STAMVS NETWORKS

Penn National Insurance

Securing Sensitive Policyholder Data with Clear NDR™

Penn National Insurance, a medium-sized mutual casualty insurance company with approximately 850 employees, needed enhanced visibility into east-west network traffic to protect sensitive policyholder data and meet regulatory requirements.

After experiencing challenges with their previous solution following a vendor acquisition, they sought a more transparent, flexible network detection and response (NDR) solution that would work in their evolving infrastructure environment.

By implementing Clear NDR from Stamus Networks, Penn National Insurance gained comprehensive visibility into internal network traffic, strengthened their security posture, and improved their ability to detect potential threats before they could impact business operations.

SNAPSHOT

Organization type: Mutual Casualty Insurance

Location: Harrisburg, Pennsylvania USA

Organization size: 850 employees

Challenge: Protecting sensitive policyholder data in a highly regulated environment while managing relationships with vulnerable third-party partners, meeting stringent NYDFS compliance requirements, and undergoing significant infrastructure changes that exposed gaps in their ability to monitor internal network traffic

Solution: The insurance company deployed Clear NDR in their virtualization datacenter environment to to bring comprehensive visibility into their east-west network traffic.

Outcome: After implementing Clear NDR, Penn National Insurance been able to close several of their security and compliance gaps and has uncovered several cases of suspicious activity and policy violations.

> *Clear NDR gives us visibility into traffic to allow us to be proactive in monitoring and potentially avoiding a possible data breach or data exfiltration—some type of security incident that could possibly cost the organization in multiple ways, via financial loss or reputational damage. We view our security products and controls as insurance for the organization.*
>
> - **John Nagengast**, Senior Information Security Architect, Penn National Insurance

The Challenge: Protecting Sensitive Customer Data in a Highly Regulated Industry

As a mutual casualty insurance company specializing in homeowners, auto, and liability insurance, Penn National Insurance handles significant amounts of sensitive policyholder information, including claims data and medical records. The company frequently exchanges information with numerous smaller third-party organizations for claims handling, which creates unique security challenges.

"We deal with a lot of smaller third-party companies," explains Nagengast. "The problem is, many of these smaller companies probably don't have dedicated security teams. We've been seeing these companies become compromised, and then adversaries are sending emails to their contacts, including our users, from trusted sources," explains Mr. Nagengast

These sophisticated attacks leverage trusted relationships, making them particularly difficult to detect with traditional security tools.

Regulatory and Compliance Requirements

While not subject to PCI compliance requirements, Penn National Insurance must adhere to insurance industry regulations and the New York Department of Financial Services (NYDFS) Cybersecurity Regulation—one of the most stringent regulatory frameworks in the financial services sector.

"We comply with NYDFS," says Nagengast. "NYDFS is one of the toughest, most stringent regulatory and compliance frameworks. If you can meet NYDFS's criteria, you're probably going to meet just about everything else."

Infrastructure Evolution Driving Security Needs

Penn National Insurance was in the process of significant infrastructure changes, including:

1. Migration from one virtualized environment to another
2. Moving their primary data center
3. Establishing a new secondary data center at another physical location

Their existing NDR solution was becoming problematic due to deteriorating support and incompatibility with their future infrastructure plans. More critically, the company identified gaps in their security posture based on the NIST Cybersecurity Framework, particularly around detecting lateral movement within their network.

> "We could see our north-south traffic with our firewalls, but there was a lot of the internal traffic traversing the network that we really didn't have visibility into," Nagengast explains. "We were looking at a network detection and response solution to help with that."

The Solution: Why Clear NDR?

Selection Process

Penn National Insurance evaluated several NDR solutions before discovering Clear NDR by Stamus Networks through online research. Key selection criteria included:

1. Compatibility with their new virtualization environment
2. Flexibility to use virtualized probes rather than physical appliances
3. Price point appropriate for a medium-sized organization
4. Transparent detection methods and reporting
5. Strong customer support

"We tend to look for solutions that are very closely aligned to our use cases," notes Nagengast. "We look for solutions where we're going to be able to utilize most of the product’s capabilities. And Clear NDR was exactly that solution for us."

Implementation

Penn National Insurance deployed the Clear NDR solution with:

- The Clear NDR Central Server installed in the new virtualization environment
- Virtual probes initially deployed in older virtualization environment for testing, with successful transition to the new environment
- Mirror ports configured on their core switches to monitor the network traffic
- Two probes in each of their two data centers to ensure redundancy and comprehensive coverage

A key advantage of Clear NDR was its support for virtualization via both OVA files (for the older environment) and ISO images (for their new virtualization environment), enabling a smooth transition between environments.

> "We were able to deploy the ISO into our new virtualization environment, and it just worked. This ease of deployment was exactly what we needed," says Nagengast.

Direct Support Experience

One of the most significant differentiators for Penn National Insurance was the direct access to Stamus Networks' technical experts. "That's one thing I really like about Stamus Networks – I'm talking to the people," Nagengast emphasizes. "I've talked to the chief strategy officer and the vice president of customer solutions on many occasions – in fact, I had both on a call one time looking at our environment while a red teaming penetration test was being conducted. And when I put a support ticket in, it's always a very senior person who is answering it."

This direct connection with the people building and supporting the product was a stark contrast to their experience with their previous vendor after acquisition.

Results: Measurable Security Improvements

Enhanced Visibility and Transparency

Clear NDR provided Penn National Insurance with comprehensive visibility into their east-west network traffic, filling a critical gap in their security posture. The solution's transparency in detection methods significantly improved their ability to understand and validate alerts.

“I really like the built-in filter sets,” says Nagengast. “We can use the Stamus pre-defined filter sets to quickly determine things like ‘Is there any executable code present, or any C2 domain activity detected, instead of having to build that filter ourselves.”

Improved Threat Verification

The detailed evidence provided by Clear NDR enables the security team to quickly distinguish between true security threats and benign internal processes that trigger alerts.

This transparency is essential for efficient security operations in a lean security team.

> "With our previous NDR, it would flag – similar events as Clear NDR. But we had a hard time figuring out why or how they determined what was found," explains Nagengast. "With Clear NDR, we can look at the detection methods and really dig in to understand why the alert was triggered."

Uncovering Policy Violations and Vulnerabilities

Clear NDR has identified important policy violations and security gaps, such as:

- Unencrypted passwords being transmitted between internal systems
- Potentially vulnerable FTP jobs
- Corroboration of suspicious activities initially flagged by other security systems

"We have been able to uncover some unencrypted passwords traversing the internal network," notes Nagengast. "And I'd rather discover that type of traffic before somebody else does."

Correlation with Other Security Tools

Penn National Insurance has also found Clear NDR extremely valuable for correlating and confirming potential issues identified by other security tools, such as Microsoft Azure's threat detection.

"For email activity, we might get a third-party compromise email alert, one of our users clicks on the link, and we would see that same type of activity within Clear NDR too, possibly as a newly registered domain," explains Nagengast. “And the data captured by Clear NDR gives us a complete picture of what actually happened, and all the supporting evidence we need to resolve the issue.”

Insurance-Specific Benefits

Third-Party Risk Visibility

The insurance industry's reliance on numerous third-party partners creates unique security challenges. Clear NDR helps Penn National Insurance monitor network communications with these partners and detect suspicious activity that might indicate a compromised third party..

"Our users are always receiving emails from trusted sources – these clients or partners. For example, they may get an email they think is coming from a known contact at a local auto body shop in conjunction with a claim they are working. That message could contain malware or a link to a dangerous site if the contact’s email had been compromised. Clear NDR sees the communication with the website, and it can tell us if our user is accessing a newly registered domain and potentially executing a phishing campaign," explains Nagengast.

Protecting Sensitive Policyholder Data

With access to substantial amounts of personal and medical information through claims processing, Penn National Insurance must maintain strict data protection standards. Clear NDR provides an additional layer of defense by monitoring for potential data exfiltration attempts.

Supporting NYDFS Compliance

The detailed monitoring and reporting capabilities of Clear NDR help satisfy requirements of the NYDFS Cybersecurity Regulation, particularly around network monitoring, threat detection, and cybersecurity program effectiveness.

Return on Investment

Protection Against Costly Breaches

While difficult to quantify precisely, the early detection capabilities provided by Clear NDR represent significant protection against potential financial and reputational damage from data breaches.

"The Stamus Clear NDR solution gives us visibility into traffic that allows us to be proactive in monitoring and potentially avoiding a possible data breach or data exfiltration, some type of security incident that could cost the organization in multiple ways, via reputational damage and/or financial loss," states Nagengast.

Operational Efficiency

The predefined filter sets and transparent detection methods enable Penn National Insurance's small security team to work more efficiently, focusing their limited resources on the most critical issues.

Non-Disruptive Security

As a passive monitoring solution, Clear NDR provides security benefits without impacting business operations. "It's passive, it's not taking action on things necessarily. We're the ones that would have to take action on an incident. So, it gives us visibility without danger of disrupting operations and negatively impacting business," explains Nagengast.

Began Protecting Immediately

Clear NDR was very straightforward to deploy in the Penn National Insurance data centers and it began protecting their operations immediately. Nagengast said, “because it uses multiple detection technologies and doesn’t just rely on algorithms that require 30-60 days to train, Clear NDR had an immediate impact.”

Looking Forward

Penn National Insurance continues to evolve their security infrastructure alongside their changing IT environment. As they complete their data center migration and fully transition to Nutanix, they plan to leverage additional capabilities within Clear NDR.

The company is also exploring the built-in traffic visibility features of its virtualization environment, which could complement Clear NDR by providing additional insights into VM-to-VM communications within that environment.

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.

STAMVS NETWORKS

229 rue Saint-Honoré
75001
Paris, France

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

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