

# Conformidade, contenção de violações e resiliência cibernética para o setor bancário

Revele os caminhos de ataque. Contenha violações rapidamente. Mantenha os sistemas bancários críticos em operação e em conformidade.

As instituições financeiras estão no centro da economia global, o que as torna alvos prioritários de ataques cibernéticos. Acontecimentos recentes mostram como um único problema pode se agravar rapidamente. O ataque de ransomware ao ICBC interrompeu a liquidação de operações com títulos do Tesouro dos EUA. Uma atualização defeituosa da CrowdStrike interrompeu a visibilidade dos endpoints. Indisponibilidades recentes da AWS afetaram serviços bancários em todo o mundo.

À medida que os bancos ampliam o uso de nuvem, serviços digitais e fornecedores terceirizados, sua superfície de ataque cresce. Surgem pontos cegos, e os invasores usam credenciais fracas e sistemas sem correções de segurança para se movimentar lateralmente em direção a ativos de alto valor. O aumento das tensões geopolíticas e as ameaças patrocinadas por Estados tornam esses riscos ainda mais graves.

## Os reguladores estão elevando as exigências

Os reguladores estão respondendo com regras mais rigorosas para melhorar a resiliência em todo o setor. O marco regulatório DORA da União Europeia estabelece padrões rígidos para a gestão de riscos de TIC, continuidade e recuperação. Também exige que as empresas compreendam as dependências complexas que sustentam suas operações.

Nos EUA, órgãos reguladores como o Federal Reserve, o OCC, a FDIC e o Departamento do Tesouro enfatizam a visibilidade em tempo real e uma contenção eficaz para ajudar a reduzir o risco sistêmico. As regras da SEC sobre divulgação de informações cibernéticas tornam essa necessidade ainda mais urgente.

Austrália e Singapura classificam os serviços financeiros como infraestrutura crítica e exigem controles Zero Trust, incluindo segmentação. A mensagem é clara: a resiliência deve ser demonstrada, não presumida.

**“Com a Illumio, demos um salto significativo para maximizar a segurança e minimizar o risco de interrupções operacionais.”**

**Steffen Nagel**

Responsável por TI  
Frankfurter Volksbank

## As pressões que os CISOs enfrentam hoje

Os CISOs precisam proteger ambientes complexos e em rápida transformação, enquanto as ameaças aumentam em velocidade e alcance. Estas pressões dificultam a resiliência:

- **A visibilidade é fragmentada.** Ambientes híbridos criam pontos cegos que tornam a resposta mais lenta e deixam endpoints expostos.
- **A fadiga de alertas é perigosa.** As equipes do SOC ficam sobrecarregadas com falsos alarmes, o que atrasa decisões e aumenta a probabilidade de deixar ameaças reais passarem despercebidas.
- **É difícil impedir a movimentação lateral.** Os invasores se deslocam pelas redes usando ferramentas comuns, e os ataques se propagam rapidamente antes que as equipes consigam contê-los.
- **As exigências de conformidade mudam constantemente.** Novas regras exigem resiliência contínua, e as falhas acarretam custos jurídicos e reputacionais graves.
- **Os endpoints são o novo campo de batalha.** As ferramentas de detecção têm dificuldade para acompanhar ameaças de dia zero, e os ataques continuam mesmo com a proteção implementada.
- **A responsabilização está aumentando.** O risco cibernético é uma questão que compete ao conselho de administração, e os CISOs precisam demonstrar melhorias mensuráveis com recursos limitados.

## Illumio: desenvolvida para contenção de violações e resiliência

A Illumio foi desenvolvida para impedir que violações se propaguem por ambientes híbridos. Sua plataforma oferece contenção rápida e escalável em sistemas na nuvem, em data centers e em endpoints. As equipes obtêm uma visão compartilhada, em tempo real, de como as cargas de trabalho se comunicam, facilitando a redução de riscos.

## Illumio Segmentation: o núcleo do Zero Trust

O Illumio Segmentation aplica a microsegmentação no nível do host, e não por meio de firewalls estáticos ou VLANs. As políticas acompanham as cargas de trabalho onde quer que sejam executadas. Controles dinâmicos baseados em rótulos permitem que as equipes definam a intenção em termos simples de negócio e se adaptem às mudanças nos ambientes.

## **Illumio Insights: visibilidade que impulsiona a ação**

O Illumio Insights usa um grafo de segurança baseado em IA para mapear o tráfego de aplicações em tempo real e destacar os caminhos que um invasor poderia explorar. As integrações com Microsoft Sentinel e Security Copilot ajudam os analistas a filtrar o excesso de alertas, concentrar-se nos riscos reais e isolar cargas de trabalho rapidamente. Ao transformar dados brutos de tráfego em inteligência acionável, o Insights melhora a resiliência e ajuda a atender às crescentes expectativas regulatórias.

## **Valor comprovado para instituições financeiras**

**A Illumio conta com a confiança de organizações financeiras líderes.** Seis dos dez maiores bancos globais e mais de 20% das empresas da Fortune 100 usam a Illumio para proteger centenas de milhares de cargas de trabalho.

O estudo Total Economic Impact da Forrester constatou que os clientes economizam, em média, US\$ 3 milhões em firewalls de data center e reduzem os custos operacionais em 90%.

As ameaças cibernéticas aos bancos são constantes, mas seu impacto pode ser contido. A plataforma Illumio ajuda as instituições a visualizar como os sistemas se conectam, impedir a propagação de ataques e responder mais rapidamente quando ocorrem incidentes.

## **Melhore a resiliência cibernética**

Saiba mais sobre como a Illumio ajuda o setor bancário a proteger sistemas críticos.

Acesse: [illumio.com/solutions/banking-and-financial-services](https://illumio.com/solutions/banking-and-financial-services)

## **Sobre a Illumio**

A Illumio é líder em contenção de ransomware e violações, redefinindo como as organizações contêm ataques cibernéticos e viabilizam a resiliência operacional. Impulsionada por um grafo de segurança baseado em IA, nossa plataforma de contenção de violações identifica e contém ameaças em ambientes híbridos multinuvem, impedindo a propagação de ataques antes que se tornem desastres.

Reconhecida como Líder no Forrester Wave™ para microsegmentação, a Illumio viabiliza o Zero Trust, fortalecendo a resiliência cibernética da infraestrutura, dos sistemas e das organizações que mantêm o mundo em funcionamento.

Copyright © 2025 Illumio, Inc. Todos os direitos reservados. Illumio® é uma marca comercial ou marca registrada da Illumio, Inc. ou de suas afiliadas nos EUA e em outros países. As marcas comerciais de terceiros mencionadas neste documento pertencem aos seus respectivos proprietários.