Devo and Zscaler

Global threat visibility and security analytics pairing creates the ultimate solution for cloud-native SOC teams.

SOLUTION SHEET

CORRELATING EVENTS WITH CONTEXT IS ESSENTIAL FOR SECURITY TEAMS

SOC leaders face tremendous challenges. Between dealing with the shift to remote work and an increasing number of advanced persistent threats (APT), the need for solutions that protect the cloud-first enterprise has never been greater. Solutions must correlate events with intelligent data sources to aid security analysts' prioritization and investigation efforts.

ENABLE YOUR TEAM TO PROACTIVELY DETECT, HUNT AND ISOLATE THREATS

Devo and Zscaler have created an integration to address this need, available now for mutual customers. The integration consists of Zscaler's Nanolog Streaming Service consolidating logs from all users, globally, in the Devo Platform, where administrators can view and mine transaction data by user, device, application and location in real time.

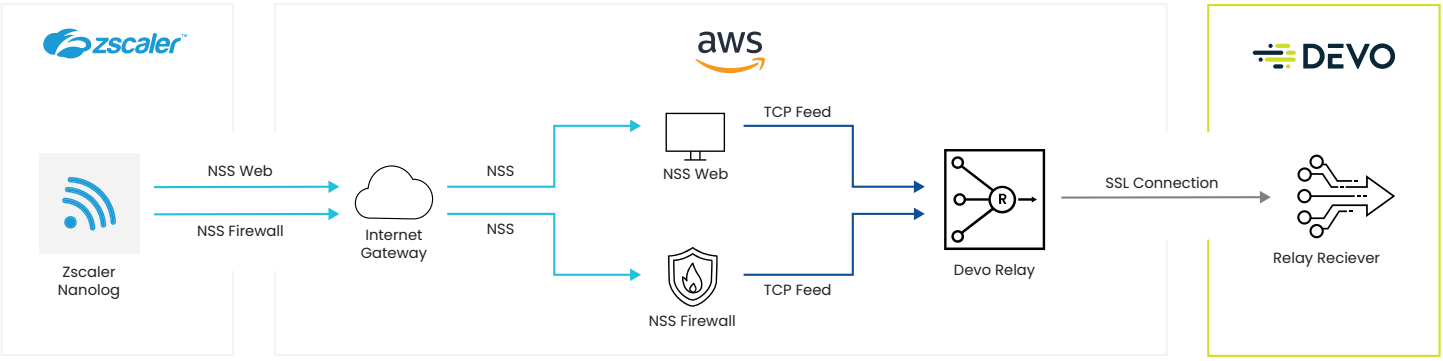
USE CASES

Threat Detection: Reduce MTTD so analysts can detect threats early and then quickly and proactively activate incident response.

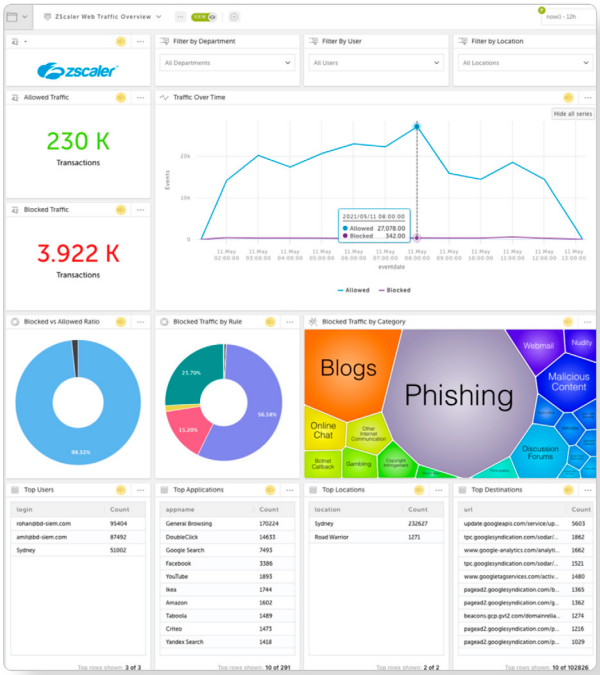
Threat Hunting: Hunt with context for threats across all data — streaming and historical — while enabling SOC analysts to target threats contextually.

Threat Alerts: Isolate threats and block additional compromises, rapidly and effectively.

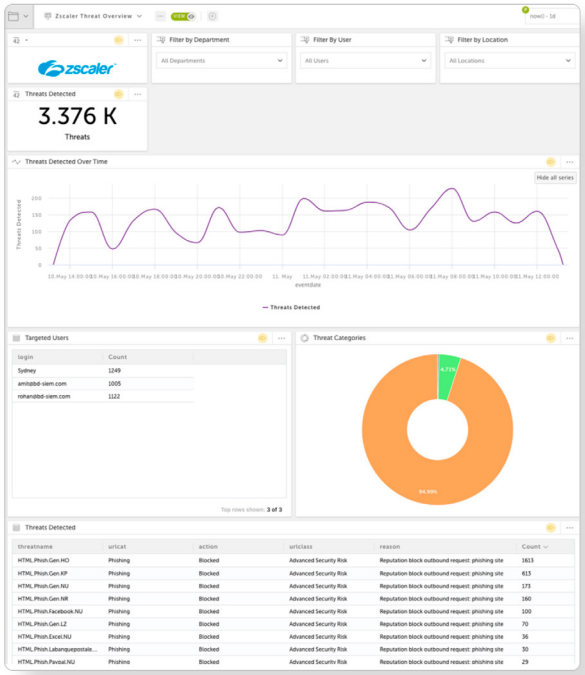
ARCHITECTURE DIAGRAM



This integration enables SOC teams to proactively monitor and react rapidly to incidents as they occur. Analysts can visualize, share and understand data in an intuitive way, enhancing and accelerating their decision-making process.



The Web Traffic Overview Activeboard in Devo, which provides overview statistics of web traffic observed by ZScaler Internet Access (ZIA).



The Threat Overview Activeboard in Devo, which provides overview statistics of web threats observed by ZScaler Internet Access (ZIA).

To access the integration, customers need valid Devo and Zscaler user accounts, a Zscaler Nanolog Streaming Server, as well as a Devo Relay deployed in their infrastructure. To learn more, Devo customers can review this documentation:
https://docs.devo.com/confluence/ndt/v7.3.0/parsers-and-collectors/collectors/zscaler-integration

Zscaler accelerates digital transformation so 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 in-line cloud security platform.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.