Las 5 razones principales por las que su empresa debe protegerse cuanto antes con EDR

Acronis

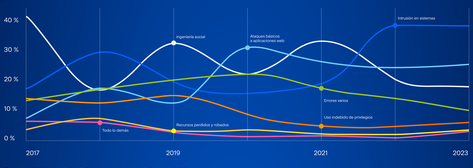
01. El aumento de riesgos digitales exigen dar prioridad a la prevención

El coste medio de una fuga de datos alcanzó en 2023 un máximo histórico de 4,45 millones de dólares. Esto representa un aumento del 2,3 % con respecto a 2022.

Fuente: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

02. Para garantizar una sólida defensa contra ataques avanzados

Los ataques son cada vez más sofisticados, por lo que se necesitan controles de seguridad más avanzados, como la EDR, para estar protegidos.

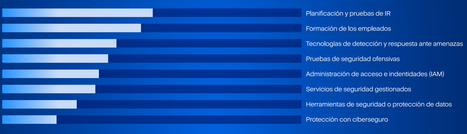


Fuente: 2023 Verizon Data Breach Investigation Report (DBIR)

03. Para conseguir una respuesta ante incidentes más rápida y un análisis más exhaustivo

El 51 % de las organizaciones tiene previsto aumentar sus inversiones en seguridad como consecuencia de haber sufrido algún ciberataque. Las principales áreas de inversión identificadas incluyen la planificación y las pruebas de respuesta ante incidentes (IR), la formación de los empleados y las tecnologías de detección y respuesta ante amenazas.

Tipos de inversión más comunes entre los que deciden aumentar sus inversiones en seguridad tras sufrir algún ciberataque



Fuente: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

04. Para garantizar el cumplimiento de los requisitos normativos vigentes e inminentes

Cada empresa de clase A deberá implementar, a menos que su director de seguridad de la información (CISO) haya aprobado por escrito el uso de controles compensatorios razonablemente equivalentes o más seguros una solución de detección y respuesta para endpoints (EDR) para supervisar cualquier actividad anómala, incluido, entre otros, el desplazamiento lateral.

Fuente: Departamento de Servicios Financieros (DFS) del Estado de Nueva York

Los tres factores que más influyen en el coste de las violaciones de seguridad, de un total de 27 factores.

Fuente: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

05. Para cumplir los requisitos de un ciberseguro

Fuente: Comisión Federal de Comercio (FTC) https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Las mejores prácticas incluyen

- Cifrado de datos confidenciales
- Evaluación de vulnerabilidades y administración de parches
- EDR
- Copia de seguridad programática y plan de recuperación ante desastres
- Políticas estrictas de autenticación (MFA) y autorización (gestión de privilegios mínimos)
- Funciones antimalware basadas en comportamiento
- Formación en concienciación sobre seguridad
- Plan de respuesta ante incidentes

Pruebe la ciberprotección holística que garantiza la resiliencia de su actividad empresarial

Comprar ahora

Probar ahora