VECTRA

Protecting High-Frequency Trading (HFT) without Disrupting Business with Network Detection and Response (NDR)

Cyber attackers target high-frequency trading (HFT) companies by attempting to gain unauthorized access to their trading systems, manipulate market data feeds, or disrupt their network connectivity, aiming to execute trades at advantageous prices before legitimate market participants, often through methods like: spoofing orders, layer-peeling, order-flow manipulation, denial-of-service attacks, malware injection, social engineering to gain credentials, and exploiting vulnerabilities in trading algorithms or infrastructure; essentially aiming to disrupt the fast-paced, millisecond-based trading environment to profit at the expense of the market. Given the rapid, automated nature of High-Frequency Trading (HFT), it's crucial to have robust security measures to promptly detect, investigate, and respond any malicious activities.

Vectra NDR provides a compelling solution for AI-driven detection for both known (suspicious activities based on known IOC's) and unknown (advanced exploits not yet public). We understand HFT security presents its own unique challenges, but utilizing NDR as part of the overall security stack is crucial for securing HFT infrastructure. HFT is a unique area in the financial sector that carries out a tremendous number of transactions at exceedingly rapid speeds using sophisticated algorithms. Capacitated to execute millions of orders within fractions of a second and no human intervention, HFT sits at the cutting-edge of financial trading technology. Yet, this dynamic, fast-tracking computational power makes HFT landscapes vulnerable to various security breaches, increasing the urgency to continually protect its cyber-physical systems. This is where Network Detection and Response (NDR) plays a critical role.

Challenges with protecting High-Frequency Trading (HFT) and Financial Services Institutions:

LACK OF VISIBILITY

- EDR's cannot be present everywhere. EDR's don't run on vendor appliances, Contractor/BYOD, and IoT/OT equipment. Right off the bat, risks around data breaches for HFT increasingly rise. Additionally, HFT environments prefer not to deploy agents such as EDRs due to concerns with latency and associated risks from software supply chains that utilize these types of deployments.
- Risks from threats that have already passed your permitter defenses including IDS/IDPS (e.g. post-compromise) that slip through undetected especially for internal threat and insider trading activities.

LACK OF REAL-TIME THREAT DETECTION OF MODERN ATTACKS

- Lack of Artifical Intelligence (AI) or Machine Learning (ML) in security stack and more reliance on manual detection methods/solutions for issues cannot scale or keep up with modern attackers today.
- Physical challenges of HFT wires can cause even more risks. Every HFT institution utilizes microwave signals linking together various data centers and exchanges around the world to conduct their trades. Therefore, the speed of sending and receiving a trade over the wire is critical and modern attackers disrupt this process to stop operations.

MEETING COMPLIANCE AND REGULATION STANDARDS

- Simplifying compliance and evolving regulations and firm policies such as those supporting FFIEC, NYDFS, SEC, FINRA, GLBA, and more are pivotal. You want to trust in your security stack in that it adheres to compliance across multi-repository architectures.
- Reduce complexity with as much security consolidation as possible for easy deployment and without impacting CPU's and overall performance for smooth operations.

Why Vectra NDR is necessary for protecting High-Frequency Trading (HFT) and Financial Services Institutions

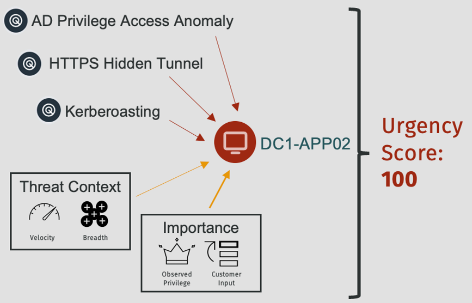
AI identifies real attacker activity in real-time

Access	Persist	Command & Control	Escalate & Evade	Recon & Discover	Lateral Movement	Exfiltration & Disruption
New Host	MFA Disabled	Hidden HTTPS Tunnel	New Host Role	Kerberoasting (x4)	Privilege Access Anomaly (x6)	Smash and Grab
Suspected Compromise Access	Trusted IP Change	Hidden DNS Tunnel	Log Disabling Attempt	Internal Darknet Scan	Suspicious Remote Exec	Ransomware File Activity
Brute-Force Attempt/Success	Admin Account Creation	Hidden HTTP Tunnel	Disabling Security Tools	Port Scan	Suspicious Remote Desktop	Data Gathering
Disabled Account	Account Manipulation	Hidden ICMP Tunnel	Suspicious Mailbox Rule	Port Sweep	Suspicious Admin	Data Smuggler
TOR Activity	Redundant Access	Multi-homed Fronted Tunnel	Log Disabling Attempt	SMB Account Scan	Shell Knocker	Hidden Tunnel Exfil (x4)
Unusual Scripting Engine	Device / Factor Registration	Suspicious Relay	Suspect Privilege Escalation	Kerberos Account Scan	Automated Replication	Botnet Abuse
Suspicious OAuth App	Logging Disabled	Suspect Domain Activity	Suspect Privilege Manipulate	Kerberos Brute-Sweep	Brute-Force	Crypto mining
Suspicious Sign-On	User Hijacking	Malware Update	Suspect Console Pivot	File Share Enumeration	SMB Brute-Force	External Teams Access
Suspicious Sign-On with MFA Fail	ECS Hijacking	Peer-to-Peer	Suspect Cred Access EC2	Suspicious LDAP Query	Kerberos Brute Force	Ransomware SharePoint Activity
Suspicious Teams App	Suspect Login Profile Manipulation	Suspicious HTTP	Suspect Cred Access SSM	RDP Recon	SQL Injection Activity	Suspicious SharePoint Download
Suspicious Copilot Access	Security Tools Disabled	Stealth HTTP Post	Suspect Cred Access ECS	RPC Recon	Internal Stage Loader	Suspicious SharePoint Sharing
Suspicious CSP Access	SSM Hijacking	TOR Activity	Suspect Cred Access Lambda	RPC Targeted Recon	Suspicious Active Directory	Exfil Before Termination
Suspicious Credential Usage	Suspect Policy Manipulation	Novel External Port	Diagnostic Logging Disabled	Unusual eDiscovery Search	Novel Admin Protocol	Suspicious Mailbox Forwarding
Root Credential Usage	Suspicious App Service Action	Threat Intel Match	Subscription Admin Abuse (x4)	Unusual Compliance Search	Novel Admin Share Access	eDiscovery Exfil
TOR Activity	Managed Identity Abuse	Vectra Threat Intel Match	VM/ARC DSC Execution	Suspect eDiscovery Activity	ICMP Internal Tunnel	Power Automate Activity (x3)
Suspicious CSP Access	Suspicious Policy (x3)		Suspect Key Vault Privilege Granted	User Permission Enumeration	Risky Exchange Op	Ransomware S3 Activity
TOR Activity	Suspect App Service (x3)		Privilege Anomaly: Root Scope	EC2 Enumeration	Internal Spear phishing	Suspect Public S3 Change
	Anomalous App Service WebJob		Privilege Anomaly: Management Group Scope	S3 Enumeration	File Poisoning	Suspect Public EBS Change
			Suspicious VM Serial Console Usage	Suspect Escalation Recon	Mailbox Manipulation	Suspect Public EC2 Change
				Organization Discovery	DLL Hijacking	Suspect Public RDS Change
				Suspicious Copilot Access	Privilege Operation Anomaly	Suspect External Access Grant
				Azure Credential Dump	Suspicious Runbook Usage (x2)	Suspicious Disk Download
				Suspect Key Vault Cred Dump	Suspicious RunCommand Execution (x3)	Cryptomining
				Suspect Key Vault Enumeration	Suspicious Extension (x3)	Suspect Public Change (x2)
						Suspect Mass Resource Delete

🟩 Data Center Network & Identity, IaaS, IoT/OT
🟦 Identity: Azure AD (Entra ID)
🟧 SaaS: Microsoft 365
🟪 Gen Ai: Copilot for M365
🟦 PaaS: AWS
🟩 PaaS: Azure

- > Top vendor in MITRE D3FEND patent references (12)
- > Over 90% MITRE ATT&CK coverage
- > Deliver over 150 pre-built behavior-based models
- > 35 patents in AI behavior-based AI detection

AI prioritizes real attacks in real-time



- > Consider and learn what's important
- > Automatically triage benign activity
- > Connect & correlate activity across domains
- > Score entities based on behavior and context

VECTRA AI HELPS WITH:

- **Agentless Threat Detection with Zero Impact on Latency** – Vectra AI precisely detects by identifying the right capture points. Both North-South and EastWest network traffic directions are monitored to provide comprehensive visibility in a "zero-trust" environment. Many existing HFT environments are already configured with the necessary SPAN/TAP traffic mirrors, and deploying Vectra AI may be as simple as connecting those traffic mirrors to the Vectra appliances. Vectra AI can deploy quickly for both on-promises environments (physical and virtual) and cloud environments (IaaS and SaaS) for seamless integration into your current security infrastructure that starts detecting right out of the box.
- **Robust cybersecurity infrastructure** – Vectra AI provides fortified command & control for a hybrid network. Even if it's encrypted, Vectra AI helps security teams maintain C2 access to mitigate successful execution of spoofing, layer peeling, order-flow manipulation, Denial-of-Service (DoS), malware injection, zero-day exploits phishing attacks, and insider collusion.
- **Reconnaissance** – Covering generic protocol agnostic (Port Scans, Port Sweeps, Darknet) and targeted (RPC Recon, File Share Enum, LDAP) is essential. Vectra AI provides reconnaissance for credentials specifically pertaining to applications, to see if an end user initiates unauthorized access.
- **Stopping Lateral Movement Attacks** – Vectra AI detects protocol agnostic exploits (Internal Stage Loader and Automated Replication); Comprised credentials (Privilege Access Anomalies, Suspicious RDP, Suspicious Admin); File encryption for impact (Ransomware File Activity) which are critical to detecting and responding to credential-based lateral movement that chains alerts in a way that finds a single source of truth.
- **Mitigate Interruption of Time-Sensitive Operations** - Vectra AI provides enhanced Threat Hunting, Investigation and Forensics with access to full network metadata in real-time which is pivotal to stopping data gathering and exfiltration activities. Vectra AI detects and responds to threats that gain access to critical systems and closely monitor all user activity.
- **Advanced Threat Intelligence** - Vectra AI detect hybrid network attacks by coupling Signatures (Suricata) with AI-driven detections to detect and stop any hybrid network attack (both known and unknown) while meeting current compliance regulations.

Risks of Relying on Legacy Solutions vs. Vectra NDR

VECTRA AI VS IDS APPROACH

- IDS solutions require a significant amount of manual effort in managing and tuning each of the separate deployed IDS sensors. With Vectra NDR and Vectra Match all of your NDR security tools are deployed on the same sensor greatly reducing your security footprint and addressing tool sprawl. Coupling Vectra NDR AI-driven detection with Vectra Match (Suricata) exploit detection for CVE's significantly reduces the number of false positives that you get with IDS. The sheer volume of data processed in HFT is colossal, extending into gigabytes per seconds and IDS rely on any deviation from standard data patterns (primarily known patterns) for their detection methods. In doing so, SecOps are not able to focus on responding to incidents because they need a lot of effort to vet each incident with all of the contextual insights from behaviors in your network to paint the full picture of the most critical and urgent threats. Furthermore, IDS, IPS and IDPS solutions are often placed at the perimeter of your network. These solutions often focus on north/west movement but can miss east/west movement and focus on in-line protection. Vectra Match with Vectra NDR focuses on detecting both known and unknown behaviors with an expanded threat intelligence database and visibility into your entire network both on-premises and in the cloud. Simply put, Vectra AI supports all IDS use cases with AI-driven supervised and unsupervised ML detections coupled with Suricata (Signature based detections) for known IOC's.

VECTRA AI VS FIREWALL APPROACH

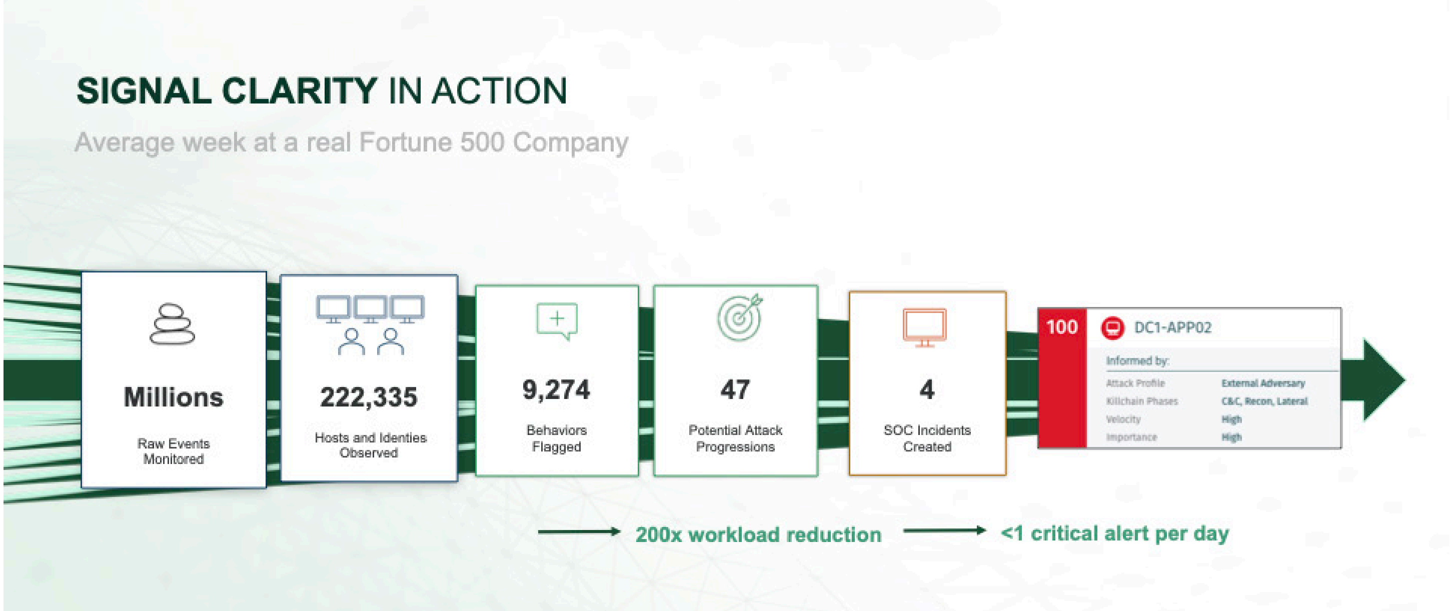
- A Firewall is meant to reduce the overall attack surface, e.g. block access to services on your computer. HFT computers are purpose built, they don't have file sharing, print sharing, remote desktop or any other service running that will slow them down. Inserting a firewall between the Trading machine and the exchange yields minimal to no benefit and oftentimes end up slowing down the trading process altogether. Additionally, relying on firewall-based permitters alone increases your risk overall. Vectra AI takes a behavioral analyst's approach to Threat Detection Investigation and Response (TDIR) use cases that focuses on user entities and resources across the network infrastructure to pinpoint what they are actually doing once they are inside (post-compromise) to identify the highest-risk threats without slowing down operations.

VECTRA AI VS EDR APPROACH

- Endpoint Detection and Response (EDR) can only monitor endpoints, leaving large areas of the network and cloud completely blind and open to modern attackers to get in. EDR's by nature are also very resource intensive as they require a lot of processing power and memory which can slow down systems because they require installing endpoint agents on each device which can impact system performance. With Vectra AI you will close visibility gaps across the entire network infrastructure including applications and workloads without impacting performance.

Risks of Relying on Legacy Solutions vs. Vectra NDR

Network metadata is the most authoritative source for finding threats. Only traffic on the wire reveals hidden threats with complete fidelity and independence. Low-resolution sources, such as analyzing logs, only show you what you've seen, not the fundamental threat behaviors that attackers simply can't avoid as they spy, spread and steal. An NDR solution specifically Vectra NDR, collects and stores key network metadata and augments it with machine learning and advanced analytics to detect suspicious activities on enterprise networks. Vectra NDR builds models that reflect normal behavior and enriches the models with both real-time and historical metadata. Vectra NDR provides a 360-degree, enterprise-wide view—from public cloud and private data center workloads to user and internet-of-things devices. By continual scrutiny of network traffic and real-time signaling of abnormal activities or behaviors by both a host or machine, Vectra NDR safeguards core trading operations from the most critical and urgent security threats. Further, the characteristics of HFT such as high speed and volume of trades, integration with various exchanges, and reliance on automated algorithms significantly increase the complexity of defining 'normal' behavior. Vectra NDR powered by the only Attack Signal Intelligence for AI-driven detection, investigation, and response becomes crucial in such scenarios to stop hybrid network attacks from causing damage to HFT operations.



SIGNAL CLARITY IN ACTION

Average week at a real Fortune 500 Company

VECTRA NDR DELIVERS:

- Real-Time Network Detection: Due to the ultra-low latency nature of HFT, any anomalous or malicious traffic must be detected and blocked immediately. As algorithms become more nuanced, manual detection of issues will not scale. Vectra AI Attack Signal Intellgience that powers our AI-driven detection can profile normal behavior patterns from vast log and traffic datasets, automatically detecting deviations and attacker behvaior across the network infrasturcutre including both incoming and outgoing network traffic including on-premises, cloud, and SaaS.
- Network Signal Clarity: Vectra NDR reduces risks from data exfiltration and insider trading risk by breaking down the siloes around true host attribution and their corresponding actions to keep operations running through a behavior based analytics approach of user entities' (both host and machine) that precisely pinpoints the most urgent and critical threats to act fast.
- Enhanced Network Controls: Vectra NDR AI-driven controls are automated to reduce Mean Time To Respond (MTTR) that does not rely on limited access controls for authentication, authorization, and principle of least privilege to detect and respond to compromised credentials or manipulated insiders' that also reduce risks and storage costs. HFT environments are sensitive and cannot introduce any latency which is why Vectra NDR can be deployed without an agent quickly out of the box and is operating system agnostic (including Linux) to give you as much flexibility as possible and get up and running fast.

Modern attackers are looking to get into HFT fast and often focus on the most accessible threat vectors to infiltrate their attack quickly. It is imperative to have an NDR solution in place because hybrid network attackers need the network to execute their attack.

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. When modern cyber attackers bypass existing controls, evade detection and gain access to customers' data center, campus, remote work, identity, cloud, and IoT/OT environments, the Vectra AI Platform sees their every move, connects the dots in real-time, and stops them from becoming breaches. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai