LAW ENFORCEMENT CASE STUDY

Police Department verifies ransomware did not exfiltrate data

Alarms alerted IT staff at a Police Department that all access to key servers had been blocked. They had been hit by a Ransomware attack with command and control on their most critical servers. The immediate response was to shut down Internet access to the network and place servers in an offline state to prevent any further access by the attacker. Of critical concern during and after an attack is determining if private data has been exfiltrated and identify servers that have been infected with the Ransomware exploit just waiting to be executed. The cost of credit monitoring and fines for data exfiltration are hefty.

Fortunately, HOPZERO's visibility security product had been actively watching the network and recording every communication in or out of the network for months. The Recorder Auditor visibility solution creates a detailed permanent real time record of every session created between every node on their network to each other and everywhere in the world. The Recorder Auditor was the key security tool used to identify the attacker and verify the extent and depth of the attack.

"Recorder Auditor verified that there was no exfiltration of private data"

The Recorder Auditor facilitated the customer with the information to identify the IP address and deep security information of the attacker including every instance where they achieved access to the server. This detailed information immediately showed the criminals originated their attack from international locations that the Police Department never needed to connect to. The powerful visual of seeing and attack surface map, quickly identified the cyber-attack location as unsafe or untrusted communications outside of the company and the country. Many organizations have logs, but until it is visualized it's hidden in cryptic logs that only security analysts can decipher. HOPZERO offers a tool to easily view cyber attacker activity and generate reports that are usable to most IT and security engineers.

Analysis of the ransomware event definitively showed that there was no exfiltration of private data attempted or completed. The Recorder Auditor equipped the IT staff with evidence logs from the Compliance and Smart Logging archive that exempted them from penalties associated with loss of private data. The required breach report was filed but penalties were not incurred because the evidence proved that no data loss was achieved. This also exempted our customer from the more onerous consumer breach notifications that would have been required had data loss occurred.

Recorder with SaaS Auditor is purchased as a bundle. Get real time graphic GeoIP maps showing your attack surface. Easily export data to create custom reports.

The Recorder Auditor had been capturing all communications sessions for months before the attack and storing them offsite in the customer's private Portal. HOPZERO does not have any access to a customer's data, but only records the who, what, when, where, and why for all data accessed on each device.

This is what made it possible to investigate and confirm the integrity of private data on the server. This archive design intelligently parses down sessions to make them lightweight and optimized for storing many years in a small amount of storage. It ensures that every session between servers and destinations are available to perform forensic investigation from past months or years. Investigation filters can be applied to the archive to quickly spot suspicious activity including exfiltration of data from internal servers to both internal and external endpoints. Recorders collect session information on source IP, destination IP, dates, time, payload size, protocols, ports, and over 40 other data points, statistics, performance metrics and risk factors.

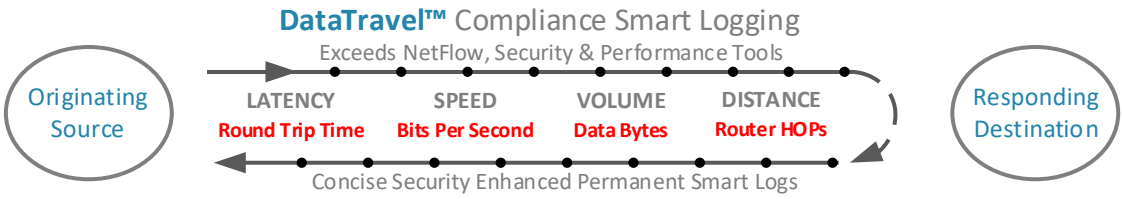
The customer's next step is to install the HOPZERO containment solution that stops server compromise. This advanced patented enforcement security layer prevents command and control exploits used in Ransomware exploits.

"HOPZERO saved us from having to pay millions in fines, notifications and credit monitoring by definitively proving that no data was lost" ~Security Manager

The HOPZERO Recorder is a subscription-based security solution and includes our SaaS Auditor. It provides unattended real-time collection of every session between all hosts and archives the information to meet compliance logging standards. The Recorder monitors the network and traps alarms to identify exfiltration or command and control attempts. Alarms are displayed on the SaaS Portal Alarms page and can be configured to send the same alarms to a central security console in the SOC. The Portal Investigation page displays a global map view of every session pair which enables rapid understanding of where data is being exchanged. The Investigation map represents the current attack surface as an interactive graphic extracted from millions of real time and archived sessions.

"Smart logging with optimized archiving ensures multi-year Compliance"

The HOPZERO Recorder logs every communication session and meets compliance requirements for NIST, GDPR, HIPAA, PCI, DoD, security standards. Concise logs add security research enhancements, building smart logs to include the Who, What, When, Where and Why. Smart logging with optimized archiving ensures multi-year Compliance is available for audits. The Recorder Auditor uses machine learning to calculate speed, distance, latency, and volume combined with threat intelligence lookups, risk scores, and over 40 different metrics to help manage risk and network performance. DataTravel™ compliance logs can be exported to Excel, Splunk, LogZilla or Elasticsearch. The Recorder monitors the network for actionable alarms on any attempt to exfiltrate data from vital servers or exploits to gain command and control from outside the "Sphere of Trust™".



Recorders only collect session meta-data from IP headers. All information is archived to a customer's private portal. Collected data is encrypted during transit and while at rest. Recorder Auditor can be used to reveal potential exfiltration risk and actual data leaks and to validate the effectiveness of the organization remediation efforts.

Learn more about Compliance Visibility at: https://hopzero.com/police

HOPZERO
11400 Concordia University Dr.
Austin, TX 78726
833-467-9376

inquire@hopzero.com

About HOPZERO

HOPZERO is an Exfiltration Prevention solutions developer. Audits and proactive security solutions allow companies to protect their private data. HOPZERO products are managed with a unified SaaS management platform providing enterprise wide visibility and safe data containment policy enforcement. HOPZERO security systems eliminate complexity and the training gaps normally associated with enterprise data security systems.