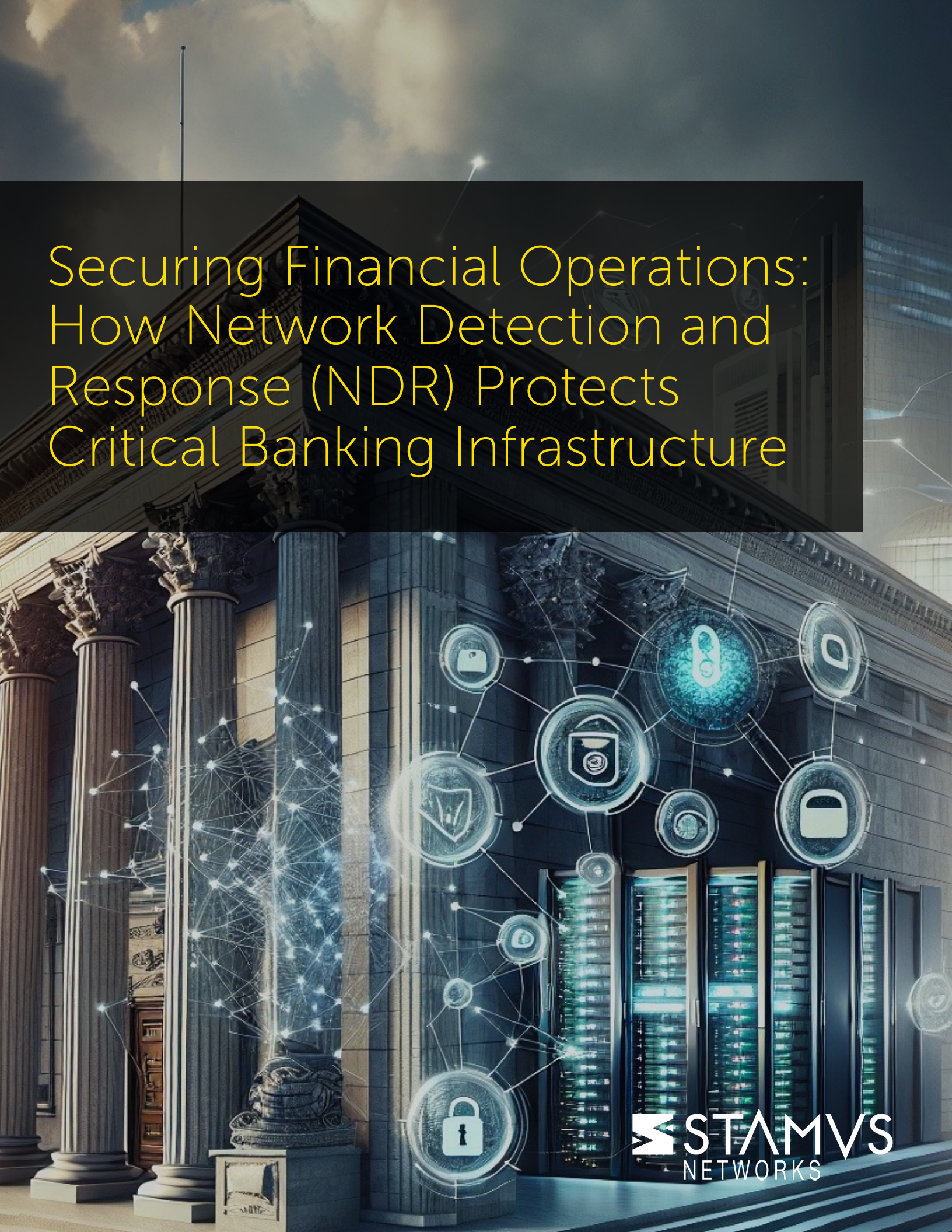
Securing Financial Operations: How Network Detection and Response (NDR) Protects Critical Banking Infrastructure



STAMUS NETWORKS

Abstract

This white paper brief explores the unique cybersecurity challenges faced by banks and financial institutions, and it outlines how network detection and response (NDR) technology is uniquely suited to deliver the sophisticated detection, monitoring, and response capabilities necessary to protect critical financial infrastructure while helping institutions meet stringent regulatory requirements.

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW

In the modern digital world, the cybersecurity threats we face have evolved. This is true across all industries and for every organization, but for financial institutions the consequences have also changed. What once might have been an isolated incident leading to a financial loss is now a systemic risk that can destabilize entire markets.

The International Monetary Fund's (IMF) "2024 Global Financial Stability Report" reveals a sobering reality: financial institutions are disproportionately targeted by cybercriminals, with attacks on financial services organizations accounting for one-fifth of all cyber incidents globally.

The impact of these attacks extends far beyond immediate financial losses, as demonstrated by the recent disruption of US Treasury market operations following a sophisticated cyber attack on the US arm of the Industrial and Commercial Bank of China (ICBC).

Top cybersecurity challenges facing banks and financial institutions:

Advanced threats and sophisticated attack vectors

Regulatory compliance

Insider threats

Third-party risk management

Operational resilience and business continuity

The financial sector's vulnerability to cyber threats continues to escalate. According to Sophos's "The State of Ransomware in Financial Services 2024", nearly two-thirds of financial services organizations fell victim to ransomware attacks last year, with average recovery costs reaching $2.58 million per incident. This trend is particularly concerning for large banks, where shared IT infrastructure and complex third-party relationships create single points of failure that could trigger sector-wide disruptions.

The stakes have never been higher. The IMF reports that financial institutions around the world have suffered direct losses of nearly $12 billion from cyber incidents since 2004, with over 20%

that amount occurring in just the last four years. More concerning still is their analysis suggesting that approximately once every decade, a cyber incident could result in losses equivalent to 800% of an average firm's operating income — a scenario that threatens both liquidity and solvency.

20% of cyber incidents target the financial sector*

In this increasingly complex threat environment, financial institutions require sophisticated defense mechanisms that can adapt to evolving challenges while maintaining operational resilience. Network Detection and Response (NDR) emerges in this case as a crucial component of any effective modern cybersecurity strategy, offering comprehensive visibility into network activities, advanced threat detection capabilities, and rapid response mechanisms that are essential for protecting financial operations and maintaining regulatory compliance.

For any financial institution seeking a Network Detection and Response solution with experience protecting the networks of leading global financial institutions and central banks, Clear NDR™ from Stamus Networks stands out as the NDR of choice. Offering high-fidelity threat declarations with correlated evidence, fully transparent multi-layer detections proven to catch the most sophisticated threats and zero-day attacks and automated response and reporting capabilities that support the requirements of major compliance regulations and cybersecurity frameworks, Clear NDR delivers detection financial institutions can trust with results they can explain.

65% of financial organizations experienced ransomware attacks in 2024*

$2.58 M

Average recovery cost of a ransomware incident, not including ransoms paid**

This white paper brief explores the unique cybersecurity challenges faced by banks and financial institutions, and it outlines how network detection and response (NDR) technology is uniquely suited to deliver the sophisticated detection, monitoring, and response capabilities necessary to protect critical financial infrastructure while helping institutions meet stringent regulatory requirements.

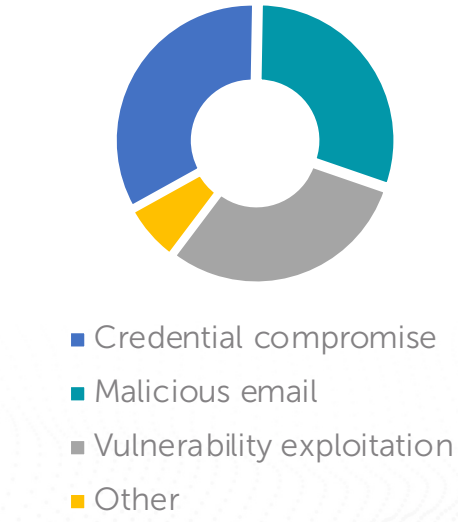
* "The State of Ransomware in Financial Services 2024", Sophos
** "2024 Global Financial Stability Report", International Monetary Fund

CHALLENGES FACING FINANCIAL INSTITUTIONS

Financial Institutions face an increasingly complex array of cybersecurity challenges that demand sophisticated detection and response capabilities. These challenges are amplified by the sector's critical role in global economic infrastructure and the vast amounts of sensitive financial data under their protection. There are 5 key cybersecurity challenges faced by financial institutions:

Advanced Threats and Sophisticated Attack Vectors

The financial sector has become a primary target for advanced persistent threats (APTs) and sophisticated cyber criminal groups such as LockBit, Conti, and Scattered Spider. According to Sophos's research, credential compromise has emerged as the leading attack vector, accounting for 30% of successful breaches in 2024. This is closely followed by malicious email campaigns and vulnerability exploitation, each responsible for 27% of attacks. The sophistication of these attacks is evidenced by the scale of their impact — when successful, ransomware attacks affect an average of 43% of computers within financial organizations..



Regulatory Compliance Requirements

Financial Institutions operate under an intricate web of regulatory frameworks and directives that mandate specific cybersecurity controls and reporting requirements. These include — but are not limited to — the Payment Card Industry Data Security Standard (PCI DSS), the EU's

Digital Operational Resiliency Act (DORA) and Network and Information Systems Directive 2 (NIS 2). Additionally, many financial services organizations opt to adhere to various national or international cybersecurity frameworks like the National Institute of Standards and Technology (NIST) cybersecurity Framework or the International Organization for Standardization (ISO) 27001 Framework.

Each regulation and framework brings its own set of requirements for monitoring, auditing, and incident response capabilities, creating a complex compliance landscape that demands comprehensive visibility into network activities and sophisticated reporting capabilities.

Compliance Examples

- PCI DSS
- NIST
- ISO 27001
- DORA
- NIS 2
- NCUA

Insider Threat Management

The privileged access that employees and contractors have to critical systems and sensitive data creates significant security challenges. Insider threats can manifest through both malicious and unintentional actions, making detection particularly difficult. The ability to identify anomalous behavior patterns and policy violations becomes crucial, especially given that internal actors often have legitimate access to the systems they might compromise.

Third-Party Risk Exposure

"More than 50 percent of IT providers of global systemically important banks supply their products and services to two or more global systemically important banks, implying a widespread overlap."

The IMF's 2024 Financial Stability Report highlights a critical vulnerability in the financial sector: The concentration of IT service providers. Major banks often share key technology suppliers, creating the potential for cascading failures across the industry. This interconnectedness means that a security breach at a single service provider could potentially impact multiple financial institutions simultaneously. The challenge extends beyond direct technology providers to include a complex web of contractors, partners, and financial market infrastructures, each representing a potential entry point for cyber threats.

Operational Resilience Imperatives

Financial institutions must maintain continuous operations while defending against cyber threats. The ICBC incident demonstrated how a successful cyber attack can disrupt critical market functions, affecting not just the targeted organization but the broader financial system. The challenge lies in maintaining robust security measures while ensuring those same measures don't impede business operations. Organizations must balance the need for comprehensive monitoring and rapid incident response with the requirement for uninterrupted service delivery.

HOW NDR ADDRESSES THESE CHALLENGES

Network Detection and Response technology provides financial institutions with comprehensive capabilities to address their most pressing cybersecurity challenges. By employing advanced analytics, machine learning, time-tested signature-based detection, and fully passive real-time threat monitoring, NDR solutions deliver the sophisticated protection required by highly-targeted financial services organizations.

NDR addresses the top cybersecurity challenges facing banks and financial institutions through:

- ✓ Comprehensive threat detection for advanced attack prevention
- ✓ Supporting regulatory compliance through robust logging and reporting
- ✓ Detecting and mitigating insider threats
- ✓ Strengthening operational resilience through automated response

Financial institutions can deploy NDR to effectively counter each of these major security challenges while maintaining operational efficiency. NDR's capabilities align directly with the financial sector's unique requirements for both security and continuous operation.

Comprehensive Threat Detection for Advanced Attack Prevention

Modern NDR solutions counter advanced threats through continuous analysis of network traffic, providing real-time detection of sophisticated attack patterns. Through the integration of multiple detection mechanisms, including signature matching, behavioral analysis, and machine learning algorithms, NDR technology can identify both known threats and novel attack patterns that might bypass more traditional network security measures.

The ability to analyze encrypted traffic without decryption is particularly crucial for financial institutions, where a significant portion of network traffic must remain encrypted for compliance purposes. Additionally, NDR's capacity to detect lateral movement within the network helps contain threats that breach the perimeter, addressing the challenge posed by credential-based attacks that Sophos identified as the leading attack vector in 2024.

Regulatory Compliance Through Robust Logging and Reporting

NDR strengthens compliance efforts by providing detailed documentation of network activities and security events. Most NDR platforms maintain comprehensive logs that capture network behavior, security incidents, and response actions, delivering the audit trail required by regulatory frameworks and directives such as DORA, NIS 2, PCI DSS, NIST, and ISO/IEC 27001.

Each security event is documented with correlated evidence, creating a clear chain of documentation that supports both compliance reporting and incident investigation. In the case of some NDR solutions, such as Clear NDR™, these reports can be automatically generated and escalated to necessary parties. This detailed record-keeping helps financial institutions demonstrate their security posture to regulators and auditors while providing valuable insights for continuous improvement of security measures.

Detecting and Mitigating Insider Threats

NDR's continuous monitoring capabilities provide a powerful tool for identifying suspicious internal activities and other anomalous behaviors. By establishing baseline patterns of normal network behavior, some NDR systems can flag anomalous actions that might indicate insider threats. This capability is enhanced through contextual, automatically escalating alerts that provide security teams with the information needed to distinguish between legitimate activities and potential threats.

Additionally, NDR's threat hunting capabilities enable security teams to proactively search for indicators of compromise. This is particularly valuable fort identifying organization-specific vulnerabilities that might be intentionally exploited by insiders with detailed knowledge of systems and procedures. In the case of Clear NDR™, users have the option of setting their custom organizational policies to receive automatic Declarations of Policy Violations (DoPVs).

These events are strong indications of breaches in internal policy, which could be a result of intentional malicious activity or unintentional practices that could leave the organization vulnerable to attack.

Strengthening Operational Resilience Through Automated Response

NDR strengthens operational resilience by enabling rapid detection and response to security events while maintaining continuous business operations. NDR's passive monitoring approach ensures that security measures don't disrupt critical financial operations. The same cannot be said of a more active monitoring system such an Endpoint Detection and Response (EDR), which required software agents to be deployed on every device within the organization. Passive monitoring on the network can address the dual requirements of security and availability.

While most NDR systems have limited response actions, they are often capable of integrating seamlessly with Security Orchestration, Automation, and Response (SOAR) platforms and EDR to automate response actions, effectively reducing the time between detection and containment or remediation. These types of integrations create a comprehensive and unified security ecosystem that can respond to threats while maintaining the operational continuity essential to financial institutions.

INTRODUCING CLEAR NDR™

Clear NDR™ from Stamus Networks delivers transparent, multi-layered network security that has proven its effectiveness in protecting some of the world's most critical financial infrastructure, including central banks and major insurance providers.


Financial Institutions


Central Banks


Government Institutions


Educational Institutions


Insurance Providers


Critical Infrastructure


Managed Service Providers


Government CERTs

Clear NDR's strength lies in its four fundamental capabilities that address the unique security needs of financial institutions:

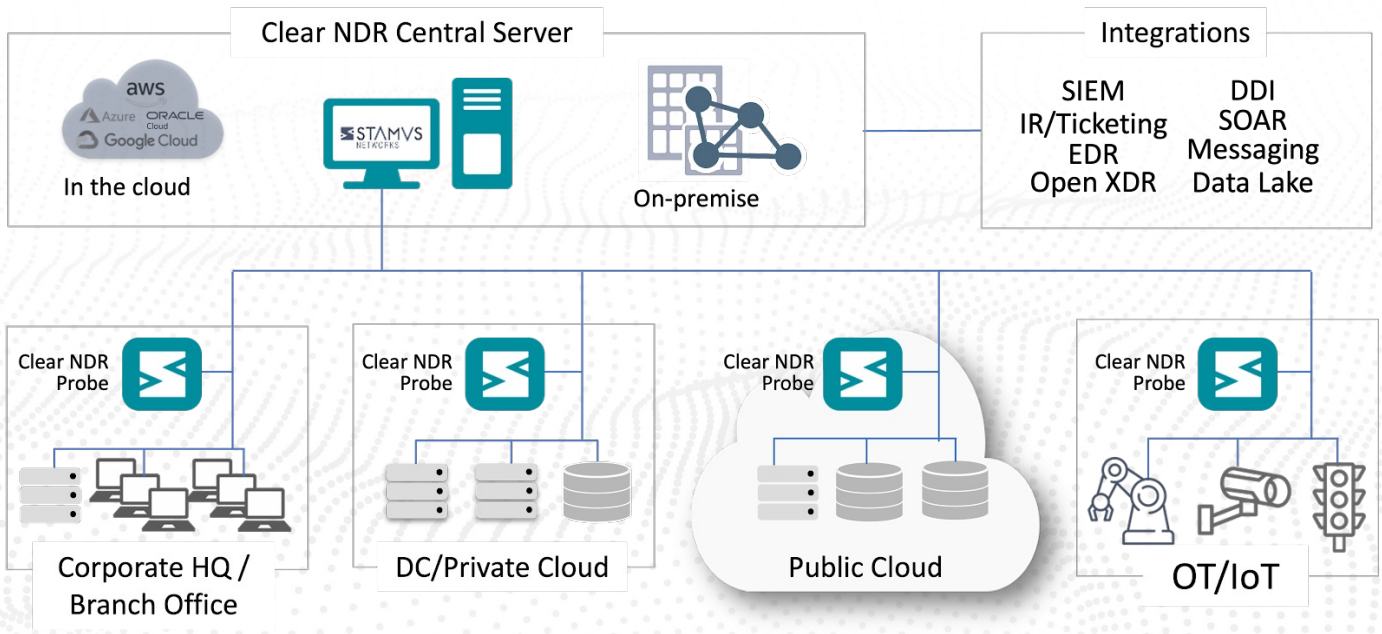
Clear Visibility – monitor activities across your entire attack surface — so you won't miss threats that evade your other controls

Clear Detection – multi-layer, transparent detections you can understand — so you can accelerate your triage and response

Clear Evidence – detailed attack timeline and complete evidentiary artifacts — so you can quickly resolve the incident

Clear Response – ultra high-fidelity threat declarations - so you have confidence you need to automate response

Implementation is streamlined through flexible deployment options — including cloud, on-premise, and hybrid environments — with immediate threat monitoring capabilities upon installation. Clear NDR complements and connects with existing security infrastructure through ready-to-deploy SOAR, XDR, and EDR platform integrations, ensuring that financial institutions can maintain operational continuity while enhancing their security posture



SECURING THE FUTURE OF FINANCIAL SERVICES

As cyber threats continue to evolve, and regulatory requirements become more stringent, financial institutions must adopt security solutions that provide both comprehensive protection and operational efficiency. The financial sector's unique position at the heart of global economic infrastructure demands security solutions that can adapt to emerging threats while maintaining the continuous operations the markets depend on.

Network Detection and Response technology has proven to be highly capable of meeting these challenges, providing the visibility, detection capabilities, and automated response mechanisms needed to protect critical financial systems. Clear NDR™ takes these capabilities further, delivering transparent, multi-layered protection that enables truly autonomous security operations.

The stakes have never been higher for financial institutions, with cyber incidents capable of causing billions in damages and disrupting critical market functions. Clear NDR provides the technology foundation needed to face these challenges, combining proven success in the financial sector with innovative capabilities that address both current and emerging threats.

- ✓ Cyber attacks cost financial institutions an average of $2.58M per incident, with threats becoming increasingly sophisticated and targeted.
- ✓ Financial institutions need comprehensive network visibility and automated threat detection to maintain operational resilience while meeting regulatory requirements.
- ✓ Clear NDR™ enables maximum visibility and comprehensive network security through advanced threat detection, automated response capabilities, and seamless integration.

Contact us today to learn how Clear NDR can enhance your institution's security posture while streamlining security operations. Our team of experts is ready to demonstrate how our platform can be tailored to your specific needs and integrated into your existing security infrastructure: contact@stamus-networks.com

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

