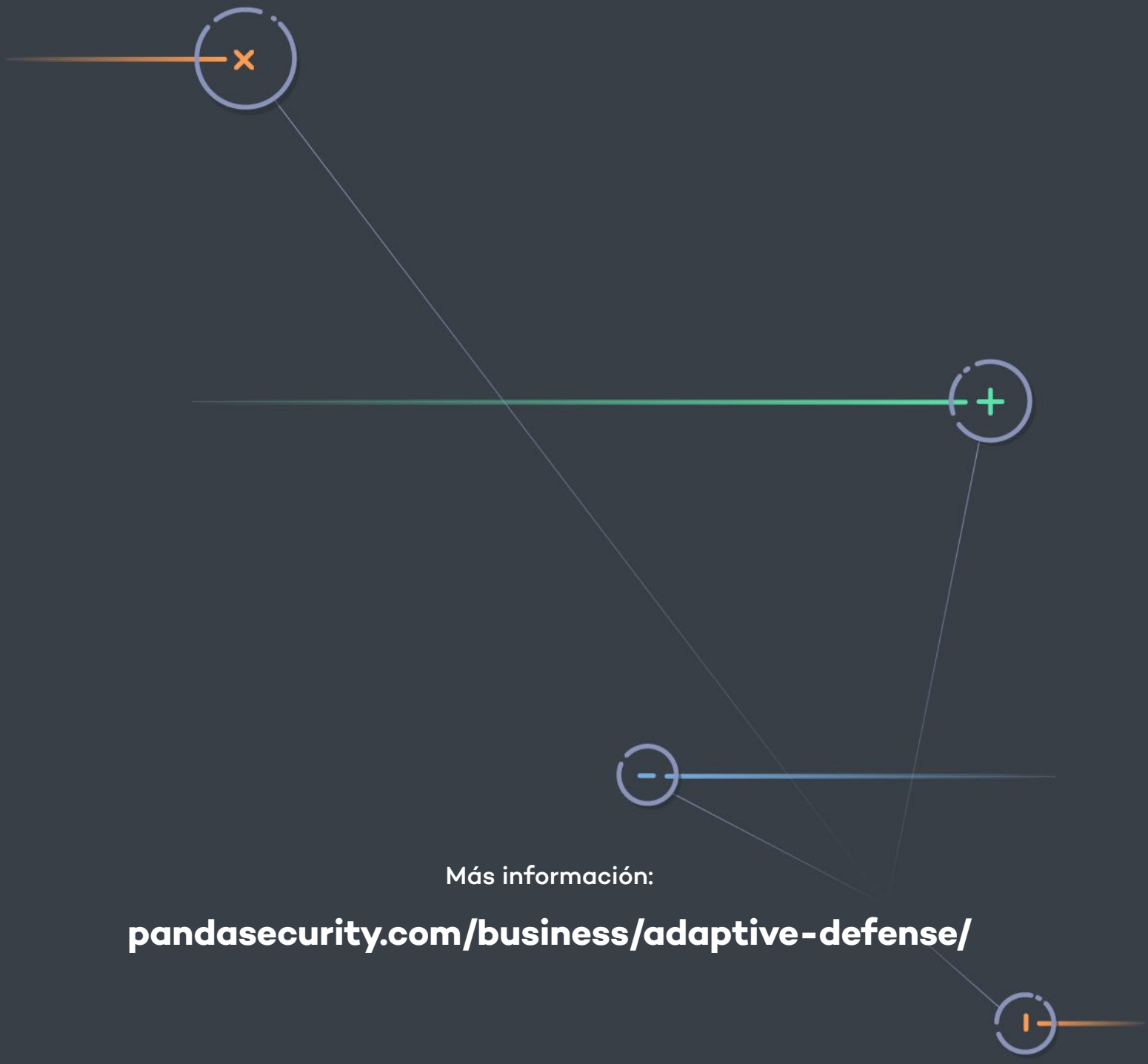
Jean-Yves Andreoletti
Integración de sistemas y redes, Ingeniero de plataformas de validación y mantenimiento.

Plataformas Soportadas y Requisitos del Sistema de nuestras Soluciones de Seguridad Endpoint

Las plataformas soportadas están en continua evolución para dar la máxima cobertura posible a los nuevos Sistemas Operativos. Por este motivo, recomendamos acceder a las ayudas online en los siguientes links:

Estaciones y Servidores Windows: http://go.pandasecurity.com/endpoint-windows/requisitos
Dispositivos macOS: http://go.pandasecurity.com/endpoint-macos/requisitos
Estaciones y Servidores Linux: http://go.pandasecurity.com/endpoint-linux/requisitos
Móviles y Dispositivos Android: http://go.pandasecurity.com/endpoint-android/requisitos

Panda Patch Management: http://go.pandasecurity.com/patch-management/requisitos
Panda Data Control: http://go.pandasecurity.com/data-control/requisitos
Panda Cloud Systems Management: http://go.pandasecurity.com/systems-management/requisitos
SIEM Feeder: http://go.pandasecurity.com/siem-feeder/requisitos
Advanced Reporting Tool: http://go.pandasecurity.com/reporting-tool/requisitos



Más información:

pandasecurity.com/business/adaptive-defense/