Zscaler Traffic Capture

AT-A-GLANCE

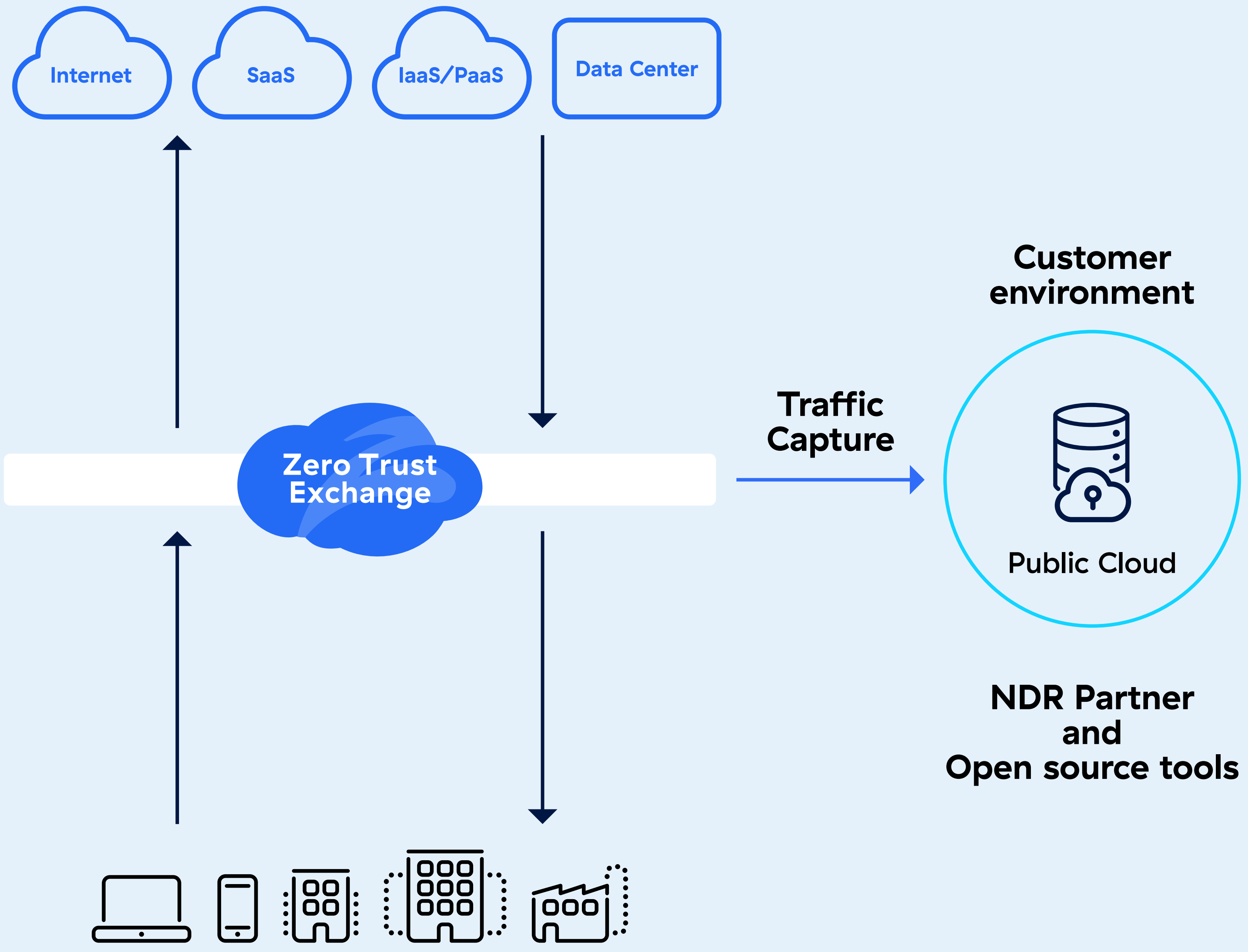
Zscaler Traffic Capture enables security teams to continuously capture traffic using granular rules for hybrid environments. It securely forwards captured traffic to customer-managed cloud storage for security investigations, deeper analysis, and threat hunting.

Overview of Traffic Capture

Zscaler offers two "Traffic Capture" add-ons, to capture traffic for further investigations.

1. Traffic Capture Essentials is a critical solution for organizations focused on security visibility, forensic investigations, and compliance. Engineered to meet the dynamic needs of SOC teams, it offers comprehensive packet capture capabilities that enhance traffic analysis based on internet access controls after decryption. The following policies can be configured to capture traffic: advanced threat protection, file type control, firewall filtering, DNS filtering, IPS control, malware protection, URL filtering.

2. Traffic capture for NDR is a comprehensive solution with more flexibility to capture enriched data, specifically designed for deeper analysis, threat hunting, and collaboration with Network Detection and Response (NDR) partners. With this add-on, ZIA administrators can enable targeted packet capture based on user, application, service, source IP, or destination IP, while also securely forwarding complete packet sequences of encrypted traffic to customer-owned cloud storage to meet regulatory requirements such as HIPAA, PCI DSS, and the federal 72-hour traffic retention mandate. For example, financial institutions can leverage Traffic Capture for auditing data flows and proving compliance with stringent regulations.



Capabilities

✓ **SEAMLESS PACKET CAPTURE**
Configure granular policies to selectively capture traffic based on specific criteria, content scan signatures, or detection logic, ensuring traffic is available for post-decryption analysis.

✓ **PROACTIVE INVESTIGATIONS**
Validate and analyze traffic behind security alerts, allowing analysts to confirm attacks, reduce false positives, and understand attacker techniques.

✓ **COMPLIANCE MADE EASY**
Meet regulatory compliance through traffic record retention, ensuring traceability and auditable evidence for compliance needs.

✓ **IMPROVE PLAYBOOK WITH NDR SOLUTIONS**
Deploy/Migrate threat signatures or detections for new exploit, auto remediate with enforcement tools.

✓ **STREAMLINED SOC EFFICIENCY**
Reduce alert fatigue and investigation times by integrating actionable traffic insights with AI-driven security workflows from NDR Integrations .

✓ **DEPLOY CUSTOM CONTROLS WITH CONFIDENCE**
Improve custom controls efficacy by testing and deploying new threat signatures leveraging captures for custom IPS, tuning, and validation before broader roll-out.

Benefits

COMPLETE VISIBILITY
Continuous traffic capture for cloud and on-premises environments for improved Analytics and Monitoring.

ENRICHED METADATA FOR CAPTURE
NDR partner would receive rich metadata in PCAPNG files for correlation and risk scoring

REDUCE COST AND ALERT FATIGUE
Effectively utilise advanced capture criteria, determining what traffic needs to be captured for monitoring.

COMPLY WITH REGULATIONS
Traffic capture can meet mandatory compliance for regulations in post breach investigations.

EFFORTLESS THREAT HUNTING
Enable your SOC teams to investigate in depth and seamlessly create playbook for protection.

COMPLETE SASE VISIBILITY
NDR partner can ingest traffic from ZIA and ZPA for correlating traffic to create user and device risk.

Traffic Capture integration with NDR vendors

Zscaler Traffic Capture seamlessly integrates with Network Detection and Response (NDR) vendors, providing packet insights that are crucial for SOC teams to detect, investigate, and respond to cybersecurity threats. The NDR partnership addresses a significant gap faced by enterprises when transitioning to cloud-based security solutions, particularly where legacy Firewall TAP traffic visibility is lost. By offering full packet captures, including encrypted traffic securely stored in AWS buckets, Zscaler becomes a critical enablement tool for NDR platforms to enhance operational workflows and support real-time threat investigation.

With Zscaler Traffic Capture, NDR vendors can provide actionable dashboards for SOC teams by analyzing behavioral patterns and identifying anomalies based on ATT&CK frameworks. This strengthens proactive threat hunting and accelerates investigations into flagged or suspicious traffic. Zscaler's capture capabilities also support compliance with federal regulations requiring extended packet visibility, ensuring comprehensive forensic readiness.

Administrators benefit from granular policy configurations across traffic criteria, enabling filter and capture based on transactional data, location groups, applications, source/destination IP, and more. Secure storage mechanisms and role-based access controls enhance data integrity for sensitive traffic.

> Our business and digital transformation depends on smarter, more proactive security. The Zscaler and Vectra AI integration gives us the ability to analyze, detect and respond to threats with precision — whether it's identifying east-west movement within our environment or mitigating encrypted network anomalies in real time. This integration doesn't just enhance our security posture, it lets us expand globally while being agile and sustainable. By aligning security to business goals we're building a resilient company that leads by example.
>
> **JOHN OPALA**
> VP and CISO at HanesBrands Inc

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 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

zscaler™

Zero Trust Everywhere