SOLUTION BRIEF

Fidelis Network and Zscaler Internet Access

Introduction

The reality of a distributed workforce is causing IT security teams to reevaluate their enterprise protection strategies. Remote employee traffic must be protected to the same standard as employees who in an office and working on the corporate network. The security standard should leverage advanced threat detection, anomaly detection, multi-stage analytic rules, and rich support for retrospective investigation—all parts of a holistic, hybrid distributed network. Steering remote traffic through an on-premises network security stack is costly and difficult to manage. It slows down IT security teams, as well as the users they are protecting. Robust network security must be available and enforced everywhere globally dispersed teams work.

The Fidelis Cybersecurity and Zscaler Solution

The combination of Fidelis Network® and Zscaler Internet Access (ZIA) allows enterprise security teams to ensure that access to websites and SaaS apps is enforced by policy, attributable, and safe, while enabling real-time and retrospective analysis for threat detection, threat hunting and data loss/theft prevention. Security analysts can query, pivot and hunt on content and context.

The Challenge

Distributed workforces are now and will remain the normal. Characterized by many employees working from home, traditional approaches to network security are no longer practical or even possible. Enterprises need to ensure that data access is consistently secured regardless of employee location.

The Solution

Fidelis Network® integrates with Zscaler Internet Access (ZIA) to ensure that traffic from employee assets—wherever they may be—is fully secured, and that long-term traffic metadata is available for analysis and investigation. The joint solution allows security teams to detect and prevent threats in real time over hybrid environments and investigate and respond with unmatched visibility at every stage of the attack lifecycle.

Fidelis Network is the NDR component of Fidelis Elevate, an Extended Detection and Response (XDR) solution that includes cyber threat detection from many sources, including network, email, endpoints, and cloud applications and services. By extending the solution to ZIA, Fidelis Elevate supports hybrid environments that span on-premises data centers, cloud IaaS, and ZIA into single threat detection platform.

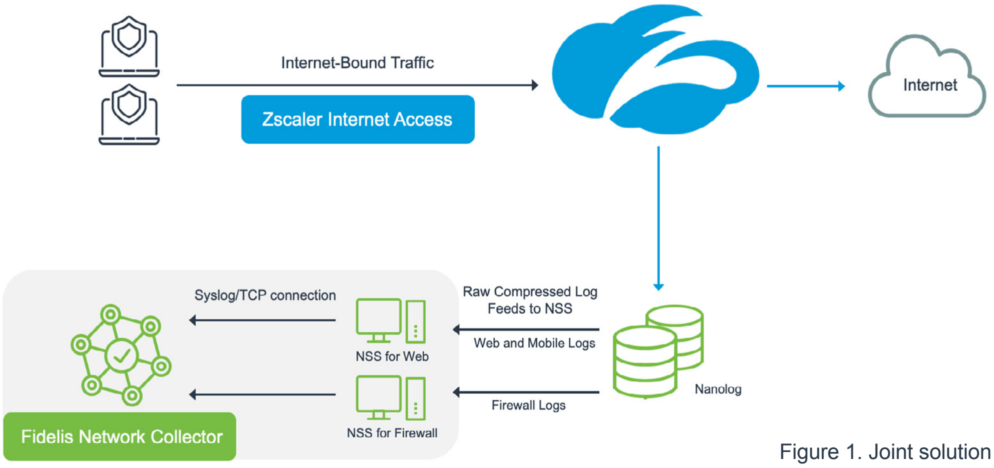

Figure 1. Joint solution deployment

Metadata about traffic passing through Zscaler Internet Access is sent to Fidelis Collector, a component of Fidelis Network, a NDR solution. Collector analyzes metadata for anomalies, runs analytic rules against it to uncover suspicious behavior spanning multiple sessions, and stores it for long-term investigation. Session metadata is searchable via an intuitive user interface (UI) that is painstakingly designed to align with the evolving needs of security analysts. Collector works in a coordinated fashion with metadata from Fidelis network sensors and ZIA to detect threats over a hybrid network.

Remote assets are incorporated into the Fidelis Network Terrain, which offers a combined view of the entire distributed enterprise. Terrain is a great starting point for understanding the overall risk of an enterprise and a springboard into deep investigations of specific activity.

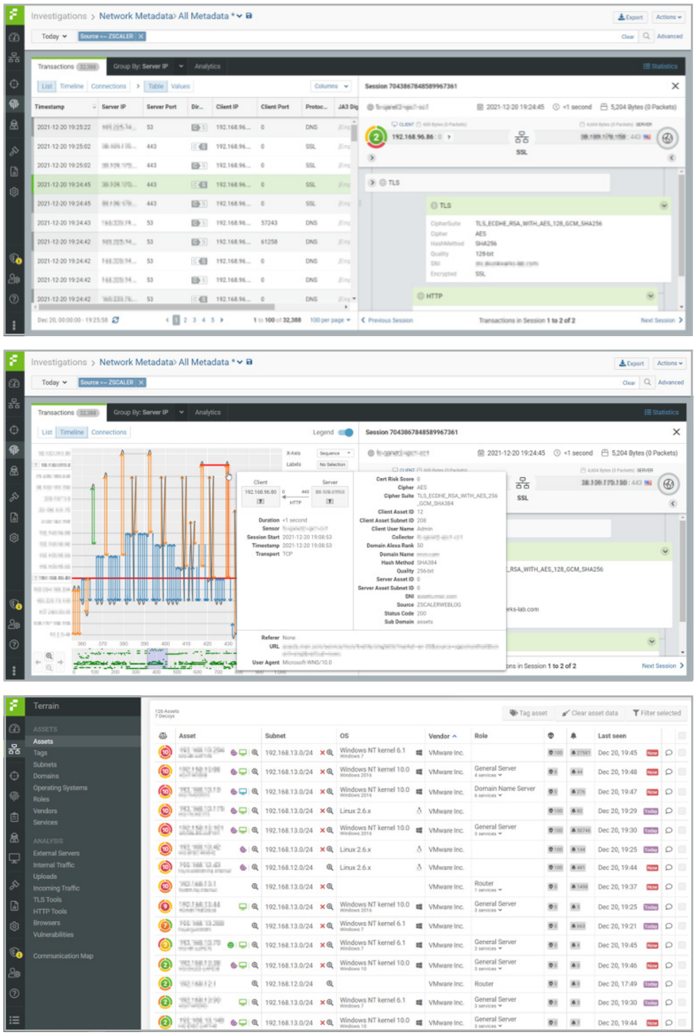

Figure 2. Screenshots of analytics and Terrain based on Zscaler log data in Fidelis Network

Solution Benefits

This joint solution enables the following security use cases for hybrid and distributed networks:

- Extend NDR to remote users with visibility, behavioral analytics and forensics into all communications channels in the enterprise
- Identify complete Terrain with all assets and associated risk in the hybrid network
- Detect cyber-attacks and insider threats emanating from working from home assets, data center assets, and shadow IT
- Find anomalous behaviors in network metadata across entire hybrid network
- Enable threat hunting, investigation and forensics to include all assets and communication in a single interface

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter **@zscaler**.

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in Active XDR and proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. Fidelis Cybersecurity is dedicated to helping clients become stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**