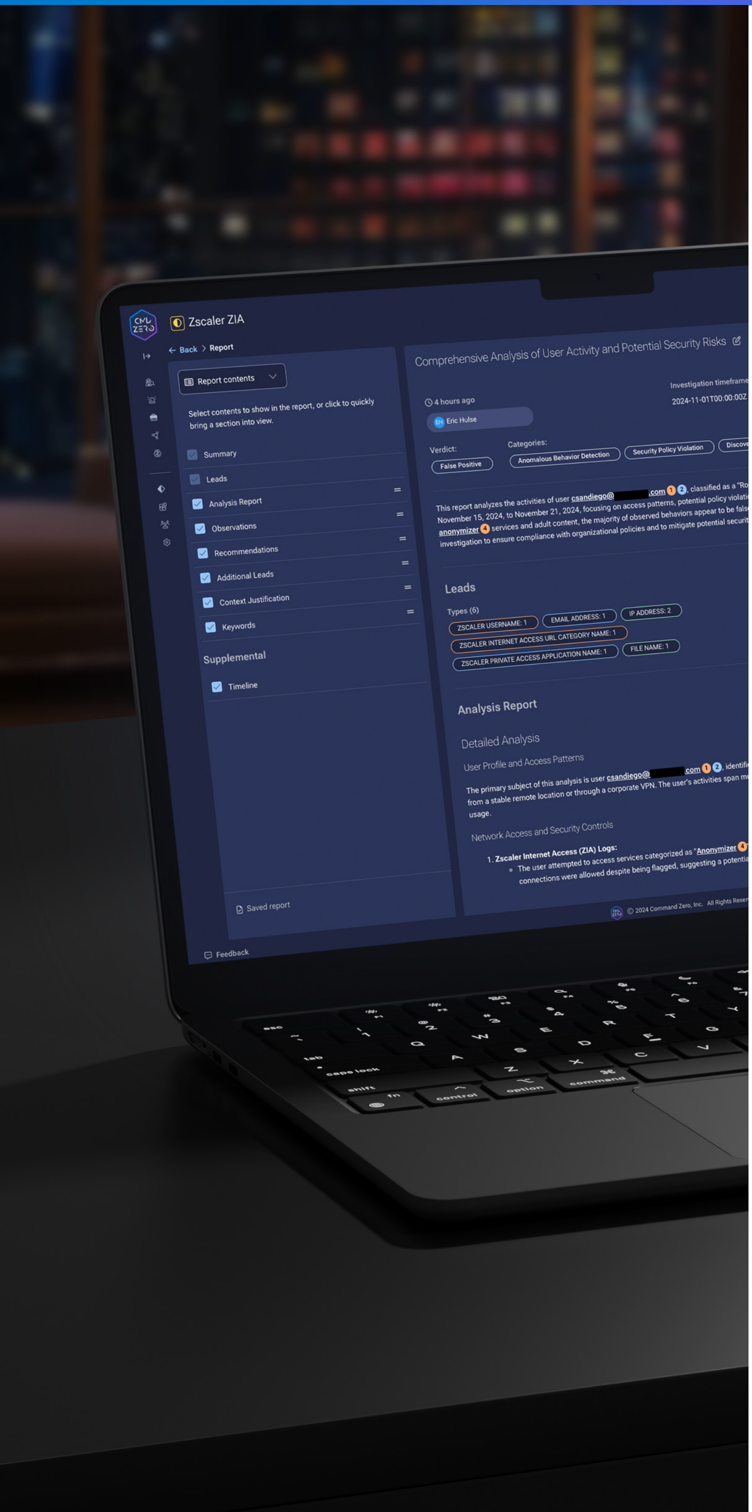
Solution Brief

Operationalize internet traffic and private access data



Select contents to show in the report, or click to quickly bring a section into view.

This report analyzes the activities of user csandiego@[redacted].com 1 2, classified as a "Ro
November 15, 2024, to November 21, 2024, focusing on access patterns, potential policy violati
anonymizer 4 services and adult content, the majority of observed behaviors appear to be fals
investigation to ensure compliance with organizational policies and to mitigate potential securi

The primary subject of this analysis is user csandiego@[redacted].com 1 2, identifi
from a stable remote location or through a corporate VPN. The user's activities span m
usage.

1. Zscaler Internet Access (ZIA) Logs:
   - The user attempted to access services categorized as "Anonymizer 4
     connections were allowed despite being flagged, suggesting a potentia

Internet and application access are the backbone of user activity

Enterprise users rely on SaaS, internal applications and services in modern architecture. These components host critical data and are frequently targeted by attackers. Understanding user behaviors and investigating irregular patterns are key to securing modern organizations today.

ZScaler secures critical traffic and generates valuable insights

While Zscaler Internet Access (ZIA) secures all internet bound traffic by inspecting and blocking threats as per enforced policies, Zscaler Private Access (ZPA) offers zero trust access to internal applications without the need for traditional VPNs. With over 500 billion transactions brokered daily through Zscaler's Zero Trust Exchange, it is evident that this traffic data contains high fidelity logs extremely valuable for security operation teams to fully understand user behaviors over hypertext protocols.

Transform traffic insights into actionable intelligence

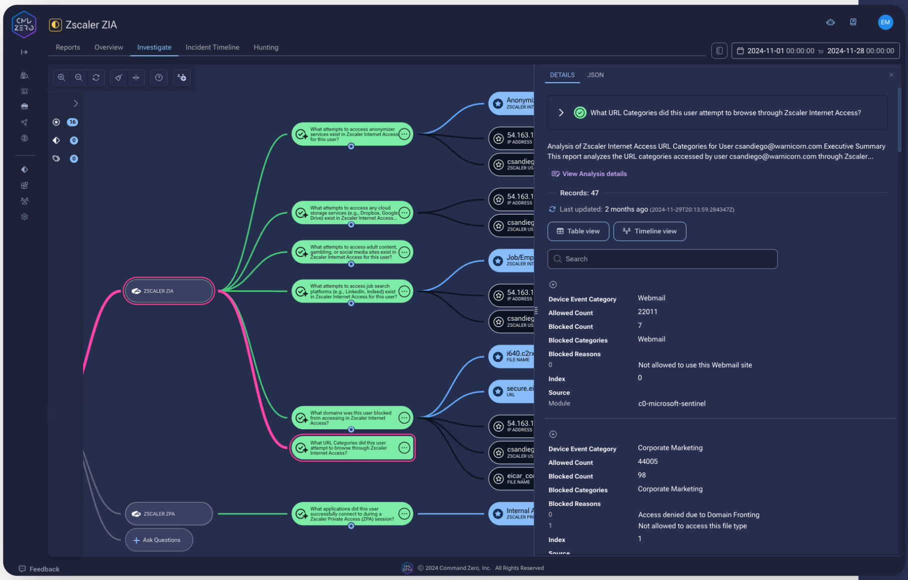
ZScaler and Command Zero have built a solution empowering practitioners with data-driven threat hunting and complex investigations. The solution ingests ZScaler ZIA and ZScaler ZPA data in the Command Zero platform thereby allowing actionable insights to security teams.

Use cases

Run threat hunts

Analysts can identify attention-worthy patterns in traffic data by asking pre-built hunting questions. ZIA and ZPA-specific hunting questions include:

- *What users attempted to access anonymizing services according to Zscaler Internet Access?*
- *What users attempted to access cloud storage services (e.g., Dropbox, Google Drive) according to Zscaler Internet Access?*
- *What users were blocked by policy violations from connecting to a Zscaler Private Access (ZPA) application?*



Zscaler ZIA
Reports
Overview
Investigate
Incident Timeline
Hunting
16
0
0
ZSCALER ZIA
What attempts to acccess anonymizer services exist in Zscaler Internet Access for this user?
What attempts to acccess any cloud storage services (e.g., Dropbox, Google Drive) exist in Zscaler Internet Access...
What attempts to access adult content, gambling, or social media sites exist in Zscaler Internet Access for this user?
What attempts to access job search platforms (e.g., LinkedIn, Indeed) exist in Zscaler Internet Access for this user?
What domains was this user blocked from accessing in Zscaler Internet Access?
What URL Categories did this user attempt to browse through Zscaler Internet Access?
ZSCALER ZPA
What applications did this user successfully connect to during a Zscaler Private Access (ZPA) session?
Ask Questions
Anonymiz
ZSCALER INT
54.163.1
IP ADDRESS
csandieg
ZSCALER US
Job/Emp
ZSCALER INT
i640.c2rx
FILE NAME
secure.ei
URL
eicar_co
FILE NAME
Internal A
ZSCALER PRI
Feedback
© 2024 Command Zero, Inc. All Rights Reserved
EM

2024-11-01 00:00:00 to 2024-11-28 00:00:00

DETAILS JSON

What URL Categories did this user attempt to browse through Zscaler Internet Access?

Analysis of Zscaler Internet Access URL Categories for User csandiego@warnicorn.com Executive Summary This report analyzes the URL categories accessed by user csandiego@warnicorn.com through Zscaler...

View Analysis details

Records: 47

Last updated: 2 months ago (2024-11-29T20:13:59.284347Z)

Table view | Timeline view

Search

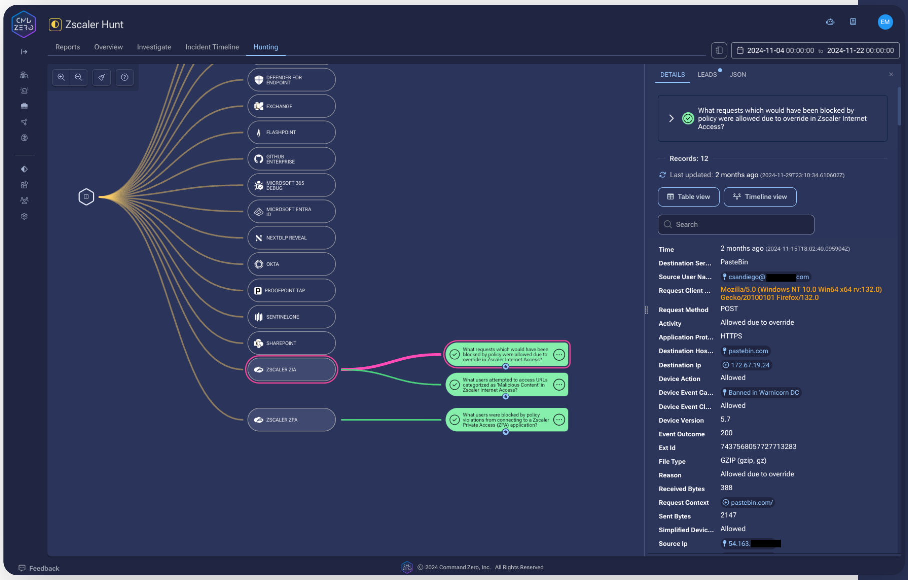
Device Event Category	Webmail
Allowed Count	22011
Blocked Count	7
Blocked Categories	Webmail
Blocked Reasons	
0	Not allowed to use this Webmail site
Index	0
Source	
Module	c0-microsoft-sentinel

Device Event Category	Corporate Marketing
Allowed Count	44005
Blocked Count	98
Blocked Categories	Corporate Marketing
Blocked Reasons	
0	Access denied due to Domain Fronting
1	Not allowed to access this file type
Index	1
Source	

Investigate traffic patterns and user behaviors

Analysts can dig into irregular patterns in traffic data or enrich user or IP focused investigations with relevant access insights from ZScaler. Analysts can leverage ZIA and ZPA focused questions including:

- *What users uploaded or downloaded a file with this name in Zscaler Internet Access?*
- *What applications did this user successfully connect to during a Zscaler Private Access (ZPA) session?*
- *What users connected to applications from this IP Address in Zscaler Private Access (ZPA)?*



Zscaler Hunt
Reports
Overview
Investigate
Incident Timeline
Hunting
DEFENDER FOR ENDPOINT
EXCHANGE
FLASHPOINT
GITHUB ENTERPRISE
MICROSOFT 365 DEBUG
MICROSOFT ENTRA ID
NEXTDLP REVEAL
OKTA
PROOFPOINT TAP
SENTINELONE
SHAREPOINT
ZSCALER ZIA
ZSCALER ZPA
What requests which would have been blocked by policy were allowed due to override in Zscaler Internet Access?
What users attempted to access URLs categorized as 'Malicious Content' in Zscaler Internet Access?
What users were blocked by policy violations from connecting to a Zscaler Private Access (ZPA) application?
Feedback
© 2024 Command Zero, Inc. All Rights Reserved
EM

2024-11-04 00:00:00 to 2024-11-22 00:00:00

DETAILS LEADS JSON

What requests which would have been blocked by policy were allowed due to override in Zscaler Internet Access?

Records: 12

Last updated: 2 months ago (2024-11-29T23:10:34.610602Z)

Table view | Timeline view

Search

Time	2 months ago (2024-11-15T18:02:40.095904Z)
Destination Ser...	PasteBin
Source User Na...	csandiego@[redacted]com
Request Client ...	Mozilla/5.0 (Windows NT 10.0 Win64 x64 rv:132.0) Gecko/20100101 Firefox/132.0
Request Method	POST
Activity	Allowed due to override
Application Prot...	HTTPS
Destination Hos...	pastebin.com
Destination Ip	172.67.19.24
Device Action	Allowed
Device Event Ca...	Banned in Warnicorn DC
Device Event Cl...	Allowed
Device Version	5.7
Event Outcome	200
Ext Id	7437568057727713283
File Type	GZIP (gzip, gz)
Reason	Allowed due to override
Received Bytes	388
Request Context	pastebin.com/
Sent Bytes	2147
Simplified Devic...	Allowed
Source Ip	54.163.[redacted]

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 Command Zero

Command Zero is the autonomous & AI-assisted investigations platform, built to transform security operations in complex enterprise environments. It accelerates expert analysis, ensures a consistent, repeatable, auditable process, enables all tier-2+ analysts to perform at the highest level.

Learn more at cmdzero.io