

Cumplimiento, contención de brechas y resiliencia cibernética para el sector bancario

Revele las rutas de ataque. Contenga las brechas rápidamente. Mantenga los sistemas bancarios críticos en funcionamiento y en cumplimiento.

Las instituciones financieras están en el centro de la economía global, lo que las convierte en objetivos prioritarios de los ciberataques. Los acontecimientos recientes muestran lo rápido que un solo problema puede agravarse. El ataque de ransomware al ICBC detuvo la liquidación de operaciones con títulos del Tesoro de Estados Unidos. Una actualización defectuosa de CrowdStrike interrumpió la visibilidad de los endpoints. Las interrupciones recientes de AWS afectaron los servicios bancarios en todo el mundo.

A medida que los bancos amplían el uso de la nube, los servicios digitales y los proveedores externos, su superficie de ataque crece. Aparecen puntos ciegos, y los atacantes utilizan credenciales débiles y sistemas sin parches para moverse lateralmente hacia activos de alto valor. El aumento de las tensiones geopolíticas y las amenazas patrocinadas por Estados hacen que estos riesgos sean aún más graves.

Los reguladores están elevando las exigencias

Los reguladores están respondiendo con normas más estrictas para mejorar la resiliencia en todo el sector. El marco DORA de la Unión Europea establece estándares rigurosos para la gestión de riesgos de TIC, la continuidad y la recuperación. También exige que las empresas comprendan las complejas dependencias que sustentan sus operaciones.

En Estados Unidos, organismos reguladores como la Reserva Federal, la OCC, la FDIC y el Departamento del Tesoro destacan la importancia de la visibilidad en tiempo real y una contención sólida para ayudar a reducir el riesgo sistémico. Las normas de la SEC sobre divulgación de información cibernética hacen que esta necesidad sea aún más urgente.

Australia y Singapur clasifican los servicios financieros como infraestructura crítica y exigen controles Zero Trust, incluida la segmentación. El mensaje es claro: la resiliencia debe demostrarse, no darse por sentada.

“Con Illumio, hemos dado un salto significativo para maximizar la seguridad y minimizar el riesgo de interrupciones operativas.”

Steffen Nagel

Responsable de TI
Frankfurter Volksbank

Las presiones que enfrentan los CISO hoy

Los CISO deben proteger entornos complejos y en rápida transformación mientras las amenazas aumentan en velocidad y alcance. Estas presiones dificultan la resiliencia:

- **La visibilidad está fragmentada.** Los entornos híbridos crean puntos ciegos que ralentizan la respuesta y dejan los endpoints expuestos.
- **La fatiga de alertas es peligrosa.** Los equipos del SOC se ven abrumados por falsas alarmas, lo que retrasa las decisiones y aumenta la probabilidad de pasar por alto amenazas reales.
- **Es difícil detener el movimiento lateral.** Los atacantes se desplazan por las redes utilizando herramientas comunes, y los ataques se propagan rápidamente antes de que los equipos puedan contenerlos.
- **Los requisitos de cumplimiento cambian constantemente.** Las nuevas normas exigen resiliencia continua, y las fallas acarrearán graves costos legales y reputacionales.
- **Los endpoints son el nuevo campo de batalla.** Las herramientas de detección tienen dificultades para mantenerse al día con las amenazas de día cero, y los ataques continúan incluso con la protección implementada.
- **La responsabilidad está aumentando.** El riesgo cibernético es un asunto del consejo de administración, y los CISO deben demostrar mejoras medibles con recursos limitados.

Illumio: diseñada para la contención de brechas y la resiliencia

Illumio está diseñada para evitar que las brechas se propaguen por entornos híbridos. Su plataforma ofrece contención rápida y escalable en sistemas de nube, centros de datos y endpoints. Los equipos obtienen una visión compartida y en tiempo real de cómo se comunican las cargas de trabajo, lo que facilita la reducción del riesgo.

Illumio Segmentation: el núcleo de Zero Trust

Illumio Segmentation aplica la microsegmentación a nivel del host, en lugar de hacerlo mediante firewalls estáticos o VLAN. Las políticas siguen a las cargas de trabajo dondequiera que se ejecuten. Los controles dinámicos basados en etiquetas permiten a los equipos definir la intención en términos sencillos de negocio y adaptarse a los cambios en los entornos.

Illumio Insights: visibilidad que impulsa la acción

Illumio Insights utiliza un grafo de seguridad basado en IA para mapear el tráfico de las aplicaciones en tiempo real y destacar las rutas que un atacante podría explotar. Las integraciones con Microsoft Sentinel y Security Copilot ayudan a los analistas a filtrar el exceso de alertas, centrarse en los riesgos reales y aislar rápidamente las cargas de trabajo. Al transformar los datos brutos de tráfico en inteligencia procesable, Insights mejora la resiliencia y ayuda a cumplir con las crecientes expectativas regulatorias.

Valor comprobado para las instituciones financieras

Illumio cuenta con la confianza de organizaciones financieras líderes. Seis de los diez principales bancos globales y más del 20% de las empresas de Fortune 100 utilizan Illumio para proteger cientos de miles de cargas de trabajo.

El estudio Total Economic Impact de Forrester encontró que los clientes ahorran, en promedio, US\$3 millones en firewalls de centros de datos y reducen los costos operativos en un 90%.

Las amenazas cibernéticas a los bancos son constantes, pero su impacto puede contenerse. La plataforma Illumio ayuda a las instituciones a visualizar cómo se conectan los sistemas, detener la propagación de los ataques y responder más rápido cuando ocurren incidentes.

Mejore la resiliencia cibernética

Conozca cómo Illumio ayuda al sector bancario a proteger los sistemas críticos.

Visite: illumio.com/solutions/banking-and-financial-services

Acerca de Illumio

Illumio es líder en contención de ransomware y brechas, y redefine la forma en que las organizaciones contienen los ciberataques y hacen posible la resiliencia operativa. Impulsada por un grafo de seguridad basado en IA, nuestra plataforma de contención de brechas identifica y contiene amenazas en entornos híbridos multinube, deteniendo la propagación de los ataques antes de que se conviertan en desastres.

Reconocida como Líder en Forrester Wave™ para microsegmentación, Illumio hace posible Zero Trust y fortalece la resiliencia cibernética de la infraestructura, los sistemas y las organizaciones que mantienen al mundo en funcionamiento.

Copyright © 2025 Illumio, Inc. Todos los derechos reservados. Illumio® es una marca comercial o una marca registrada de Illumio, Inc. o sus filiales en Estados Unidos y otros países. Las marcas comerciales de terceros mencionadas en este documento son propiedad de sus respectivos titulares.