illumio

INDUSTRY GUIDE

Zero Trust Segmentation in Banking and Financial Services

Banks and other financial institutions are turning to Zero Trust Segmentation to guard against ransomware and similar cyberattacks that can trigger financial losses and reputational damage

Modern Bank Robbers Are Zeroing in on Financial Services

Banks, investment houses, retail brokerages, lenders, fintech startups and other financial services institutions are the proverbial "big game" for cybercriminals. The reason is simple: That's where the money is.

Financial services was the top industry targeted by cybercriminals for five consecutive years of 2016-2020, according to an IBM report. In 2021, financial services accounted for 22.4% of attacks, in second place just behind manufacturing – but still very much a prime target for ransomware and other cyberstrikes.

Of attack types, ransomware was far and away the most prevalent in financial services, accounting for 36 percent of attacks across all industries, IBM reported.

Risk of a cyberattack is heightened as banks and other institutions undergo digital transformation, introduce new cloud systems, and expand partnerships with third-party products and service providers. Brisk M&A activity, continued use of legacy IT and cybersecurity systems, and a shift to remote work can also erode an institution's security posture.

Those technological and business changes broaden the attack surface and pose new challenges to visibility. Detecting and identifying a breach is becoming more difficult across complex and interconnected networks. If a breach does occur, a bank can suffer sizable financial losses and negative publicity that undermine confidence among commercial and retail customers, business partners, counterparties, investors and regulators.

Guarding against ransomware and other kinds of cyberattacks has become more than just a cybersecurity problem – it's now a business resilience challenge at the highest levels.

In this guide, we explore the unique cybersecurity challenges facing banks and other financial services providers. We examine how Zero Trust Segmentation provides an invaluable defense that protects both the financial institution and its customers across a rapidly changing landscape.

> "The increasing use of digital services and the widespread reliance on technology, together with the growing use and interconnectedness of third-party products and services, are increasing financial market infrastructures' vulnerability to cyberattacks."
>
> **European Central Bank**

Cyberattack Risks to Financial Institutions Are Rising

Chief information security officers (CISOs) in banking and financial services are keenly aware of the threat that cybercrime poses to their organizations. Governments are as well. For example:

- The U.S. names financial services as one of 16 critical infrastructure sectors that, if incapacitated by an attack, could have devastating consequences.
- The European Union is implementing a new cybersecurity regulatory framework called the Digital Operational Resilience Act (DORA), affecting thousands of EU financial institutions.
- Australia in late 2021 named financial services as a critical infrastructure sector, introducing an enhanced regulatory framework affecting banks and other financial institutions.

High on the long list of cybersecurity risks are diminished customer trust, sizable financial loss and regulatory non-compliance.

Customer trust and churn

A high-profile cyberattack can erode customer trust, trigger churn and deter would-be customers. In fact, a study by Ponemon Institute and IBM found that in banking, lost business amounts to 55 percent of the overall cost of a data breach.

Customers expect that banks can protect their sensitive data, such as government ID numbers and physical addresses, from being stolen and sold on black markets. That concern is heightened in times of rising inflation and interest rates, making customers even more discriminating in choosing a financial services provider.

> "Trust can be damaged by a cyberattack, and with attacks increasingly focused on brand reputation and information assets, the potential impact to trust is of significant concern to financial institutions."
>
> **EY, How Financial Services Boards Are Addressing Top Cyber Risks**

Overall financial loss

The average cost of a data breach in financial services reached $5.97 million in 2021, 37 percent higher than the average across other industries, according to the Cost of a Data Breach Report 2022 from Ponemon Institute and IBM.

Those costs include lost business, cyberattack response and remediation, and regulatory or civil litigation fines. The financial impact can be especially damaging to smaller and mid-market institutions that lack the resources and more sophisticated cyberdefenses of larger competitors.

Regulatory requirements and penalties

Financial services CISOs are under pressure to strengthen cyberdefense as regulatory requirements tighten, new threats emerge and business models evolve.

Security leaders are challenged to stay on top of ever-changing standards such as ISO 27001, PCI-DSS, SWIFT and COBIT, along with standards from organizations such as the National Institute of Standards and Technology and the Center for Internet Security.

Numerous reports state that Board of Directors members have been named as defendants in cybersecurity litigation for being in breach of regulations. Though none have been held liable, these instances increase the pressure security leaders face.

Regulatory and industry bodies around the world are mandating or recommending increased visibility, improved segmentation of IT assets, and a transition to Zero Trust architectures.

For example, the Monetary Authority of Singapore's Cyber Security Advisory Panel in late 2021 endorsed Zero Trust security principles to address cyberthreats. And the Bank Policy Institute, a U.S.-based advocacy organization comprised of leading banks, urged banks to implement a Zero Trust strategy as a critical cyberdefense in2022.

In an in-depth paper, the Bank Policy Institute noted that:

"Legacy perimeter-based defense models used by financial institutions are insufficient to prevent malicious actors from causing financial, operational, reputational and client harm... In a Zero Trust Architecture, we look to improve security posture by moving layered controls closer to the resources instead of relying on the network perimeter itself."

Regulatory and civil legal actions further raise the stakes for robust cybersecurity. For example, Capital One agreed to pay $190 million to settle a class-action lawsuit suit over a data breach involving 100 million customers. The firm suffered both a financial loss and negative publicity that can undermine consumer trust.

$5.97 million
average data breach cost
in financial services

Ponemon Institute/IBM,
Cost of a Data Breach Report 2022

A Growing Attack Surface Attracts Cybercriminals

The volume and sophistication of cybercrime targeting financial institutions continues growing, even as banks and other providers invest in security technology and resources that are advanced compared to other industries. A study of financial services institutions by VMware found that in 2021:

- 63 percent of financial institutions saw an increase in cyberattacks.
- 74 percent of financial services leaders experienced at least one ransomware tack.
- 63 percent of those victims paid the ransom.
- 66 percent saw attacks targeting market strategies.

Phishing, attempts to exploit vulnerabilities, password spraying, and VPN access are among the top attack vectors. And the universe of bad actors is expanding, with nation-states and state-sponsored hackers becoming more prevalent and creative.

Cybercriminals are looking to exploit an attack surface that has broadened at many financial institutions in the past few years, driven by several dynamics:

- Increased digitization of financial services
- IT diversification with digital transformation
- Inconsistent security measures across disparate systems
- Growing networks of external partners and providers
- Onboarding new systems after merger, acquisition or divestiture
- Reliance on aging legacy systems
- Increased work-from-home and remote staff

The changing landscape and growing cyberthreats are prompting leading financial institutions to augment and simplify their traditional perimeter-based defenses with Zero Trust Segmentation.

"The rapid digitization of financial services, which accelerated with the pandemic, has led to an increase in global cyber threats. Third-party attacks pose significant risks to the financial industry due to our reliance on a myriad of providers and suppliers."

Financial Services Information Sharing and Analysis Center, Navigating Cyber 2022

Illumio Zero Trust Segmentation in Banking and Financial Services

Illumio's Zero Trust Segmentation technology enhances traditional perimeter and firewall defenses to embed security at a far more granular level into the interior of networks and data centers. Instead of a single firewall protecting hundreds of applications and devices, security is applied at each asset individually.

Financial services CISOs use Illumio to help achieve three top objectives of protecting customer data, achieving regulatory compliance, and enabling digital transformation:

1. **Protect customer data** by understanding access to systems, implementing security policies to limit systems access, and reporting and analyzing all traffic that doesn't match rules.
2. **Achieve regulatory compliance** by scoping vulnerabilities across the full environment, mapping application dependencies, applying granular segmentation policies, and monitoring connectivity for vulnerability and compliance violations.
3. **Enable digital transformation** with visibility into relationships between data center and cloud components, by securing both on-premises and cloud applications consistently, and by integrating with DevOps processes to automate security at scale.

Zero Trust benefits in banking

The Bank Policy Institute cites security and business benefits in recommending that banks adopt Zero Trust security:

- Reduced attack surface
- Improved application and data protection
- Enhanced visibility across assets
- Reduced risk of malware
- Faster breach detection
- Continuous security compliance
- Streamlined mergers and acquisitions

Illumio's defense-in-depth model bars lateral movement of malware, even if it's able to infiltrate an asset, such as an application or device. It's like thieves breaking into a building, but they can't move beyond the first room they entered.

Illumio follows the Zero Trust principle that no application, device or user can be trusted without verification and must therefore only have least-privilege access. As a result, financial institutions can protect critical assets and stop malicious actors from reaching critical systems and data, guarding against loss of customer and market data, or a major operational failure.

Segmentation Security, Ransomware Containment and Visibility

Named a Leader in The Forrester New Wave™: Microsegmentation, Q1 2022, Illumio's core capabilities equip banks and other financial institutions to:

- Secure critical assets and services, even in the event of a breach.
- Stop the spread of ransomware across networks, data center servers and applications.
- Realize comprehensive visibility across applications, devices and networks.

1. Secure critical assets and services

Illumio Zero Trust Segmentation ensures that access to any asset or application is secure and authenticated. It eliminates paths that allow lateral movement and enforces and maintains policy within large, rapidly changing environments. With Illumio, you can:

- **Easily segment assets, environments, users and groups.** Build Zero Trust access rules through data-driven policy design, automatic policy creation, and scalable enforcement using your existing network and device infrastructure.
- **Enforce policies dynamically to consistently secure evolving applications, devices and networks.** Write simple rules to govern access and communications across internal and partner systems. Policies will automatically update as systems change.
- **Operate at the host level.** Manage existing host-based firewalls that scale easily. Managed from a single console, all without moving cables or changing your virtual infrastructure.

Illumio stops ransomware in ways that legacy security tools simply cannot. With Illumio, you will reduce your attack surface, limit the blast radius of a successful breach, and protect your most sensitive data, applications and assets.

> "Many financial services organizations are taking a Zero Trust approach to cybersecurity. [Zero Trust] lays the foundation to help organizations meet the challenges caused by evolving business models, shifting workforce dynamics, and IT environments."
>
> **Deloitte, Security in the Age of the Porous Perimeter**

"Zero Trust segmentation or microsegmentation is fine-grained control of application needs, user access, and data repositories. Tools help automate, orchestrate, test and implement granular policy across network security controls."

Forrester, Trusting Zero Trust

2. Contain ransomware

Illumio immediately shrinks your attack surface by automating workflows — like policy discovery, authoring, distribution and enforcement — that block communications on any high-risk port in your network. With Illumio, you can:

- **Pinpoint your critical sources of ransomware risk.** See all of your commonly exploited pathways, orphaned legacy connections, and data flows that are out of compliance with your existing security policies.
- **Proactively close and monitor high-risk pathways.** Close commonly exploited ports in your environment while monitoring those ports that must remain open.
- **Create a reactive containment switch to stop in-progress incidents.** Develop a one-click solution that can precisely block communications down to the workload level, isolating and protecting unaffected systems during an incident.

Global 250 bank meets SWIFT compliance requirements

The IT team at a Global 250 bank tackling SWIFT compliance requirements struggled with building granular microsegmentation policies using a traditional firewall approach. The task proved complex and time-consuming while limiting the flexibility the bank needed.

By implementing Illumio, the bank realized real-time visibility into application dependencies and vulnerabilities. IT and application owners collaborated to swiftly create microsegmentation policies that isolated diverse systems running on premises, in the cloud, and on bare metal servers and virtual machines.

As a result, the bank secured its payment systems, strengthened control over traffic flows, and achieved SWIFT compliance that had been exceedingly difficult with its previous approach.

"Microsegmentation with Illumio Core is more scalable, more agile and quicker to implement than other solutions," says the bank's VP of enterprise systems. "Illumio's ability to work on virtual machines, on-premise, bare metal, or in the cloud has ensured consistent security across our environments."

See the case study

"Ransomware can result in a sudden and unplanned suspension of critical core banking services, and payment of a ransom does not guarantee records can be restored in a timely fashion or even restored at all. In severe cases, this could result in the financial institution's failure."

Conference of State Bank Supervisors, Electronic Crimes Task Force, Ransomware Preparedness

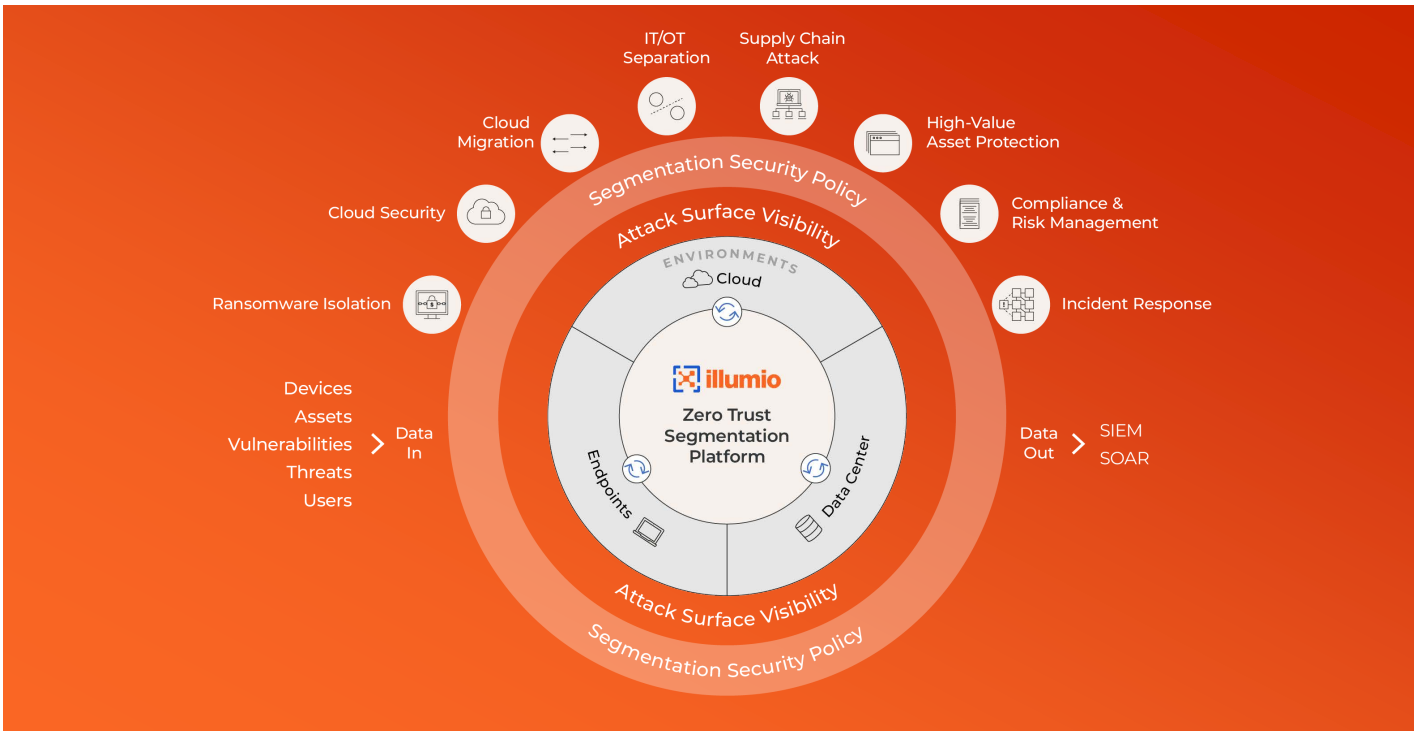
3. Visualize device and system communication

Illumio provides actionable insights by mapping all communications between assets, including applications, clouds, containers, data centers and endpoint devices. And it does this without touching or changing your network. With Illumio, you can:

- **Build real-time network visibility.** Automatically map the internal communications and outbound Internet connections for each of your applications, systems and workloads.
- **Lower operational risk by identifying unnecessary connections.** Build a clear picture of your vulnerable systems, noncompliant data flows, and excessive communications. You'll gain a better understanding of what's open and why.
- **Share a unified view of your communications for your teams and your SIEM/SOAR tools.** Create tight collaboration, offering customized views for Network Ops, Security Ops, DevOps and DevSecOps. Feed real-time data to your SIEM or SOAR.

"Zero Trust is an information security model moving from perimeter-based defense to minimizing trust by continuously verifying that access is secure, authenticated and authorized."

Forrester, Trusting Zero Trust



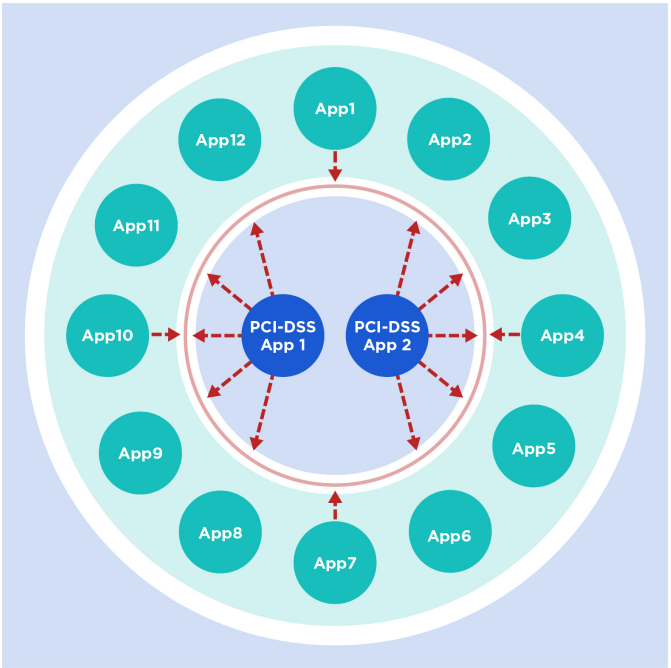
The Illumio platform addresses multiple cybersecurity use cases in banking and financial services.

Sample use case with PCI-DSS

PCI-DSS requirements dictate that controls be in place around a cardholder data environment (CDE) to ensure that PCI data is contained within a boundary.

Illumio lets you easily define an enforcement boundary to segment PCI-DSS apps and non-PCI-DSS apps. That ensures that all traffic across the cardholder data environment is on an explicit allowlist, quickly and effectively addressing the PCI-DSS compliance requirement.

Illumio's visibility allows you to clearly see the full scope of a CDE. As a result, you avoid needlessly expanding segmentation across out-of-scope systems at significant time and cost, or making segmentation too narrow and jeopardizing compliance.



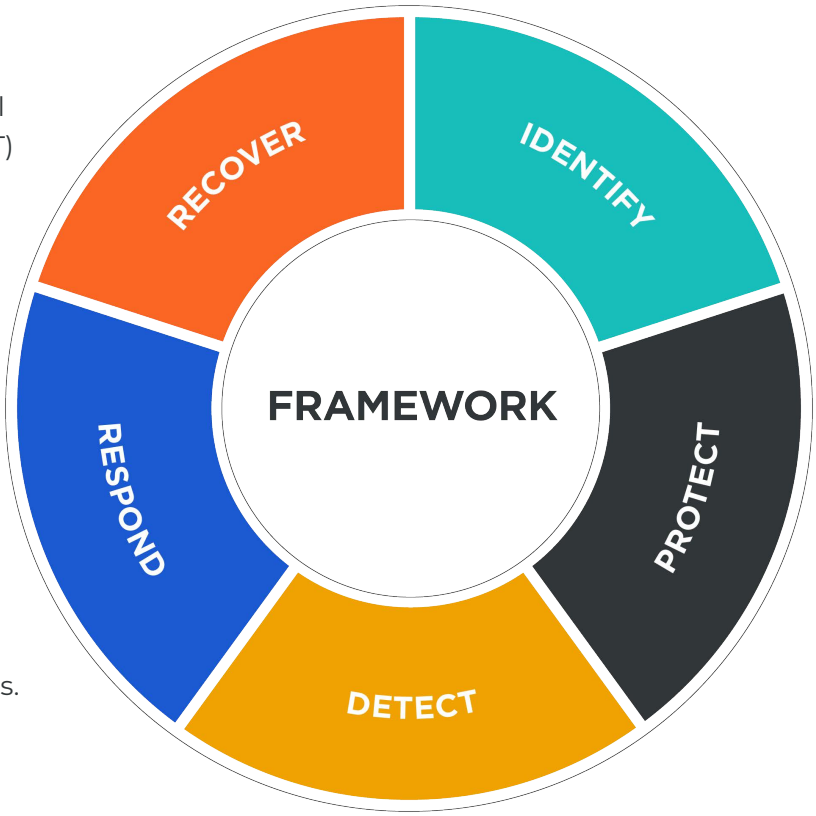
Production

Illumio makes it easy to create an enforcement boundary to meet PCI-DSS compliance requirements.

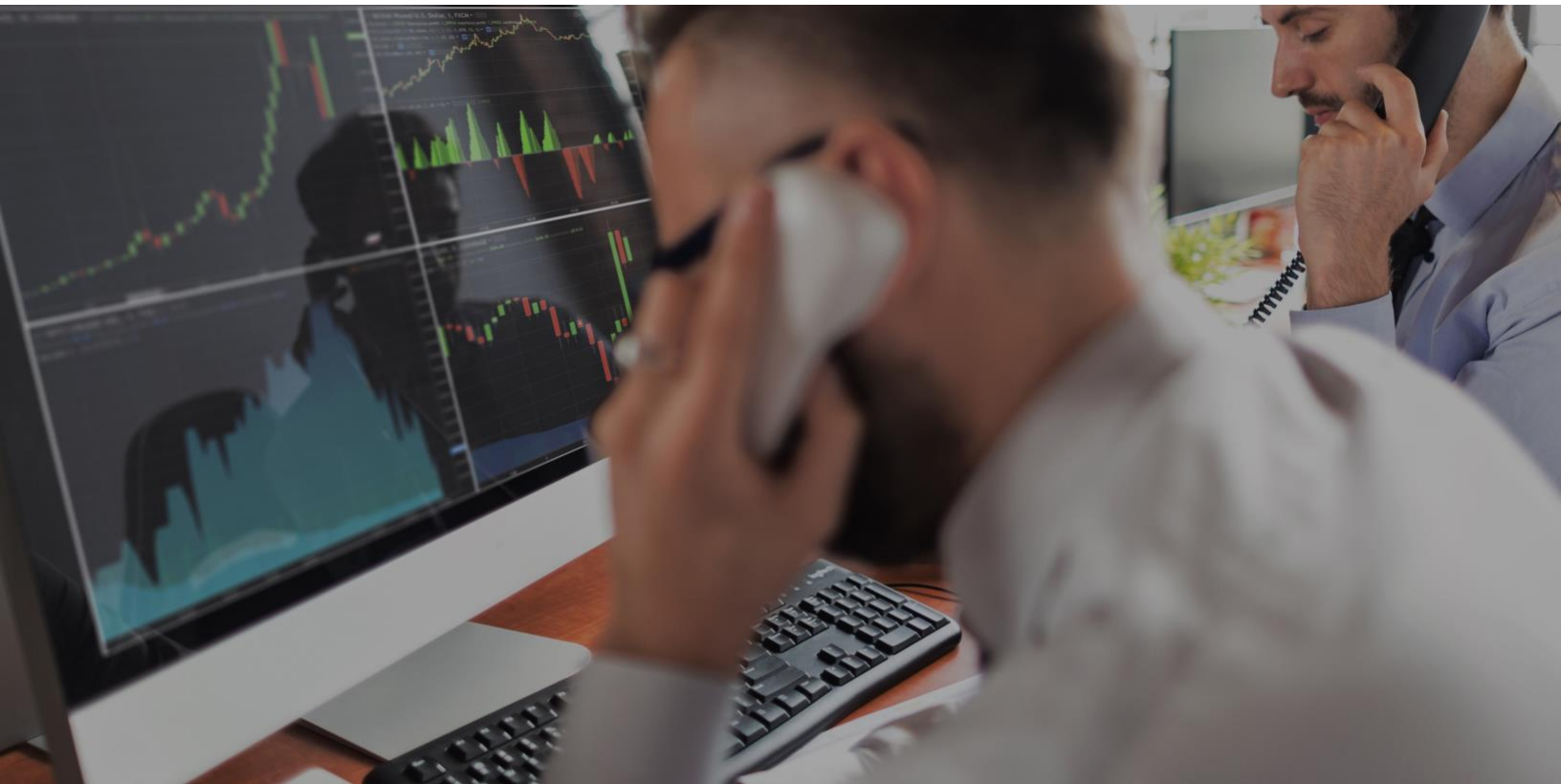
Aligning With the NIST Cybersecurity Framework for Banking

Illumio solutions align with the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, which supplies the foundation for a model specific to financial services that's managed through the Cyber Risk Institute, a subsidiary of the Bank Policy Institute.

Illumio supports the framework and its five pillars of Identify, Protect, Detect, Respond and Recover. Illumio solutions including Illumio Core, Illumio Endpoint and Illumio CloudSecure products, along with Illumio technology partners, provide additional security capabilities and functionality specific for financial institutions.



The NIST Cybersecurity Framework is based on five steps of Identify, Protect, Detect, Respond and Recover.



Illumio NIST Mapping

Illumio makes it far easier for financial services organizations to implement the NIST Cybersecurity Framework, as well as support Zero Trust security practices. Together, these complementary initiatives greatly improve cyber resilience for organizations in this sector.

Illumio streamlines the adoption of the NIST framework and simplifies the path to Zero Trust security. In this section, we will look at each of the steps in the NIST Cybersecurity Framework and how to use Zero Trust Segmentation to achieve them.

Identify

Identifying what to protect and when to do it can sometimes become the most complex and controversial part of any cybersecurity strategy. Budget and resource restrictions often limit the ability to protect everything to the same level and at the same time.

The first step is a simple audit to identify which systems will have the biggest impact on delivering core services. Core banking, trading systems, payment systems and financial risk management are likely to be at the top, with functions such as catering or car parking at the other end of the spectrum. Using a model that maps the likelihood of an attack with the impact of an attack will help pinpoint the relative risk of each area.

The second step is to understand your communications pathways – what is talking to what.

Illumio generates a simple map to show all devices and their communication flows with traditional IT systems, such as applications, servers, databases, the Internet, or even smart devices. It is important that this map include any communication with workloads or services in the cloud. This is especially true as banks increasingly use a hybrid model for hosting applications, with components running across private data centers and multiple public clouds.

Illumio's application dependency map uses metadata from IT devices, and information gathered from OT and IoT security platforms such as Cylera and Armis. It can also be enriched with data from a CMDB (configuration management database) like ServiceNow and from the asset inventories in a public cloud.

The Illumio Core Services Detector will identify core IT services that need protecting like DNS, DHCP, etc. The need to perform this task is stated in the NIST CSF, and unlike many other solutions, Illumio provides real-time traffic flow information without impacting the operation of the network.

With this knowledge, generating the required security policies is a much simpler process.

Protect

Once you have identified what to protect, you then need to enforce that protection. The simplest first step is to deploy Zero Trust Segmentation.

Zero Trust Segmentation prevents communications except for those that are allowed and verified – enforcing the concept of "least privilege."

Illumio allows for these security policies to be implemented natively on supported operating systems and cloud service providers, and – through technology integrations – across a multitude of other platforms including mainframes, AS/400, switches, load balancers and traditional firewalls.

With least-privilege security controls consistently deployed across a hybrid network, financial organizations can stop a cyberattack at its first point of entry – preventing any further movement across the network.

With Zero Trust Segmentation, you can block specific traffic routes and ports that cyberattackers and ransomware typically use. Or you can block all traffic on a given pathway while allowing only traffic from specific sources.

This limits the lateral movement of an attack like ransomware that is trying to access high value assets. Ransomware will use popular existing protocols like RDP to move around the network.

By limiting this movement, you can contain ransomware and prevent it from reaching high value assets like core banking and trading systems.

Zero Trust Segmentation helps ensure that a bank can continue to deliver services and protect customer data even while undergoing a cyberattack.

Detect

Detecting an attack is key to neutralizing the threat – and the quicker the better.

Detection covers a number of technologies. Tools like EDR/XDR (extended endpoint detection and response) and NGAV (next-gen anti-virus) monitor your computing systems looking for "indicators of compromise" (IoCs).

IoCs raise the suspicion that a piece of code could be malware. Other security tools like NDR (network detection and response) and UEBA (user and entity behavior analytics) monitor for activities on the network that fall outside of normal baselines.

The final part of the puzzle is detecting any connections that should not be allowed (e.g., direct access from the payments network to the Internet). Illumio will generate an alert if a threshold for non-allowed attempts is breached to detect lateral movement of a potential attack.

Segmenting the network is shown to improve the performance of EDR systems by restricting the spread of an attack, thereby reducing the area required for detection.

Respond

Once an attack is detected, you must respond instantly. As soon as an attack starts, it needs to be stopped. Zero Trust Segmentation supports this essential security capability.

Illumio's incident response segmentation can be built as a manual response or automated within various incident response security systems, including SOAR (security orchestration, automation and response) and SOC (security operation center) tools.

Once any system detects an attack, the workflow within a management system can automatically trigger a lock down of all the relevant ports and protocols that an attack would use. Alternatively, entire sections of the network can be isolated.

With Zero Trust Segmentation, you can effectively lock down ransomware and attacks to help maintain services while the malicious code is removed from your computing systems.

Your response process and configurations should be planned and tested for efficacy because any attack could be devastating with unknown consequences. Establishing a cyber resilience plan and practicing the response can make the difference between being able to maintain services and risking patient lives.

Recover

The last action is to recover services. If the attack is still underway, any premature repair work could create new risks.

With Zero Trust Segmentation, security and IT teams can set up protection around individual departments and systems, so they can resume operations, shielded from the attack.

Once the location of an attack is identified and contained, high-value systems like Internet banking or exchange-connected infrastructure can be released back to normal operation.

EDR systems will be able to track and recreate the path of the attack to identify weak points and vulnerabilities in your network. Using the Explorer feature in Illumio Core, you can quickly identify and block any connections using a given method of attack.

As part of recovering a network, Illumio can help to accelerate the process by several days since there is no need to build network-based separation between the bad, gray and clean networks.

German bank strengthens regulatory compliance

At Frankfurter Volksbank, IT leaders needed a way to comply with cybersecurity regulations from the German Federal Financial Supervisory Authority, as well as various requirements such as ISO 27001.

Regulatory compliance, and improvements to the bank's overall security posture, simply weren't possible with traditional, perimeter-based defenses. Illumio proved to be the ideal solution.

With Illumio, the bank gained complete network visibility and could easily isolate critical systems with host-based segmentation. Illumio's real-time application dependency map delivers vital insights into vulnerable pathways and workloads.

"With Illumio, we have made a significant leap to maximize security and minimize the risk of operational disruptions," says Steffen Nagel, head of IT. "Illumio has filled a gap for which there was previously no solution. In addition to meeting compliance regulations, we have seen drastic improvements in our overall security posture."

See the case study

Segmentation – a Closer Look

Segmentation defined

Segmentation is the practice of blocking off systems from other systems on the network using access controls enforced by the systems themselves or by other IT devices under the control of the security team. The goal of segmentation is to prevent lateral movement; that is, to prevent attackers who gain access to one system from moving freely to other systems as part of their attack.

Segmentation isolates systems. An attacker might gain access to a single endpoint – a laptop that they infect with ransomware, for example – but they won't be able to move laterally across the network to other systems and spread malware. This is because segmentation controls will block them, preventing access to specific network ports, IP addresses and protocols.

For example, many types of ransomware rely on Remote Desktop Protocol (RDP), originally designed to provide help desk agents with remote access to a system for troubleshooting. By blocking this protocol by default, segmentation can prevent many types of ransomware from spreading.

Even if attackers manage to infect a single endpoint, they'll find themselves trapped there, as though they had broken into a building but found themselves locked in the room they broke into.

With Illumio's real-time visibility and Zero Trust Segmentation controls, financial institutions can build the cybersecurity they need to safeguard customer data, protect against ransomware, and achieve regulatory compliance.

Network-Based Segmentation vs. Host-Based Segmentation

There are various ways of implementing segmentation. Some financial institutions try configuring their network switches and routers and perimeter firewalls to implement network segmentation controls, but that typically leads to two problems.

First, it's difficult to translate high-level policies into detailed networking rules on switches, routers and firewalls. For example, it's nearly impossible to create a practical networking rule based on a high-level policy that a web application should have network access only to the services it needs to perform its intended functions.

Inevitably, rules programmed into network gear end up being too strict or too lax. As a result, either application functionality or security resilience suffers.

The second problem is a lack of precision. With thousands or tens of thousands of endpoints on a network, it's difficult to enforce endpoint-specific controls from network gear and perimeter firewalls.

A better solution is to implement Zero Trust Segmentation on individual endpoints themselves. This approach takes advantage of the host-based firewalls built into endpoints such as laptops and servers. A host-based approach offers these advantages:

- **Direct, simplified control**
  It's easier to enforce security rules for endpoints like laptops on the endpoints themselves rather than on network devices like routers and firewalls. Network firewall rules are overly complex as it is without

trying to implement access controls that, for instance, differentiate a manager from a subordinate in a particular department.

- **Segmentation that works everywhere**
  Enforcing segmentation rules on endpoints themselves is much more practical now that so many employee endpoints are used in remote locations like home offices. If an employee isn't on an internal network, internal network devices can't enforce segmentation rules. Host-based segmentation enforces segmentation policies wherever an endpoint happens to be.
- **Pinpoint accuracy for rapidly isolating threats**
  Security teams can use an endpoint's host-based firewall to isolate the endpoint if they suspect it has been compromised. Because the firewall is on the endpoint itself, it isolates only the affected network, not the whole LAN or VLAN to which the endpoint is connected. Security teams don't have to risk misconfiguring firewalls as they rush to isolate an endpoint or, once an incident is resolved, to restore its connectivity.

Illumio compartmentalizes key asses and processes across a financial institution to provide finely grained protection from attack at the host level without re-engineering the network.

Learn More About Illumio for Banking and Financial Services

Cyberattacks on financial institutions are likely to increase across rapidly changing landscapes. Banking and financial services CISOs committed to best-in-class security are turning to Zero Trust Segmentation to maximize the cyber resilience of their institutions, helping protect customer and market data from sophisticated attackers.

To learn more about how Illumio can strengthen cybersecurity at your financial institution:

- Explore our products, including Illumio Core for workloads, Illumio Endpoint for user devices, and Illumio CloudSecure for cloud-native security.
- Schedule a demo and consultation with one of our healthcare security experts.
- Sign up for a virtual hands-on lab session.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.