VECTRA SECURITY THAT THINKS® | zscaler™

SOLUTION BRIEF

# Securing Zero Trust Access for a remote workforce

The Vectra Cognito Platform integrates with Zscaler Zero Trust Exchange to provide end-to-end access protection from remote workers to app, and the ability to identify and respond to modern attacks in real time.

## The Problem

Over the past few years, and even more so over the last months, 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 over 70% of employees around the world working remote and companies anticipating it staying that way, this new distributed workforce is forever working outside the boundaries and control of the corporate office.

The remote accessibility of corporate networks render both traditional network security solutions and endpoint solutions incapable of controlling data storage and providing visibility into its retrieval.

## KEY HIGHLIGHTS

- Over 70% of employees around the world are working remotely and companies are planning for a hybrid remote work model going forward.
- Zscaler and Vectra Network Detection and Response helps to monitor and protect this remote workforce.
- A hybrid network security model that spans both cloud workloads and on-prem applications allow you to track and stop attackers earlier in the kill chain – all while keeping access to your applications available and easy for the entire extended workforce.

Filtering access through the implementation of virtual firewalls is cumbersome to maintain, and VPN throughput to corporate applications impacts the user experience and is easily circumvented by attackers.

Furthermore, VPNs allow access to the network, further granting bad actors the ability to move laterally and access additional corporate assets.

The need for improved secure access to corporate applications and data has never been greater.


## The Solution

To address these issues, Zscaler and Vectra have joined forces to offer organizations reliable secure, monitored access to business-critical applications through modern security-as-a-service platforms.

Modern cyberattacks often start with the attacker stealing or compromising valid enterprise accounts. These so called *account takeover attacks* circumvent preventative security solutions like MFA and provide the attackers with a starting point into a cloud service or enterprise network. Once access has been established, attackers move laterally to new accounts or between cloud and hybrid networks. Because of the nature of these attacks – leveraging valid accounts and multiple disparate services – traditional security solutions struggle to stop them.

To mitigate this, a better approach is to leverage Zscaler's Zero Trust platform, enabling secure access to the internet and applications.

Combined with Vectra Network Detection and Response, the joint solution helps to monitor and protect the remote workforce. This joint solution of market leading NDR along with market leading Zero Trust platform makes the transition to this new norm easier, faster, secure, and manageable.

By leveraging a hybrid network security model that spans both cloud workloads and on-prem applications in tandem with learning behavioral models that understand hosts and identities, it allows you to track and stop attackers earlier in the kill chain – all while keeping access to your applications available and easy for the entire extended workforce.

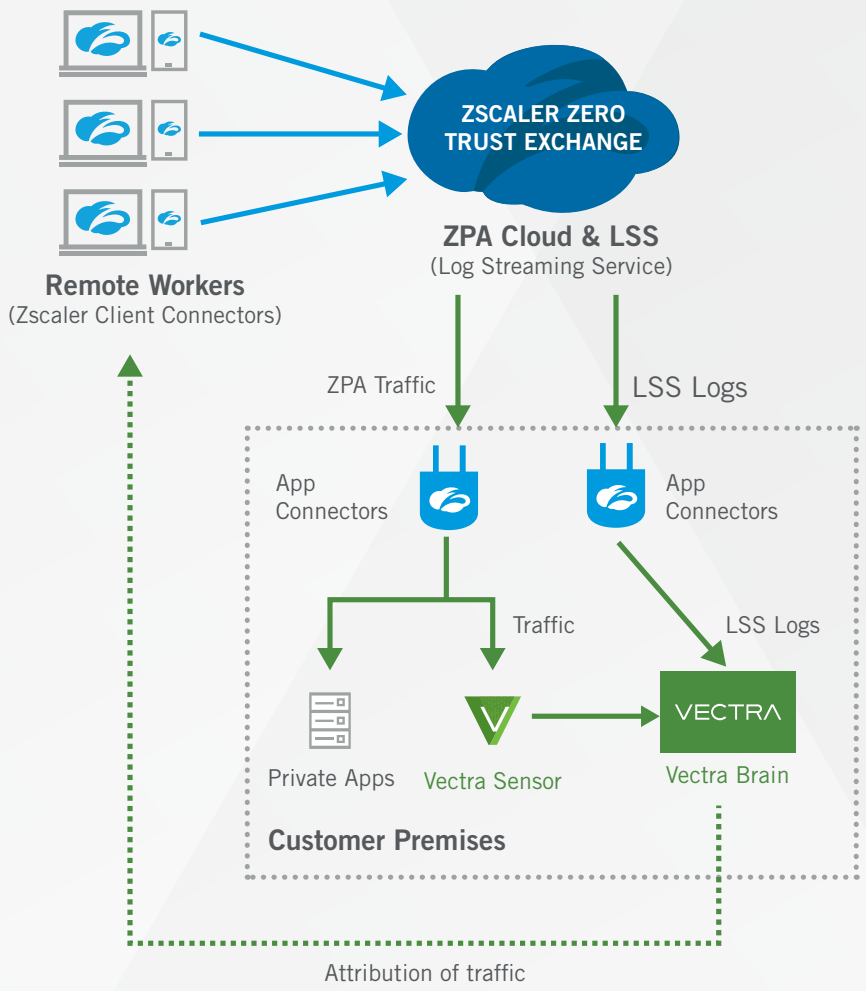
## The Zscaler and Vectra Integration

### Zscaler Private Access (ZPA) and Vectra Cognito Platform

**ZeroTrust access visibility:** Zscaler ZPA allows secure access to business-critical internal applications whether they are on-prem or in the cloud. Vectra continually monitors all interactions and accounts used, and identifies malicious intent from both account compromises as well as malicious insiders. This allows organizations to have full visibility into interactions on their network, and to take action to stop attacks before they lead to data loss or ransomware attacks.

### Integration Benefits

- **Reduced risk** – The Zscaler inline and integrated security stack combined with Vectra identity and 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 your workforce is accessing business-critical private applications and workloads by securing access and monitoring how accounts are being used once access has been granted.



## About Vectra

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

## About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100-percent cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, the Zscaler multitenant, distributed security cloud protects thousands of customers from cyberattacks and data loss, so they can embrace cloud agility, speed, and cost containment—securely.

**For more information please contact a service representative at info@vectra.ai.**

Email info@vectra.ai vectra.ai