VECTRA | zscaler

Vectra AI + Zscaler Secure Zero Trust Access

Together Protecting modern networks from modern attacks

Key Challenges

Over the past few years, networks – and the way we work – have fundamentally changed. Traditional network security that focused on the physical boundaries of our offices, specifically policies enforced with firewalls to control where users can go and what they can access using network access control, has become obsolete. With the rise of remote and hybrid work, this new distributed workforce is forever working outside the boundaries and control of the "traditional corporate office" by shifting outside of on-premises infrastructure, creating visibility gaps into network traffic and introducing added complexity and blind spots into visibility from remote users, moving to the Cloud and SaaS, and encrypted protocols such as TLS, DTLS, or IPSec that complicate monitoring and inspection.

Solution Overview

The Vectra AI Platform deeply integrates with both Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) to provide continuous monitoring of network traffic sourced from an endpoints (e.g. end user) that traverse SASE solutions such as Zscaler ZPA and ZIA coupled with the Vectra AI Platform for attack detection, investigation, and response.

With the shift to more remote work, network traffic moving outside of internally hosted applications and workloads have increased, creating blind spots that modern attackers are taking advantage of. With these integrations, The Vectra AI Platform automatically receives traffic from Zscaler to detect cyber threats hidden in approved applications and encrypted traffic, correlates those threats to the hosts that are under attack, and delivers unique context about what attackers are doing, enabling security teams to quickly prevent attacks and mitigate loss. With Vectra's AI models purpose-built to detect real cyber attacker behavior with automatic AI detections to stop command and control, botnet monetization, internal reconnaissance, lateral movement, and data exfiltration in real-time.

Ultimately, the Vectra AI and Zscaler joint solutions enables SOC teams with:

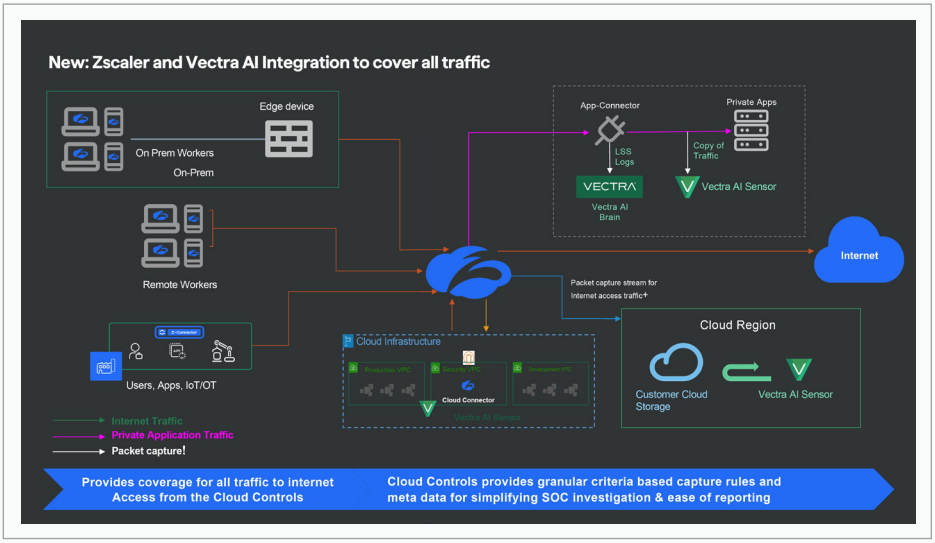
- Improved visibility – Close visibility gaps at the network edge as your teams shift into SSE environments
- Reduced complexity – Simplify workflows and reduce alert fatigue with unified tools
- Advanced threat detection – AI-enabled Detection and Response to accelerate investigation while automating threat mitigation
- Better Threat Hunting – Enhanced forensics capabilities that enable proactive and streamlined threat investigation
- Zero Trust Enforcement – Accelerate Zero Trust adoption beyond traditional on-premises networks to encompass both identity and cloud environments through Zero Trust Tunnels.
- Legacy VPN Replacement – Replace legacy VPNs and maintain visibility without compromising security.
- Incident Response – Speed up root cause analysis with contextual data from both Vectra AI and Zscaler.

Key Benefits:

- **Eliminates Blind Spots at the Network Edge** - Remove blind spots at the network edge without impacting user connectivity or administrative workflows - through the expanded integration of Vectra AI and ZIA and ZPA.
- **Detect Advanced Attacker Techniques** - Detect advanced threats like evasive C2, hybrid attack paths, lateral movement, account compromise, and identity escalations that bypass traditional tools.
- **Enhanced Forensics and Investigations** - Accelerate threat hunting with rich forensic context that supports proactive investigation workflows to respond to attacks fast.

How it Works

- **Comprehensive Traffic Collection** – Ingest traffic directly from Zscaler (e.g. ZTunnel 1.0/2.0, GRE, IPSEC, or PAC) for users on-premises or remote at speed and scale
- **Full Transparency** – Collect traffic without requiring changes to user connectivity patterns or impacting overall user experience
- **Secure Cloud Packet Delivery** – Vectra AI integrates with ZIA's cloud-based Traffic Capture to deliver complete packets securely based on customer-defined policies and storage
- **AI-enabled Threat Detection and Response** – Access Vectra AI-detections for full AI, metadata, Vectra Match inspection, and advanced investigation and response capabilities



Conclusion

The Vectra AI and Zscaler integration enables SOC teams to operate with clarity and speed. By combining Zscaler's Zero Trust Exchange with Vectra's AI-driven detection, SOC analysts can see more, investigate faster, and respond decisively—without the need for legacy infrastructure or sensor-heavy deployments.

INTEGRATION BENEFITS:

- **Reduced risk** – The Zscaler inline and integrated security stack combined with the Vectra AI Platform modern network visibility significantly reduces attacker dwell time and the business loss caused by security breaches, malicious insiders, and downtime.
- **Increased SOC efficiency** – Comprehensive visibility from workforce to network to applications provides a complete view of the threat landscape. Automatic prioritization of alerts augments your SOC, and one-click drill down and pivot between consoles, as well as cross-platform workflow, expedites investigation and response by up to 34x.
- **Access visibility** – Full insight into how the workforce is accessing applications and from where, giving insights that can help scale infrastructure as needed.
- **Secure zero trust architecture** – Ensure that only the authorized users are accessing business-critical private applications and workloads by securing access and monitoring how accounts are being used once access has been granted.

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. The Vectra AI Platform delivers AI-driven Network Detection and Response (NDR) to surface and stop threats across the data center, campus, remote work, identity, cloud, and OT environments. In the first-ever Gartner® Magic Quadrant™ for Network Detection and Response, Vectra AI was named a Leader and positioned highest for Ability to Execute and furthest for Completeness of Vision. 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.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160+ data centers globally, the SASE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

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