At a glance

Industry

- Securities

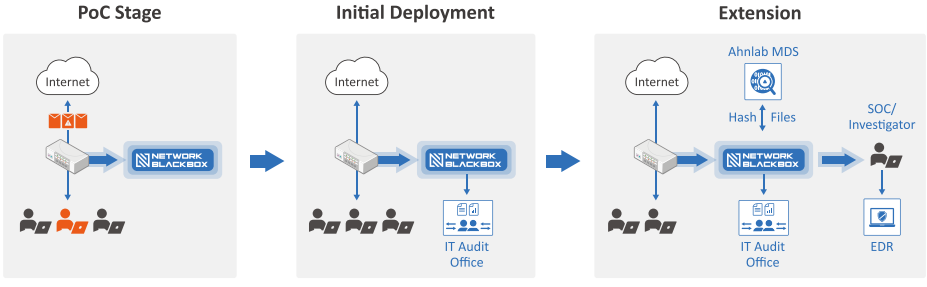
Challenge

- The exchange of information among analysts is in various ways (Cloud, Web Mail etc.) making it difficult to track and secure
- Identifying Users Using Cloud Storage

Outcome

- Reduced IT audit activity blind spots in Shadow IT environments
- Real-time response system to malicious file infection and internal information leakage through the Internet
- Ability to detect unauthorized content usage and audit policy violations
- Reduced incident response times

Case of detecting the personal information leakage through PoC



In today's fast-paced business environment, the threat of cyber-attacks is ever-present, and the financial industry is particularly vulnerable to these attacks. Recently, a securities company discovered a personal information leakage through PoC, which highlighted the need for a comprehensive security solution to protect against advanced cyber threats. The company realized that traditional security solutions were not enough to detect and prevent these types of attacks, and they turned to Quad Miners for a solution. The securities industry is a highly regulated and competitive market, and security is of utmost importance to protect sensitive financial data and maintain the trust of clients. The national No. 1 securities firm recognized the need for a comprehensive security solution to safeguard against cyber threats and maintain the confidentiality of customer data.

Quad Miners' Network Detection and Response (NDR) solution was implemented to address the company's security challenges, including the detection of personal information leakage through Proof of Concept (PoC) attacks. The company recognized the importance of a solution that could detect advanced persistent threats (APTs) and respond to them quickly to minimize the risk of data breaches and financial loss.

In addition to addressing the company's immediate security concerns, Quad Miners' NDR solution Network BlackBox also provided the company with the flexibility to expand its operations by integrating APT solutions. This integration allowed the company to enhance its security posture and stay ahead of emerging threats.

In this case study, we will examine how Network BlackBox helped the securities company to detect and respond to personal information leakage through PoC attacks, as well as how the company expanded its security operations through APT solution integration. We will explore the benefits of the NDR solution and how it helped the company achieve a more secure and resilient infrastructure.

Background

Due to the nature of analysts' work, it is necessary to ensure safe internet use to analyze company fundamentals. In addition, the securities firm had a shadow IT work environment where analysts used separate applications without sanction from the company for work efficiency. This posed a significant security risk, as these applications could be used to exfiltrate sensitive data or introduce malware into the network.

To address these challenges, the securities firm had implemented security policies for shadow IT work environments. However, they still experienced blind spots in their security defenses due to limited application support with security policies. Additionally, the firm had DLP (Data Loss Prevention) solutions in place, but these solutions had limited application support, leading to further blind spots and security vulnerabilities.

Network BlackBox was implemented to address these challenges and provide the securities firm with a comprehensive security platform. The NDR solution offered complete visibility into network traffic, allowing the firm to detect and respond to advanced cyber threats, including those posed by shadow IT applications. The solution also provided the flexibility to expand its security policies to include more applications and devices, minimizing the blind spots and security vulnerabilities.

Challenge

In the securities industry, the exchange of information among analysts is crucial for making informed investment decisions. However, this exchange of information occurs in various ways, including cloud-based applications, web mail, and SaaS file exchange, making it difficult to track and secure. This poses a significant challenge for the security team, as they must identify information about apps and content in use internally to minimize the risk of data loss or theft.

Furthermore, identifying users who are using cloud storage adds another layer of complexity to the security challenge. The securities firm operates DLP solutions, but these solutions have limited application support with security policies, leading to blind spots in the security defenses. The lack of application support makes it challenging to monitor and secure data flowing through cloud-based applications, creating a significant security risk.

Another challenge faced by the securities firm is the delayed follow-up response from the IT Audit Office. As a result, security incidents may not be addressed in a timely manner, leading to further security vulnerabilities and risks.

Solution

Network BlackBox provided the securities firm with a comprehensive security platform to address their challenges. The following features of the solution helped the firm enhance their security posture:

Quad Miners' Application Parser was the only competitive Proof of Concept (PoC) solution to detect information leakage, beating out competitors such as RSA and Darktrace. This feature allowed the firm to identify sensitive data that was being transferred through various channels, including shadow IT applications.

Quad Miners' Network Blackbox offered complete visibility into network traffic, allowing the firm to detect and respond to advanced cyber threats in real-time. The Network Blackbox was integrated with a file dynamic analysis system, Ahnlab MDS, to check all files between internet transactions. This integration allowed the firm to respond quickly to potential threats by using Endpoint Detection and Response (EDR) in integration with the SOC system.

The Network Blackbox also helped the firm monitor network traffic to determine who was using unauthorized cloud storage. This allowed the firm to identify employees who were using non-sanctioned applications and take appropriate action to mitigate security risks.

Outcome

After implementing Network BlackBox , the securities company saw significant improvements in their security posture. The provision of an Application Parser, which is only available in competitive PoCs like RSA and Darktrace, enabled the detection of information leakage that was previously overlooked. Network Blackbox also integrated with a file dynamic analysis system, AhnLab MDS, to check all files between Internet transactions and respond in real-time through EDR integration with the SOC system. This allowed the company to establish a real-time response system to malicious file infection and internal information leakage through the Internet.

Additionally, the NDR solution enabled the monitoring of network traffic through Network Blackbox to determine who used unauthorized cloud storage. This provided the ability to detect unauthorized content usage and audit policy violations through Internet network full packet collection, reducing IT audit activity blind spots in Shadow IT environments. Furthermore, the visibility into the whole network traffic provided by the solution enabled the company to reduce incident response times, achieving a more efficient and effective response to security incidents. Overall, Network Black Box helped the securities company achieve a more comprehensive and effective security platform to protect against cyber threats and maintain the confidentiality of customer data.

Summary

In this case study, Quad Miners provided an NDR solution to a national No. 1 securities firm that faced challenges with blind spots in their security defenses due to a shadow IT work environment and limited application support with security policies. The NDR solution offered complete visibility into network traffic, enabling the firm to detect and respond to advanced cyber threats and minimize blind spots and security vulnerabilities. As a result, the firm was able to reduce IT audit activity blind spots, establish a real-time response system to malicious file infection and internal information leakage, and achieve visibility into the whole network traffic to reduce incident response times.

Why do Security Companies need NDR solution?

Securities companies deal with sensitive financial data and are subject to strict regulations, making them attractive targets for cyber attackers. A Network Detection and Response (NDR) solution provides a comprehensive security platform that allows securities companies to detect and respond to advanced cyber threats, including those posed by shadow IT applications. By implementing an NDR solution, securities companies can maintain the confidentiality of customer data, reduce the risk of security breaches, and comply with regulatory requirements.