Acronis

Acronis Adv. Security y EDR

Alejandro López

Ingeniero de Soluciones
para Latinoamérica
alejandro.lopez@acronis.com

#CyberFit

¿Qué es EDR?

EDR (Endpoint Detection and Response) es una plataforma de seguridad que correlaciona los eventos para identificar **amenazas avanzadas o ataques en curso** y tomar las medidas necesarias.

Principales funciones de EDR según Gartner:

- Detectar los incidentes de seguridad
- Contener los incidentes en el endpoint
- Investigar los incidentes de seguridad
- Proporcionar una guía para la corrección

La necesidad de tener EDR

Contra los ataques avanzados solo vale una seguridad avanzada

Más del 60 % de las violaciones de seguridad **incluyen alguna modalidad de hackeo**.

De media, las organizaciones tardan **207 días** en identificar una violación de seguridad.

Los ataques son inevitables y hay que estar preparado

Se tardan **70 días** en contener una violación de la seguridad.

El coste total de una fuga de datos es de **4,35 millones de dólares** de media.

El **76 % de los equipos de seguridad** y TI tienen que afrontar **la falta de una visión en común** de las aplicaciones y los recursos.

Para muchos, cumplir las normativas es imprescindible

Las normativas exigen a las empresas **comunicar los incidentes de seguridad** en un plazo concreto: por ejemplo, 72 horas, en el caso del RGPD.

El **70% de las fugas de datos incluyen información de identificación personal** (se requiere un análisis tras el incidente para la comunicación según las normativas).

Fuentes: "Data Breach Investigations Report", Verizon, 2022; "Cost of data breach report", 2022, IBM Security y Ponemon Institute; "Costs and Consequences of Gaps in Vulnerability Response", ServiceNow, 2020, "Investigation or Exasperation? The State of Security Operations", IDC

Cómo ayuda EDR a proteger contra más amenazas

*Tenga en cuenta que los ataques de mayor complejidad suelen generar costes más elevados

Paso siguiente – Antimalware vs. EDR

Categoría	Antimalware	EDR
Objetivo	Bloquear/prevenir ataques	Detección y respuesta posincidente
Tecnología de detección	Detecta y detiene archivos, procesos o comportamientos **"malos conocidos".**	Detecta la **"intención"** mediante la correlación de una serie de acciones que realiza un atacante para lograr su objetivo.
Visibilidad de los ataques	Baja. Solo muestra las amenazas detectadas y bloqueadas.	Alta. mayor alcance de los incidentes y correlación de las etapas del ataque para mostrar: • ¿Cómo consiguió acceder? • ¿Cómo ocultó su rastro? • ¿Qué ha dañado? • ¿Cómo se propagó?
Funciones de respuesta	Bloquea automáticamente los procesos **"malos conocidos"** y pone en cuarentena las amenazas.	Ofrece una gran variedad de funciones de respuestas, concretamente: • Contener los incidentes en el endpoint • Investigar los incidentes de seguridad • Proporcionar corrección

Lanzar un servicio de EDR suponía un reto, hasta ahora

Las soluciones EDR existentes presentan un alto nivel de complejidad, costos importantes y un largo plazo de rentabilización. Sin embargo, con Acronis, empresas de todos los tamaños pueden contar con un partner que ofrece un uso eficaz y eficiente de EDR.

Retos	 **Coste y complejidad**	 **Continuidad empresarial limitada y fragmentación de soluciones**	 **Conflicto con el canal y capacitación**	 **Necesidad de mejora de análisis de incidentes y del tiempo respuesta**	 **Insuficiente concienciación sobre cumplimiento de normativas**
Oportunidad con Acronis	**Innovación que extiende la EDR a sectores populares del mercado**	**Protección en el marco del NIST: desde la identificación hasta la recuperación**	**Verdaderamente centrados en los partners proveedores de servicios y clientes**	**Análisis y respuesta rápidos**	**Cumplimiento de normativas con la facilidad que necesita**

Acronis
Cyber Protect Cloud

#CyberFit

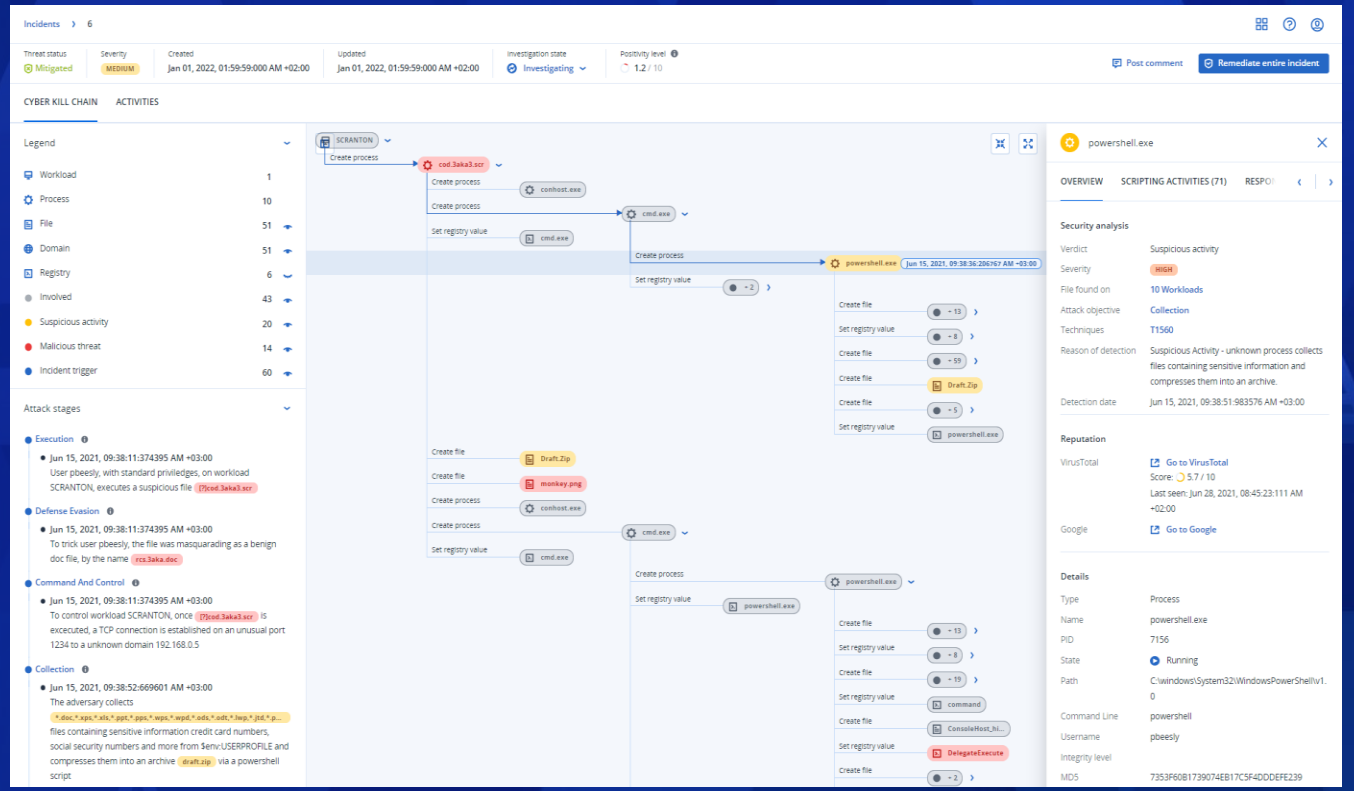
Advanced Security + Endpoint Detection and Response (EDR)

Diseñada para simplificar la seguridad en los endpoints:

1. **Rápida priorización y análisis de incidentes de seguridad**

2. **Continuidad de la actividad empresarial** con copia de seguridad y recuperación integradas

3. Rápido lanzamiento de nuevos servicios con una plataforma unificada y un solo agente fáciles de desplegar, administrar y escalar



Acronis

#CyberFit

Funciones de investigación rápida de incidentes

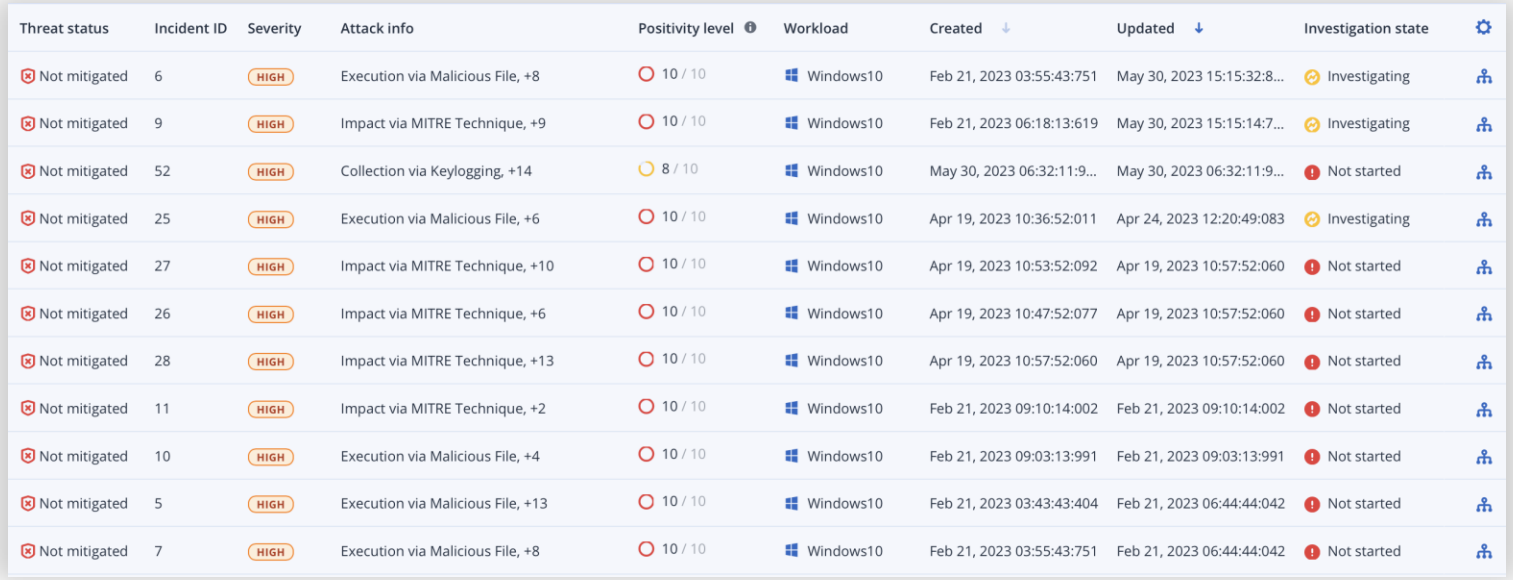
Advanced Security + EDR

Simplifique la priorización de incidentes

Supervisión y correlación de eventos con priorización de ataques y basada en IA

Advanced Security + EDR supervisa y correlaciona continuamente los eventos a nivel de endpoint para detectar cadenas de eventos maliciosos que, cuando se observan como eventos aislados, pueden parecer legítimos:

- Aproveche la **priorización de incidentes de seguridad** basada en IA en todos los endpoints, en lugar de una simple lista de todas las alertas o de analizar cientos de registros.
- **Céntrese en lo que importa** y descargue a su equipo de tareas que consumen muchos recursos, como la caza de amenazas proactiva.
- Utilice una fuente de inteligencia sobre amenazas emergentes para **buscar automáticamente indicadores de compromiso**.



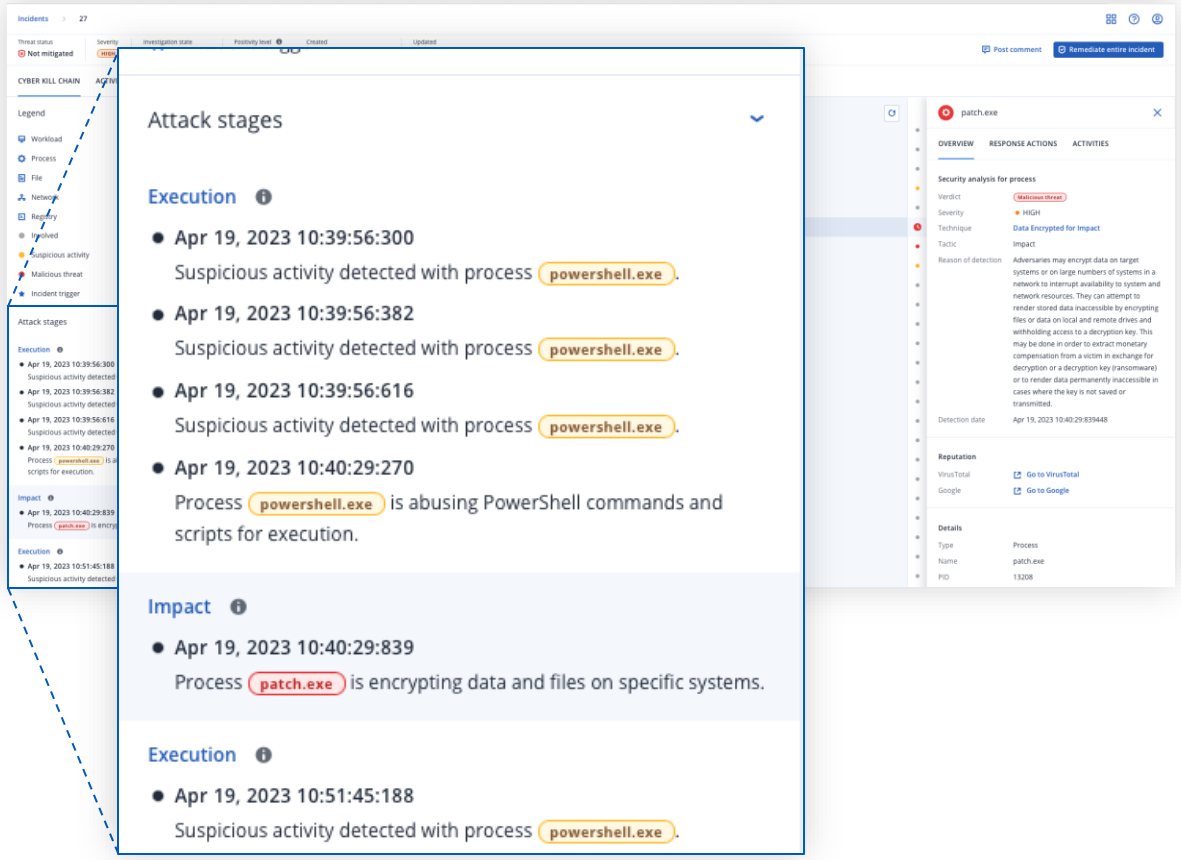
Threat status	Incident ID	Severity	Attack info	Positivity level	Workload	Created	Updated	Investigation state
Not mitigated	6	HIGH	Execution via Malicious File, +8	10 / 10	Windows10	Feb 21, 2023 03:55:43:751	May 30, 2023 15:15:32:8...	Investigating
Not mitigated	9	HIGH	Impact via MITRE Technique, +9	10 / 10	Windows10	Feb 21, 2023 06:18:13:619	May 30, 2023 15:15:14:7...	Investigating
Not mitigated	52	HIGH	Collection via Keylogging, +14	8 / 10	Windows10	May 30, 2023 06:32:11:9...	May 30, 2023 06:32:11:9...	Not started
Not mitigated	25	HIGH	Execution via Malicious File, +6	10 / 10	Windows10	Apr 19, 2023 10:36:52:011	Apr 24, 2023 12:20:49:083	Investigating
Not mitigated	27	HIGH	Impact via MITRE Technique, +10	10 / 10	Windows10	Apr 19, 2023 10:53:52:092	Apr 19, 2023 10:57:52:060	Not started
Not mitigated	26	HIGH	Impact via MITRE Technique, +6	10 / 10	Windows10	Apr 19, 2023 10:47:52:077	Apr 19, 2023 10:57:52:060	Not started
Not mitigated	28	HIGH	Impact via MITRE Technique, +13	10 / 10	Windows10	Apr 19, 2023 10:57:52:060	Apr 19, 2023 10:57:52:060	Not started
Not mitigated	11	HIGH	Impact via MITRE Technique, +2	10 / 10	Windows10	Feb 21, 2023 09:10:14:002	Feb 21, 2023 09:10:14:002	Not started
Not mitigated	10	HIGH	Execution via Malicious File, +4	10 / 10	Windows10	Feb 21, 2023 09:03:13:991	Feb 21, 2023 09:03:13:991	Not started
Not mitigated	5	HIGH	Execution via Malicious File, +13	10 / 10	Windows10	Feb 21, 2023 03:43:43:404	Feb 21, 2023 06:44:44:042	Not started
Not mitigated	7	HIGH	Execution via Malicious File, +8	10 / 10	Windows10	Feb 21, 2023 03:55:43:751	Feb 21, 2023 06:44:44:042	Not started

Analice los ataques en minutos para generar una respuesta rápida

Aproveche la interpretación humana y basada en la IA de los ataques

Permita que su equipo analice los ataques sin esfuerzo, de manera ágil y sencilla:

- **Disfrute de visibilidad total de la cadena de ataque:**
  la evolución del ataque corresponde al marco MITRE (estándar del sector).
  - ¿Cómo consiguió acceder?
  - ¿Cómo ocultó su rastro?
  - ¿Cómo provocó daños?
  - ¿Cómo se propagó?
- **Ahorre tiempo y dinero evitando la necesidad de realizar** cursos de formación rigurosa o contar con personal muy especializado para analizar horas de incidentes de seguridad.



Acronis

#CyberFit

Funciones de respuesta y recuperación integradas

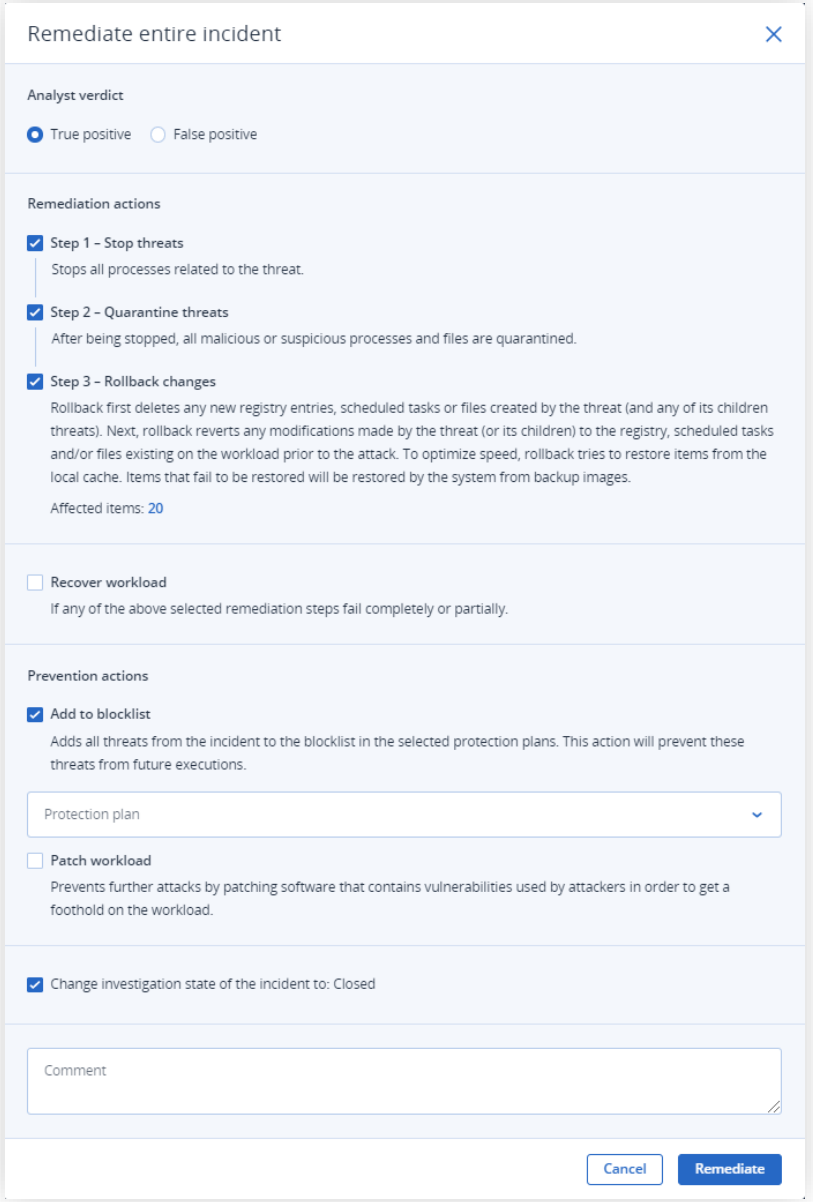
Advanced Security + EDR

Detenga las violaciones de seguridad y garantice la continuidad de la actividad empresarial

Triunfe allí donde las soluciones individuales fallan. Aproveche todo el potencial de una plataforma con funciones integradas para ofrecer a la empresa una resiliencia sin precedentes.

- **Contenga las amenazas aislando en la red** el recurso informático afectado.
- **Investigue en mayor profundidad** mediante **conexiones remotas** y **copias de seguridad forenses**.
- **Corrija los daños, anulando los procesos de malware, poniendo en cuarentena las amenazas y revirtiendo los cambios.**
- Evite la reproducción de los incidentes, **aplicando los parches de software** y **bloqueando la ejecución de las amenazas analizadas**.
- **Garantice una continuidad de la actividad empresarial sin precedentes**, con funciones de **recuperación** integradas, como la **reversión de ataques específicos,** la **recuperación a nivel de archivos o imagen,** y la **recuperación ante desastres**.

Seleccione las acciones que quiere llevar a cabo y responda con un solo clic.



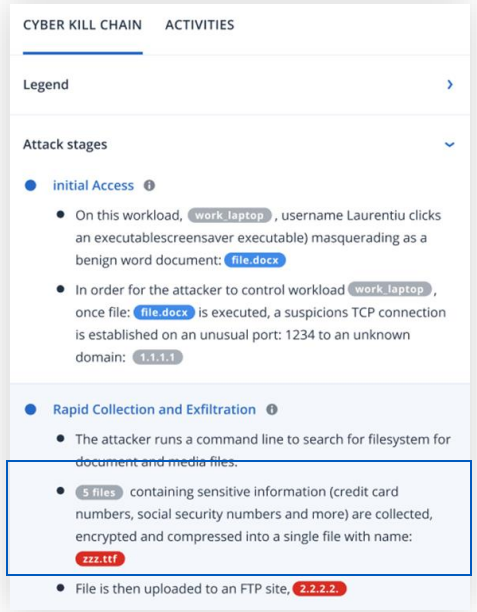
Integrada con protección de datos

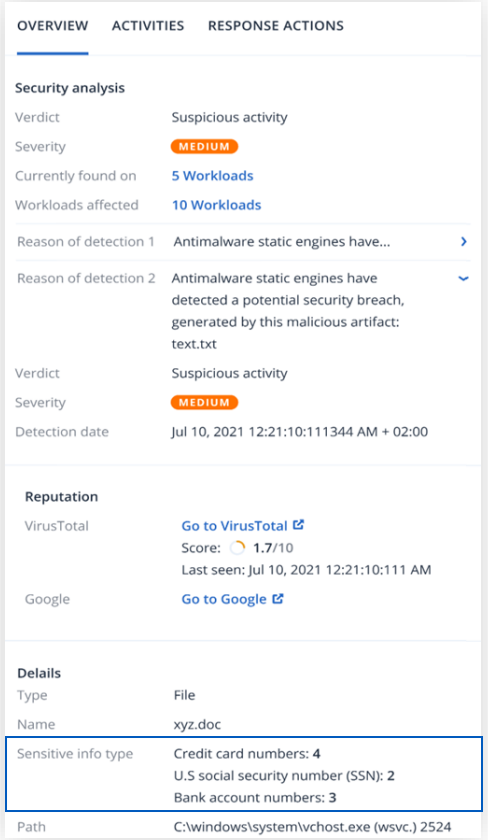
Proteja los datos confidenciales y garantice la continuidad de la actividad empresarial con un solo clic

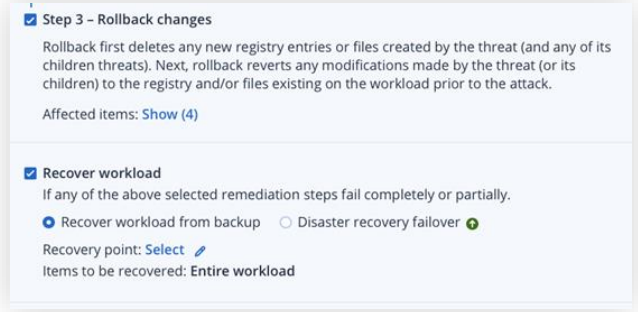
Detecte más rápidamente los ataques dirigidos a datos confidenciales con clasificadores de datos preconfigurados para marcos normativos habituales, como el RGPD, la *HIPAA y la PCI-DSS*

Garantice la continuidad de la actividad empresarial con la mejor **copia de seguridad y recuperación** integradas para más de 20 tipos de recursos informáticos, y disfrute de:

- Reversiones automáticas en caso de ataque de ransomware
- Reversiones específicas para cada ataque
- Recuperación a nivel de archivos y de imagen
- Recuperación ante desastres, incluida orquestación y automatización
- Prevención proactiva de la filtración de datos confidenciales a través de dispositivos locales
- Protección de los datos almacenados con cifrado AES-256 y funciones de recuperación segura







Acronis

#CyberFit

Casos de uso principales

Advanced Security + EDR: 4 casos principales

Detección y neutralización de ataques antes de la vulneración de seguridad

- **Supervisión y correlación de eventos** en los endpoints
- **Bloqueo de amenazas habituales** con protección de endpoints galardonada
- **Detección de amenazas avanzadas** y análisis en minutos

Respuesta antes de que el daño esté hecho

- **Verdadera continuidad de la actividad empresarial,** con recuperación preintegrada
- **Reducción del impacto**: cuarentena de procesos, aislamiento de recursos informáticos
- **Limitación de la superficie de ataque** para mejorar la protección en el futuro

Cumplimiento de normativas y ciberseguros

- **Informe sobre los incidentes en los endpoints** según el marco MITRE ATT&CK®
- **Clasifique los datos confidenciales**
- **Recopile datos forenses** en copias de seguridad

Consolide las soluciones

- **Lance los servicios y amplíelos con rapidez mediante** una **sola** plataforma
- **Reduzca los costes gracias a la** administración unificada de servicios

Acronis

#CyberFit

Motores y funciones de detección

Advanced Security + EDR

Con motores de detección de reconocido prestigio

Seguridad empresarial aprobada por AV-Comparatives

Prueba de protección con datos reales: **0 falsos positivos**

Prueba de protección antimalware: **0 falsos positivos**

Certificación AV-Test

Detección y neutralización de ataques avanzados: **100 % de detección**

0 falsos positivos

Certificación ICSA Labs

0 falsos positivos

Certificación VB100

0 falsos positivos

Medalla de oro en protección de endpoints

4.5 Excellent

Miembro de Microsoft Virus Initiative

Miembro de AMTSO (Anti-Malware Testing Standard Organization)

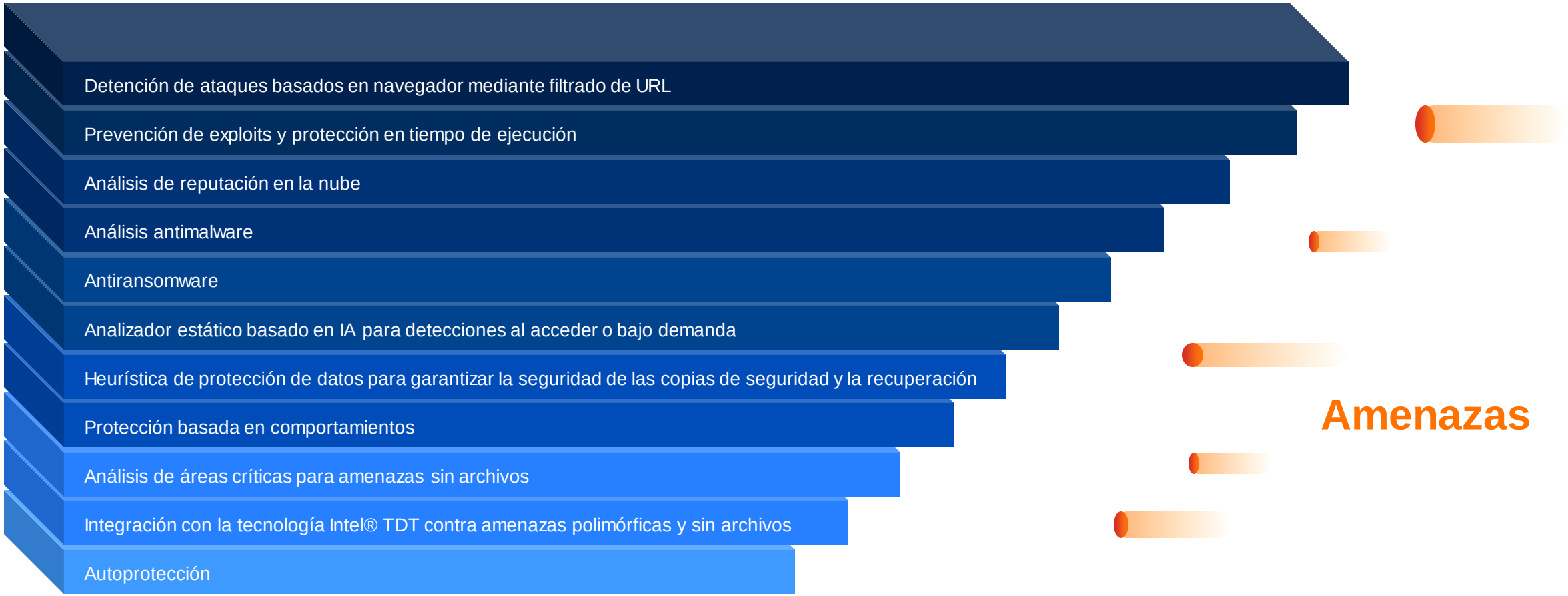
Miembro de APWG (Anti-Phishing Working Group)

Participante y ganador en las pruebas de Anti-Malware Test Lab

Miembro de VIRUSTOTAL

Miembro de CSA (Cloud Security Alliance)

Motores y funciones de detección multicapa de Acronis

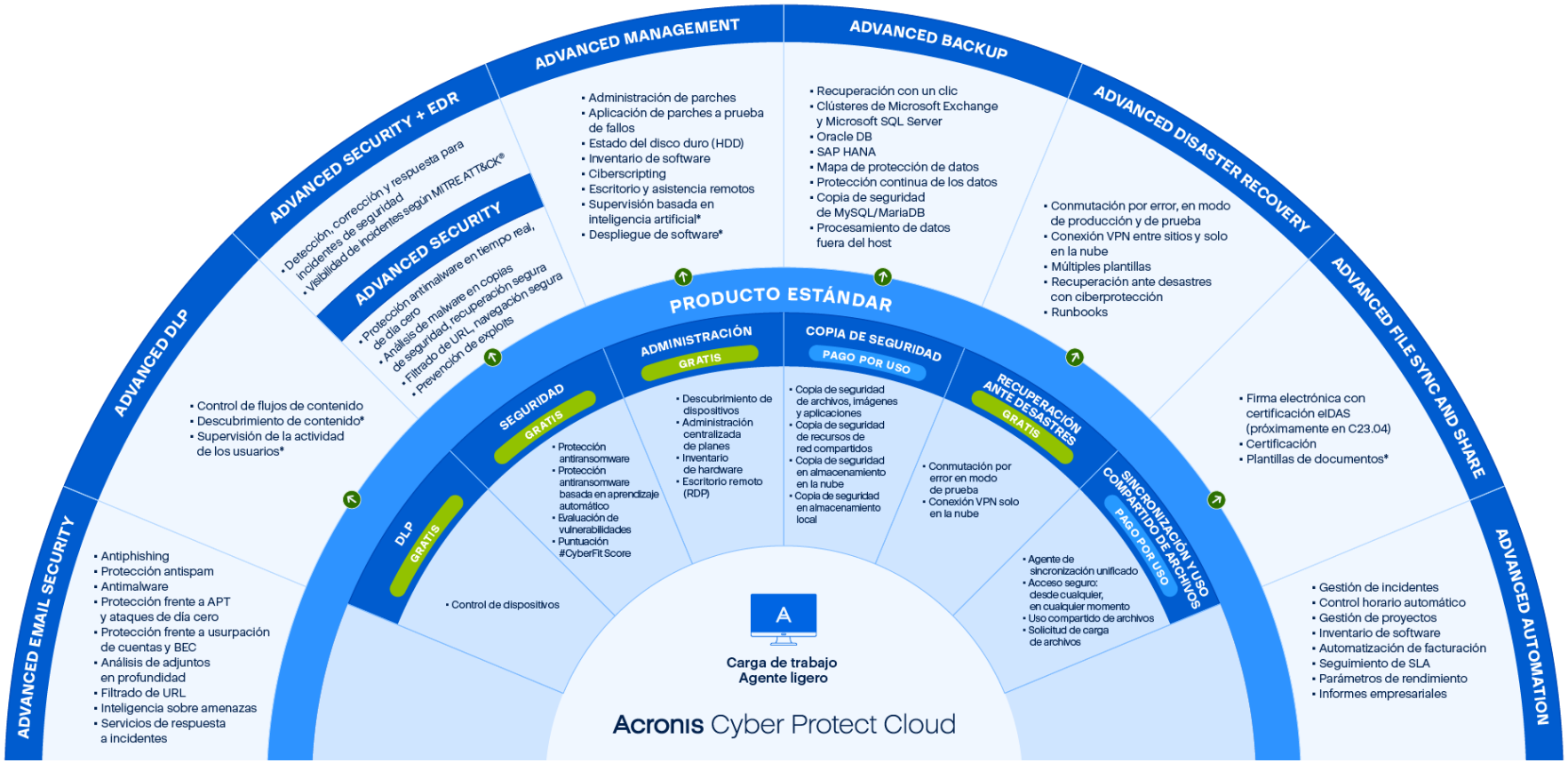


Acronis

#CyberFit

Plataforma de ofrecimiento

Añada paquetes Advanced:
Security, Backup, Disaster Recovery, Email Security, File Sync and Share, Management, DLP y **ahora EDR**



* Próximamente

Optimización de todos los recursos informáticos

Rápido lanzamiento de servicios

Consolidación de proveedores

Acronis

#CyberFit

¿Qué hace de Advanced Security + EDR una oferta inigualable?

¿Qué hace de Acronis EDR una solución inigualable?

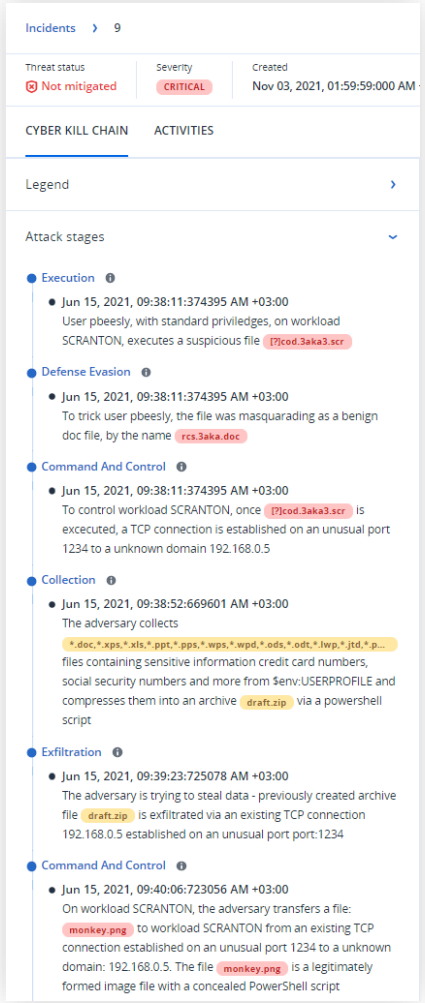
Interpretación de la cadena de ataques basada en IA y fácil de entender

Valor:

- Reduzca el análisis de incidentes de horas a minutos.
- Visibilidad del ataque a través de MITRE ATT&CK®: comprenda cómo llegó el ataque, cómo progresó y cuál fue su impacto.

Soluciones EDR tradicionales:

- Gráfico de la cadena de acontecimientos que se deben interpretar manualmente por su cuenta



Respuesta con un solo clic, incluida la recuperación preintegrada

Valor:

- Corrección completa de incidentes con reversión en un solo clic
- Investigue, corrija, recupere y cierre las brechas de seguridad a través de una consola centralizada

Soluciones EDR tradicionales:

- Conjunto básico de funciones de corrección
- Requieren productos de terceros y un laborioso trabajo manual

Consolidación con una plataforma y un agente únicos

Valor:

- Reducción de costes
- Administración simplificada y centralizada
- Escalabilidad rápida

Productos especializados:

- Dispersión de soluciones
- Administración que consume muchos recursos
- Escalabilidad limitada

Tecnología de Acronis

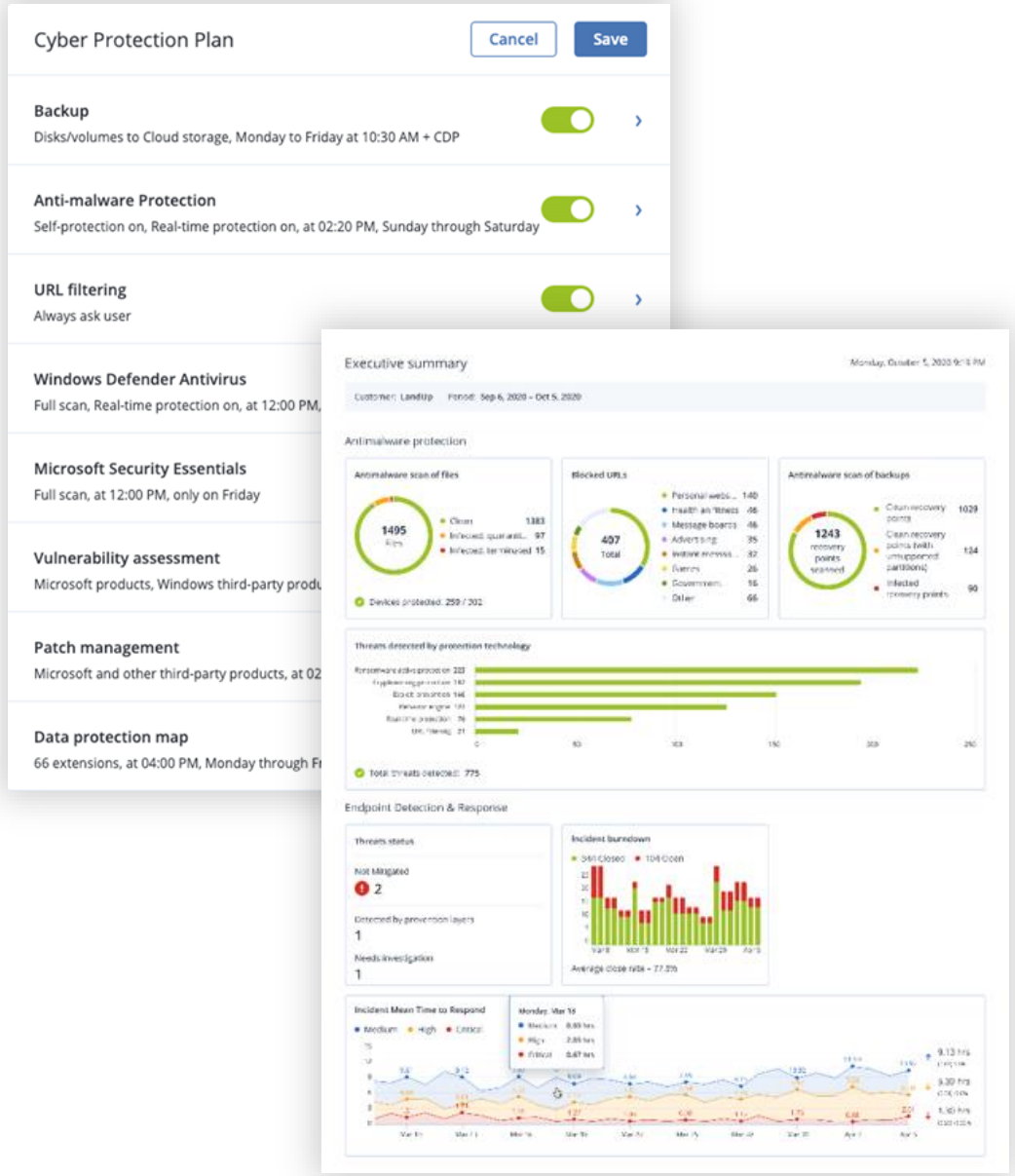
Triunfe allí donde las soluciones individuales fallan. Aproveche todas las ventajas de una plataforma con funcionalidades consolidadas

- **Aprovisionamiento con un único agente**
  - Incorporación de nuevos clientes un 20 % más rápida, en relación con las soluciones individuales
  - Aprovisionamiento de nuevos servicios en minutos
  - Mejora ostensible del rendimiento de los endpoints
- **Tecnologías de detección galardonadas:**
  - Detección basada en comportamientos y firmas, inteligencia artificial/aprendizaje automático/inteligencia automática, antiexploits, anticryptojacking, antiransomware, seguridad del correo electrónico con detección dinámica a nivel de hardware de próxima generación, filtrado de URL
- **Preintegración con la mejor protección de datos y administración de endpoints**

Rápido aprovisionamiento de servicios

Protección total en todo el marco del NIST

Mejor rendimiento



Acronis

Cyber Foundation

Program

Transformando vidas a través de la educación

Trabajemos juntos para generar conocimiento, aportando cada una de nuestras experiencias y fortalezas particulares para crear juntos un futuro mejor.

¡Participe con nosotros!