VECTRA
SECURITY THAT THINKS.

CASE STUDY

Nissho Electronics stops data breaches from enterprise to cloud

At Nissho Electronics Corp., making cutting-edge U.S. technology available to enterprise organizations in Japan is at the very heart of its mission.

Since 1985, Nissho Electronics Corp., a U.S. subsidiary of the Tokyo-based Sojitz Group, has helped Silicon Valley startups introduce their products and services to enterprise customers and markets in Japan.

“We partner and invest in early stage startups like Vectra that develop innovative new technologies and disruptive business models,” explains Hidenori Okumura, product manager of corroboration platforms at Nissho, which includes security products and services.

Three big challenges

According to Okumura, the company had growing concerns about its own network and cloud security posture due to rise in advanced cyberattacks. These hidden threats easily evade firewalls, IDS and other legacy security systems and spread inside networks in search of assets to steal.

> “There were too many logs to analyze.This has a negative impact on operational costs and time.”
>
> **Hidenori Okumura**
> *Product Manager of Corroboration Platforms*
> *Nissho Electronics Corp*

NISSHO ELECTRONICS

Organization

Nissho Electronics

Industry

Technology

Challenge

Needed early detection of threats, wanted to detect and respond faster to outside threats, and wanted to create audit reports about regulatory compliance and adherence to data-handling policies

Selection criteria

An AI-based network detection and response (NDR) solution that quickly identifies critical threats worth investigating and provides reporting

Results

- Dramatically reduced the time to detect and respond to alerts and improved the threat-hunting accuracy of their SOC team
- Can disclose information to members of their board as soon as possible
- Confidence that Vectra will detect the earliest signs of a cyberattack and prevent data breaches

“We had three major challenges,” he recalls. “First, we needed early detection of threats due to careless or intentional misuse by insiders. Second, we wanted to detect and respond faster to outside attacks. And third, we wanted to create audit reports about regulatory compliance and adherence to data-handling policies.”

Nissho had used its SIEM to analyze firewall logs, which was a manual, time-consuming operation.

“There were too many logs to analyze,” says Okumura. “It would take a long time to investigate every potential threat event because there was no way to tell if one represented a critical attack or anomalous user behavior. This has a negative impact on operational costs and time.”

Nissho was also concerned about the recent spike in credential abuse and account takeovers in SaaS-based Microsoft Office 365, which affects more than 30% of organizations each month. Attackers use social engineering to exploit human behavior, elevate account privileges and steal critical business-data.

The company understood that it needed visibility inside the network and public cloud to identify and stop hidden cyberattackers who move laterally in traffic to spy, spread and steal.

Solution: The Cognito™ NDR platform

To combat these response and cloud security challenges, Nissho became an early adopter of Cognito Detect™ from Vectra®.

Cognito Detect leverages AI to instantly identify and stop cyberattackers in cloud and data center workloads, SaaS offerings like Microsoft Office 365, and user and IoT devices.

“Vectra uses AI-derived machine learning to detect and respond faster to early attack behaviors before a breach happens,” says Okumura. “It also identifies anomalous behaviors. All detections are prioritized so you can quickly stop threats that pose the highest risk. This is why we chose Vectra.”

> “With Vectra we can disclose information to members of our board as soon as possible. We have also dramatically reduced the time to detect and respond to alerts and improved the threat-hunting accuracy of our SOC team.”
>
> **Hidenori Okumura**
> *Product Manager of Corroboration Platforms*
> *Nissho Electronics Corp*

By automating threat detections, prioritization, and other manual Tier-1 and Tier-2 security tasks, Cognito Detect significantly reduced the security operations workload at Nissho. And its compliance reporting capabilities ensure that top management is always up to date on business risk as it relates to cybersecurity.

“With Vectra we can disclose information to members of our board as soon as possible,” says Okumura. “We have also dramatically reduced the time to detect and respond to alerts and improved the threat-hunting accuracy of our SOC team.”

To speed up AI-assisted threat hunting and incident investigations, Cognito Detect collects relevant logs and metadata from all network traffic. The collected metadata is then enriched with deep security insights and detailed context about each attack, including all compromised users, accounts, devices, and whether the attack is part of a larger campaign.

Stopping data breaches in Office 365

In the SaaS world, Office 365 dominates the productivity space, with more than 250 million active users each month. It is the core of enterprise data sharing, storage, and communication, making it an incredibly rich data trove.

Consequently, Office 365 is now the focus of cyberattackers. Despite the increased adoption of multifactor authentication and other security controls, financial and reputational damage from Office 365 data breaches continue to mount.

Of those breaches, account takeover attacks are the fastest growing and most prevalent. A study by Forrester Research estimates the cost of account takeovers at $6.5 billion to $7 billion annually.

To stop these account takeovers, Nissho is planning to deploy Cognito Detect for Office 365 from Vectra, which ingests activity logs from multiple Office 365 SaaS services like Microsoft Azure Active Directory, Teams, Outlook, SharePoint, OneDrive, and Exchange.

With a thorough understanding of Office 365 application semantics, Cognito Detect for Office 365 applies AI-derived machine learning model to proactively detect and respond to hidden cyberattackers and stop data breaches in SaaS environments.

For more information please contact a service representative at info@vectra.ai.

To identify credential abuse and account takeovers, the machine learning models detect malicious behavior patterns in logins, file creation and manipulation, data loss protection configurations, and changes to mailbox routing configurations and automation.

Detections are correlated to user account privileges and prioritized based on risk, giving Nissho a comprehensive threat narrative to quickly respond and mitigate attacks and stop data breaches.

“Cognito for Office 365 is very important to us as well as to our own customers,” says Okumura, adding that Nissho recently switched from Google Workspace, formerly G Suite, to Microsoft Office 365.

“As a customer, investor and solution provider, we are confident that Vectra will continue as a market leader in NDR by allowing enterprise organizations to detect the earliest signs of a cyberattack and prevent data breaches,” he adds.

> “As a customer, investor and solution provider, we are confident that Vectra will continue as a market leader in NDR by allowing enterprise organizations to detect the earliest signs of a cyberattack and prevent data breaches.”
>
> **Hidenori Okumura**
> *Product Manager of Corroboration Platforms*
> *Nissho Electronics Corp*

Email info@vectra.ai vectra.ai