Advanced Network Security for the Modern Enterprise.

Powered by Vehere AI Network Security

vehere

HUNT BEFORE BREACH™

Cyber security breaches are becoming common.

Rising faster. Breaching sensitive data.
Those needing to protect need to extend
beyond traditional tools.

GLOBAL SCENARIO

5.55

Billion accounts breached in 2024.

3

USD trillion – Damage caused by cybercrimes worldwide, 2015.

9.5

USD trillion – estimated damage caused by cybercrimes worldwide, 2024.

~3,000

Cyberattacks recorded in the Middle-Eastern region, 2024.

(*Source: Surfshark, Secure Works* | *05.11.24*, *CybelAngel* | *06.01.25*)

3,207

₹ crore funds lost due to cyber-fraud in India between FY 19-20 to FY 23-24.

5.82

lakh – Number of cyber fraud cases reported in India from FY 19-20 to FY 23-24.

2.93

lakh – Cyber fraud cases reported in India in FY 23-24 (₹2,054.6 crore lost).

98

Ransomware attacks reported in India in 2024.

(*Source: The Hindu* | *13.11.24, Indian Express* | *04.01.25, PIB* | *20.09.24*)

Legacy defenses have blind spots.

Competence lies in modern technology.

Proactive defense. Effective deployment.

So that network traffic deviations can be addressed with speed.

Counter breach attempts before they unfold.

Something revolutionary has emerged to safeguard networks.

An effective line of defense.

This is what Vehere is purpose built for.

Proactive cybersecurity for financial institutions.

Challenges

Today's advanced attacks can attack anyone, move anywhere, and disrupt anything.

Vehere AI Network Security monitors your entire network for threats.

Unlike others service providers who focus on end-points and perimeters.

Solutions

#1 Safeguard financial institutions from cyber threats through proactive detection and response.

Help cyber analysts proactively assess cybersecurity postures and detect malicious behaviour without interrupting business processes.

#2 Stop threats proactively to minimize potential losses and account takeovers.

Analyze attacker behaviour across the entire network, with more than 90% of MITRE ATT&CK techniques covered.

#3 Reduce noise alert.

Reduce the alert noise by nearly 85% with machine learning that understands your network, eliminating false positives and focusing on real attacks.

#4 Identify and score threats.

Proactively identify over 3x threats by automation to correlate, score and rank incidents by their severity.

Who we are.
What we do.

Vehere was established in 2006, positioned as a new-age Cyber Defense software company.

Vehere specializes in AI-powered Cyber Network intelligence with the objective to lead the field with innovative security solutions.

Vehere's cyber defense software is battle-tested by the world's toughest defense and intelligence agencies.

Vehere has been supporting counter-terrorism analysts of the defense and intelligence sector for more than a decade.

Vehere is trusted by Fortune 500 companies (Telecom, BFSI, Smart Cities) to protect their critical infrastructure from cyber threats in real-time.

10 key elements that make Vehere the ideal choice.

01

Comprehensive network visibility

Captures Flow and Raw Network Traffic Packets for an in-depth analysis of every data packet.

02

Advanced threat detection

Ensures the swift detection, compliance and protection of sensitive data while maintaining customer trust.

03

Proactive threat hunting

Delivers threat hunting at scale with upto 2 million IoCs, detecting botnets, malicious domains and missed indicators.

04

Extensive protocol analysis

Offers an extensive protocol coverage (5000+) and application-layer protocol analysis.

05

Strong identity and access management

Offers solutions with two-factor authentication to protect accounts and limit access to sensitive data.

06

Network segmentation

Device categorization through asset registers to classify devices and effectively enforce granular security policies.

07

Detecting concealed threats in encrypted traffic

Secure authentication frameworks like Kerberos and LDAP for controlled access to encryption keys and credential management to prevent unauthorized decryption. Safeguards PII, SPI and PCI data from potential breaches.

08

Historical data for forensic analysis

Provides solutions that capture all network traffic without degradation for seamless live and historical analysis.

09

Successful integration with existing systems

Seamless integration with existing tools such as SIEM, SOAR and ticketing systems for smarter threat detection and incident response.

10

Zero-day detection

Utilizes sandbox technology to detect Zero-Day malware, which exploits vulnerabilities before they are patched to analyze their behaviour without compromising critical systems.

What Vehere offers.

Network Detection and Response

Flow and raw network traffic: We enhance our client's network security and performance through advanced monitoring solutions that provide 100% visibility of the network traffic. With flow and raw network traffic packet (PCAP), our solution provides valuable insights into client network performance, usage and security.

Next-gen Sandbox

Zero Day Malware Detection:
Our next-gen Sandbox Technology is designed to detect zero-day malware and previously unknown threats, exploiting vulnerabilities before they are patched.

Threat Hunting

Artificial Intelligence and Machine Learning: Our innovative AI and ML solutions address the growing threat landscape. Our ML DNS Analytics harness advanced machine learning algorithms to analyze DNS traffic, identifying anomalies and threats in real-time.

UltraHunt 2mn IOCs: With the help of our advanced technology, two million indicators of compromise (IOCs) can be processed at line rate, which smoothly integrates large amounts of threat intelligence into the client's security operations.

Retrospective detection: Our retrospective rule detection capabilities permit security teams to sift historical data, identifying IOCs previously missed.

Network Forensics

Indexed-raw: The patent-pending indexed-raw technique allows for the quick retrieval of packets, guaranteeing the accessibility of critical information when needed.

Full digital forensics: We offer lossless network traffic capture, a critical capability for our clients, ensuring that no essential evidence is lost during data collection.

Intrusion Detection System

E-W and N-S: Whether the traffic is monitored East-West (E-W) or North-South (N-S), our behavior-based protocol detection capabilities provide a proactive identification of irregularities, permitting our clients to secure their network and optimize performance.

A quick glance

Feature	Traditional tools	Vehere AI Network Security
Detection technique	Rule-based	Behaviour-based Signature-based ML
False positives	High	Minimal
Zero-day detection	Limited	Sandbox-enabled
Visibility	Partial	100%

BIG NUMBERS THAT DEFINE US

2+
Million, indicators of compromise

85%
Reduction in alert noise that understands your network

90%
Of blind spots eliminated

CUSTOMER STORY

Helping a financial powerhouse strengthen its network security.

Overview

A prominent nationalized bank with headquarters in the APAC region grew profits at an annualized 55% in the fourth year of FY 23-24.

The bank's total business was ₹4,66,000 crore during that year.

The bank maintained a high Provision Coverage Ratio, while reducing Gross Non-Performing Assets (GNPA) and Net Non-Performing Assets (NNPA).

This bank comprises an employee strength of 20,000+ and firm size of USD 30 billion.

It engaged Vehere for its advanced AI Network Security solution to protect against cyberattacks.

WHY THE BANK CHOSE VEHERE

For its innovation commitment

For internal/operational efficiencies

For enhancing business process outcomes

For improving compliance and risk management

For identifying and detecting threats

How Vehere addressed the challenges

Challenge #1

The bank was exposed to sophisticated cyberattacks (phishing, ransomware, and insider threats) that could have jeopardized financial stability and customer fund security.

Solution

Vehere detected and mitigated sophisticated phishing attacks and internal data exfiltration attempts.

Vehere analyzed the network traffic and identified suspicious activities.

Vehere engaged in early detection through anomaly detection, intrusion alerts and malware detection from unknown user agents.

Challenge #2

Legacy systems with outdated security patches and limited visibility into encrypted traffic exposed the bank to cyberattacks; attackers exploited known vulnerabilities to access sensitive data.

Solution

Vehere achieved a real-time visibility into all network traffic, including encrypted communications. Vehere used JA3 fingerprinting and loss-less full-packet technology. This helped analyze every data packet passing through the network.

Challenge #3

Security incidents had earlier disrupted the bank's network, leading to availability issues and operational reliability.

Solution

Vehere improved response time by analyzing packet content; it identified more than 5,000 protocols and offered a complete communication perspective between devices and the detection of potential anomalies.

Vehere ensured timely system protection through robust incident-response technologies.

Vehere's Network Forensic helped detect, analyze, contain, eradicate and recover stages; this enabled swift remediation to prevent lateral movement and data exfiltration.

Vehere's winning formula

Prudent vendor support

Customizing the detection rules

In-built detection by static rules and ML detection capabilities

WHAT OUR CUSTOMER HAS TO SAY

"The overall experience with the vehere product was satisfactory, with good support from the technical and support teams. They were prudent to adapt and customize the product as per any requirement."

– Manager, IT Security and Risk Management

CUSTOMER STORY

Helping a co-operative bank become more secure, efficient and reliable.

Overview

A prominent bank (established in 2015) started with 16 co-operative societies and 69 individuals as members.

The bank's aim is to become a universal bank in the co-operative sector with a network across States and overseas. It offers an array of financial services to every customer segment under one roof with professionalism and social commitment.

This leading Indian financial institution (employee strength 4,000+ with a reported profit after tax of ₹209 crore in FY 23-24) turned to Vehere to reinforce its network.

The challenges faced and how Vehere addressed them

Challenge #1

Before adopting the Vehere AI Network Security solution, the bank lacked a complete visibility into network traffic, making it difficult to distinguish between normal and abnormal behaviors.

This absence of continuous monitoring hindered timely threat detection and response.

Solution

With the help of Vehere, the bank gained a real-time visibility into all network traffic, including encrypted communications, using JA3 fingerprinting.

Our lossless full-packet technology ensures complete capture and in-depth analysis of every data packet across the network.

Challenge #2

Traditional monitoring systems overwhelmed the bank with false positives, generating alerts that did not reflect real threats.

This led to alert fatigue and an inefficient allocation of resources, undermining security efficiency.

Solution

Reduced false positives using advanced machine learning algorithms, contextual analysis, customizable thresholds and continuous monitoring.

This enhanced the differentiation between normal and anomalous behaviour, improving the efficiency and accuracy of security operations.

Challenge #3

The bank's security tools reliant on pre-defined signatures failed to detect novel or zero-day attacks.

The bank required a proactive solution capable of real-time network behaviour analysis to identify and mitigate emerging threats effectively.

Solution

Enabled detection of zero-day malware—unknown threats exploiting unpatched vulnerabilities—using next-gen Sandbox Technology.

Suspicious files are isolated and analyzed in a controlled environment, ensuring that the main systems remain secure.

Advanced behavioural analytics further detect and neutralize sophisticated threats within the network.

Challenge #4

Configuring traditional security tools was complex and time-intensive, demanding specialized expertise.

Without a dedicated security operations team, the bank struggled to optimize these systems, weakening its security posture.

Solution

Centralized management and the monitoring of diverse IT infrastructure enhanced visibility, secured sensitive financial data and ensured operational resilience.

The proactive approach minimized downtime, improved efficiency, and supported smooth operational continuity.

WHY THE BANK CHOSE VEHERE

Cost management

Enhancing internal/ operational efficiencies

Improving business process outcomes

Improving compliance and risk management

Vehere's winning formula
Product functionality and performance
Product roadmap and future vision
Strong customer focus

WHAT THE GLOBAL SECURITY LEADER HAD TO SAY

"We are using Vehere NDR for one of our banking customers. The product has enhanced features to identify anomalies across the network with the help of AI/ML-based policy fine-tuning."

CUSTOMER STORY

Vehere NS enhanced network security and management robustness at a major financial institution.

Overview

One of India's largest commercial banks catered to millions of customers across the nation and the world. As of December 31, 2024, the Bank had a customer base of nearly 50 crore and over 64,000+ ATMs.

The bank comprised a global network of 22,405 branches in India and 233 overseas offices in 36 nations.

The bank offers holistic financial services – retail banking, corporate banking, investment banking and international banking.

The Bank's mission is to remain one of India's most respected financial institutions.

WHY THE BANK CHOSE VEHERE

Enabled a comprehensive analysis and forensic investigation

Assisted in threat identification

Helped detect malicious content

Identified and responded in advance to threats

Facilitated systemic automation

Empowered through data-driven decision making

Ensured a complete compliance with regulations such as GDPR and DLP

Facilitated timely incident responsiveness

The challenges faced and how Vehere addressed them

Challenge #1
Skill gaps and expertise shortages

There was a lack of expertise in the management of complex network environments.

Solution

An intuitive platform with automated tools was provided to simplify network management.

Challenge #2
Network visibility issues

There was a difficulty in tracking IP addresses and analyzing encrypted traffic.

Solution

Deep packet inspection and detection of non-standard traffic emerged.

Challenge #3
Complex rule creation

Challenges were encountered in setting precise rules to detect threats.

Solution

Vehere introduced customizable rule sets, aligned with business needs.

Challenge #4
High costs and inefficiency

There were rising costs and time involved in maintaining network solutions.

Solution

Vehere helped streamline operations through automation and AI.

Challenge #5
Data privacy and security

There was a difficulty in identifying and masking sensitive data.

Solution

Vehere implemented PII masking and strengthened compliance.

Challenge #6
Inefficient threat detection

There was an inability to detect advanced threats.

Solution

Vehere enhanced anomaly detection using AI and ML models.

Challenge #7
Limited forensic analysis

There was an inability to extract and analyze detailed network traffic data.

Solution

Vehere's detailed packet-level analysis provided better insights.

Challenge #8
Poor alert management

There was a lack of context and delayed notifications for security events.

Solution

Vehere improved alert accuracy and responsiveness through actionable intelligence.

Quantitative improvements

Increased analyst efficiency

- 30% reduction in mean time to respond (MTTR) to security incidents.
- 30% boost in analyst productivity through automated tasks and streamlined workflows.

Comprehensive data retention

- 100% retention of raw packet capture data for a specified period, enabling a thorough forensic analysis and incident investigation.

Enhanced network visibility

- 30% faster packet analysis and troubleshooting.
- 20% reduction in the time taken to identify and resolve suspicious network activity.

Stronger threat detection

- 20% improvement in detecting advanced threats and zero-day exploits.
- 20% decrease in false positive alerts, improving analyst efficiency and reducing alert fatigue.
- Enhanced accuracy of machine learning models for anomaly detection.

Reliable platform

- 99.5% uptime, ensuring continuous network monitoring and protection.

Qualitative improvements

Improved threat detection

- Enhanced ability to distinguish between normal and suspicious traffic.

Stronger security posture

- Greater visibility into network activities, enabling proactive threat detection and response.
- Improved compliance with industry regulations and security standards.

Better user experience

- More intuitive and interactive GUI for easier operations and analysis.
- Simplified workflows and reduced manual effort.

.

WHAT OUR CUSTOMER HAS TO SAY

> "Vehere's NDR has the best potential as it provides the ability to view packet-by-packet information for any session, which other network security tools do not possess. It also provides the ability to create customised interactive dashboards for threat hunting needs."

A TRISYS PRODUCT
info@trisyscom.com

Vehere Technologies Pvt. Ltd.

1390 Market Street
Suite 200
San Francisco, CA 94102

Unit No. 5, 1st Floor
Andaz, Asset Area 1
Aerocity, New Delhi-110037

E: sales@vehere.com
W: www.vehere.com