Customer
Case Study

Enhanced Security for LIA-ROC with VMware NSX Network Detection and Response

The LIA-ROC

In November 1998, the Taipei Life Insurance Association was restructured and promoted as a national-level association, later known as the Life Insurance Association of the Republic of China (LIA-ROC).

Industry

Financial Services

VMware footprint

VMware® NSX® Network Detection and Response™

The Life Insurance Association of the Republic of China (LIA-ROC) and 11 other insurance companies launched the pilot phase of the Protection/Claims Consortium Blockchain, a platform that enables the exchange of information. Due to this, it was critical to safeguard all the nodes in the blockchain from hackers. The LIA-ROC therefore introduced VMware NSX Network Detection and Response, which leverages its next-generation sandbox inspection technology to deliver the strongest line of defense for information security.

A one-stop, simplified application process

The LIA-ROC aims to use the Protection/Claims Consortium Blockchain for the Insurance Industry platform as a one-stop service. This benefits policyholders by simplifying the application process for claim settlement and personal data updates, and enables insurance companies to reduce operational costs for staffing and overlapping investments. The number of participating insurance companies is expected to grow from the current 11 to 18 following the official launch in 2021.

The LIA-ROC will also leverage the blockchain sharing platform to continue to promote its electronic policy authentication and evidence preservation mechanisms. Keeping records of policyholders' insurance policies and data change history can be used as proof to resolve disputes between policyholders and insurance companies.

> "The introduction of VMware NSX Network Detection and Response effectively resolves the problem of 'trust' in the blockchain sharing platform and successfully establishes robust defensive standards for information security, so that insurance companies are more confident participating in the consortium."
>
> Chung-Ho Wung, Insurtech Operational Sharing Platform Coordinator, LIA-ROC

Vital prevention against malicious attacks

As the Insurance Bureau specifically requires the LIA-ROC to maintain a Level A information security rating as an organizational standard, NSX Network Detection and Response is therefore vital as a gatekeeper to prevent the lateral movement of malicious attacks and to rigorously protect the security of file exchanges between systems.

In the selection of its sandbox inspection solution, the LIA-ROC studied international research reports and the MITRE ATT&CK information security framework, which is highly regarded by the global information security industry. The association found that NSX Network Detection and Response is not only recommended by Gartner, NSS Labs and other organizations but is also in line with various MITRE ATT&CK strategies, making it the top choice.

The LIA-ROC expected to face numerous challenges in the implementation process, including a tight project timeline and high system integration complexity. However, with NSX Network Detection and Response's comprehensive API mechanisms and ready-made Sample Code, LIA-ROC was able to construct a highly flexible deployment framework to implement seamless integration of the sharing platform with all insurance companies' systems in the shortest timeframe.

Zero impact on processing efficiency despite data volume spikes

The volume of documents exchanged during the current pilot phase is modest, but once the platform is officially operational, surges are expected as the number of applications grows. Quickly performing inspections and making accurate decisions without impacting processing efficiency will become a significant challenge. Knowing that a large national experimental research organization has already adopted NSX Network Detection and Response to handle heavy data traffic with ease, the LIA-ROC is highly confident in its ability to support data volume spikes.

"The introduction of VMware NSX Network Detection and Response effectively resolves the problem of trust in the blockchain sharing platform and successfully establishes robust defensive standards for information security, so that insurance companies are more confident participating in the consortium," says Chung-Ho Wung, Insurtech operational sharing platform coordinator, LIA-ROC.

Fighting AI with AI

To prevent hackers from exploiting the document exchange process for malware attacks, the LIA-ROC is committed to the use of Zero Trust architecture, like the approach in entry-exit security screening. This ensures that any file that leaves its original source and enters a new system is subject to NSX Network Detection and Response full-system emulation sandbox inspection, so only safe data files are released.

The full-system emulation feature in NSX Network Detection and Response creates a virtual environment that simulates CPU, memory configurations and even fabricates user trails. This tricks malware into interacting with this environment so that its activity can be recorded and analyzed, and the threat neutralized. As a result, no malware has made a successful intrusion into the consortium blockchain in more than three months of pilot operations.

Hackers today are increasingly exploiting the power of AI to come up with new attacks that are constantly mutating to evade detection. Fortunately, the NSX Network Detection and Response next-generation sandbox integrates AI and ML technologies to gain in-depth insight into the potential connectivity behavior of all programs and dynamically analyzes exploits. By fighting AI with AI, it not only detects modified attack techniques but also returns feedback to the consortium blockchain's defense mechanisms.

Future seamless cooperation with VMware NSX Network Detection and Response

Moving forward, LIA-ROC plans to establish a centralized resource pool to support flexible scheduling and user payments. To achieve this, it may need multiple VMware products, such as VMware vSphere® virtualization platform, VMware vSAN™ Software-Defined Storage platform, VMware NSX virtual firewall and micro-segmentation technology, and VMware Carbon Black™ endpoint protection system. NSX Network Detection and Response is able to seamlessly interface and smoothly cooperate with these systems, ensuring that LIA-ROC is set up for success in the future.