Datasheet | SSE

Trend Vision One™

Zero Trust Secure Access

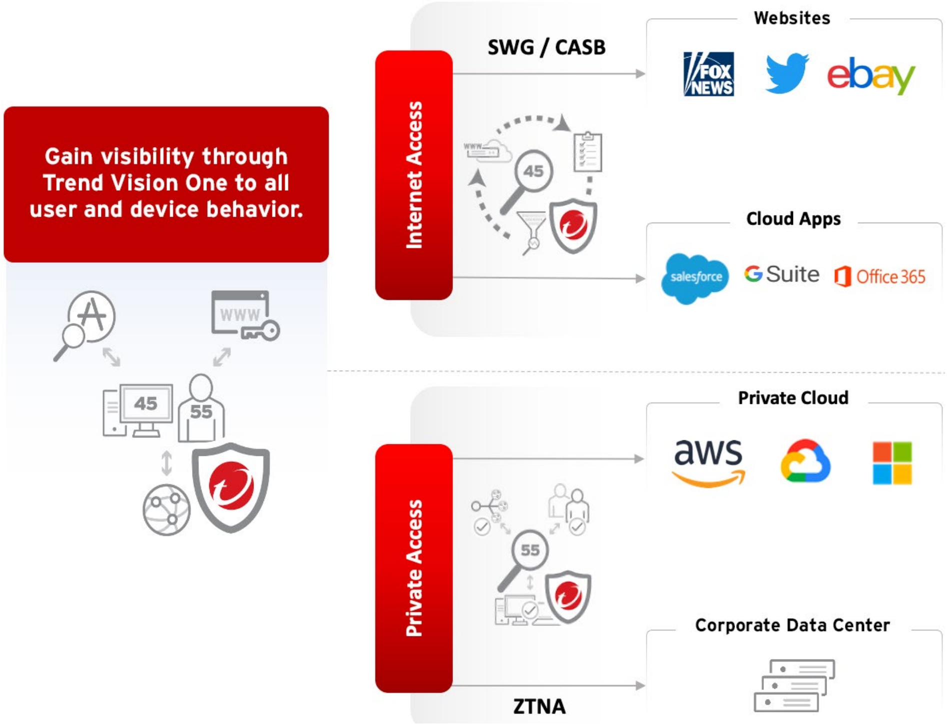
Centralized management with integrated security policy, response, and visibility

As the recent transition to a remote or hybrid workforce has widened the digital attack surface, increasing cyber risk significantly across many organizations, the old adage of "trust, but verify" is no longer practical. The growing interest and movement toward zero trust architectures in the past few years has shifted this approach to the more accurate "never trust, always verify."

And for good reason. The broad implicit-trust methods and practices haven't kept pace with stealthy, more resourceful threat actors. Organizations need to modernize the methods used to securely connect users, devices, and applications no matter where they are or what they need to access.

ONE PLATFORM. ONE AGENT. COMPLETE VISIBILITY.

Introducing Trend Vision One™ – Zero Trust Secure Access:



Secure Access is part of Trend Vision OneTM. The modern cloud-native platform integrates attack surface risk management (ASRM), extended detection and response (XDR), and Secure Access.

Through Trend Vision One, organizations can enrich continuous adaptive risk and trust assessment to drive zero-trust architectures that support their business objectives. With Secure Access, no user or device should be inherently trusted.

In relation to SSE, Secure Access provides secure web gateway (SWG), cloud access security broker (CASB) and zero trust network access to secure access of users and devices across network, web, cloud, and private apps–all in one platform.

This strengthens your overall security posture by enforcing strong access control permissions from multiple identity services across the organization.

What is zero trust?

This new security model drives change in how organizations develop and maintain networks.

The concept centers around the removal of implicit trust for subjects accessing resources from certain parts of the network.

Instead, the assumption is made that there is an intruder within the network, so all connections between subjects, devices, and assets will be checked to verify authorization and authentication, and to evaluate the risk/security posture of the device before the connection is established.

GAIN INSIGHT. ENFORCE CONTROL. REDUCE RISK.

Continuous risk assessment

As we continue to measure cybersecurity risk more closely to business risks, we can see that it is not a "one and done" concept.

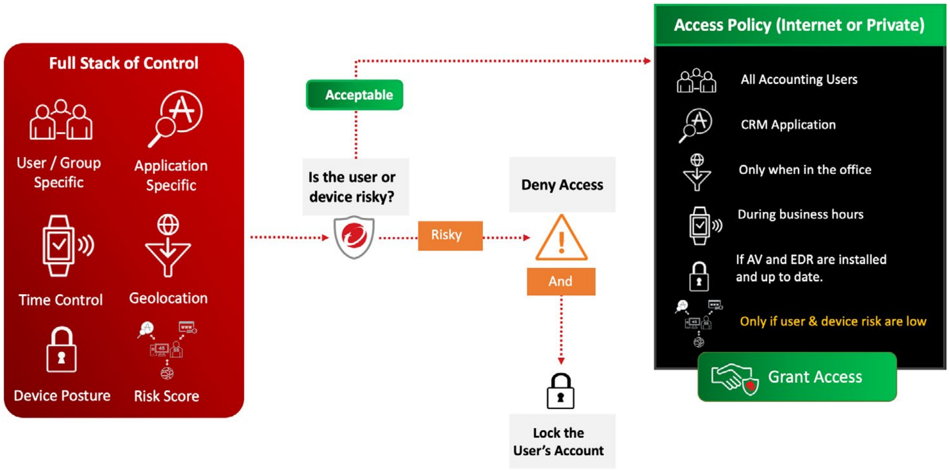
Indeed, risk is always changing and must be continuously assessed to be useful as a mechanism to improve security posture. Trend Micro™ Operations Dashboard provides that function of continuous risk assessment for Secure Access. It gathers telemetry and data to automate decisions by leveraging the Trend Micro endpoint agent and network solutions.

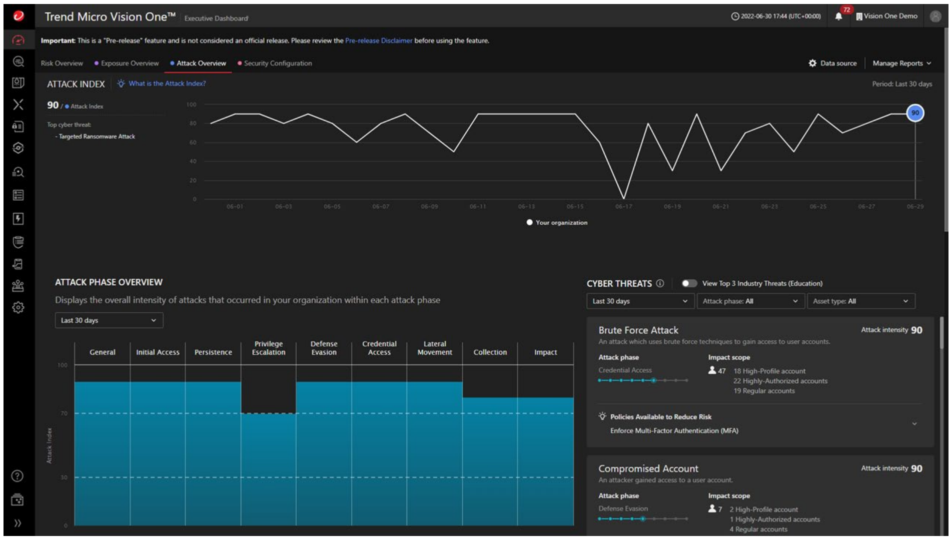
At regular intervals and dynamically in real-time, risk rating data from the Operations Dashboard is used to evaluate current connections between users, devices, and applications. If, at any point, the risk rating exceeds customizable thresholds, the connection is blocked, and the network is protected against exposure. When the risk returns to within tolerance, the connection can be reestablished, and operations can continue securely.

> There is an 'inherent trust' organizations have in their architecture, and zero trust is prohibiting attackers from piggybacking on that trust.

Eric Skinner

Vice President of Market Strategy, Trend Micro





Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

ATTACK INDEX | What is the Attack Index?

90 / Attack Index

Top cyber threat:
- Targeted Ransomware Attack

Period: Last 30 days

ATTACK PHASE OVERVIEW

Displays the overall intensity of attacks that occurred in your organization within each attack phase

Last 30 days

CYBER THREATS | View Top 3 Industry Threats (Education)

Last 30 days | Attack phase: All | Asset type: All

Brute Force Attack — Attack intensity 90

An attack which uses brute force techniques to gain access to user accounts.

Attack phase: Credential Access

Impact scope: 47
18 High-Profile account
22 Highly-Authorized accounts
19 Regular accounts

Policies Available to Reduce Risk
Enforce Multi-Factor Authentication (MFA)

Compromised Account — Attack intensity 90

An attacker gained access to a user account.

Attack phase: Defense Evasion

Impact scope: 7
2 High-Profile account
1 Highly-Authorized accounts
4 Regular accounts

Powered by Trend Vision One™ ASRM

Rethinking trust in your organization

In most organizations, implicit trust is the standard. This exposes the business to considerable risk, where a single compromised identity can begin to wreak havoc in the environment and move throughout the network largely unabated.

Much like digital transformation, the path toward zero trust is a journey, not a solution. There are several "initial steps" that can be taken depending on the highest priority risk in your organization and your current security posture. While more use cases exist, which can be implemented over time as your organization moves towards zero trust architecture, the initial steps include:

1. **SWG: Securing access to the internet with real-time insights**
2. **CASB: Secure access to cloud applications with control**
3. **ZTNA: Secure access to business-critical resources with a modern approach**

> A streamlined, integrated offering with a single agent for XDR, CASB, and ZTSA, along with straightforward pricing.

451 Research

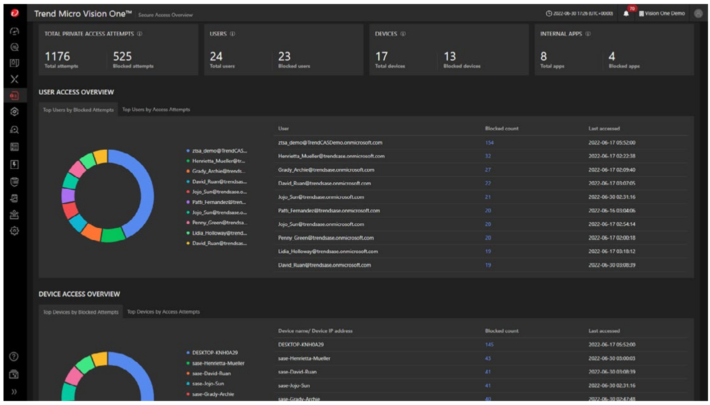
S&P Global
Market Intelligence

1. SWG: Securing access to the internet with real-time insights

- Provides agent and agentless protection for secure web browsing and unsanctioned app access
- Presents highly contextualized data to Trend Vision One for greater visibility
- Offers visibility into internet access and browsing to return security and policy control
- Protects both corporate and bring-your-own (BYO) devices
- A native part of Trend Vision One
- Powered by Trend Micro™ Web Reputation Service, Trend Research, and our Operations Dashboard.

2. CASB: Secure access to cloud applications with control

- Features agent and agentless protection to sanctioned software as a service (SaaS) apps
- Delivers secure access to SaaS apps, checking for policy violations and security risks
- Reduce the risk of unauthorized access to data and critical information
- Monitor application activity through granular cloud-app action control
- Provides continuous risk assessment powered by our Operations Dashboard
- Provides a simple-to-manage interface within Trend Vision One



TOTAL PRIVATE ACCESS ATTEMPTS
1176 Total attempts
525 Blocked attempts

USERS
24 Total users
23 Blocked users

DEVICES
17 Total devices
13 Blocked devices

INTERNAL APPS
8 Total apps
4 Blocked apps

USER ACCESS OVERVIEW

Top Users by Blocked Attempts | Top Users by Access Attempts

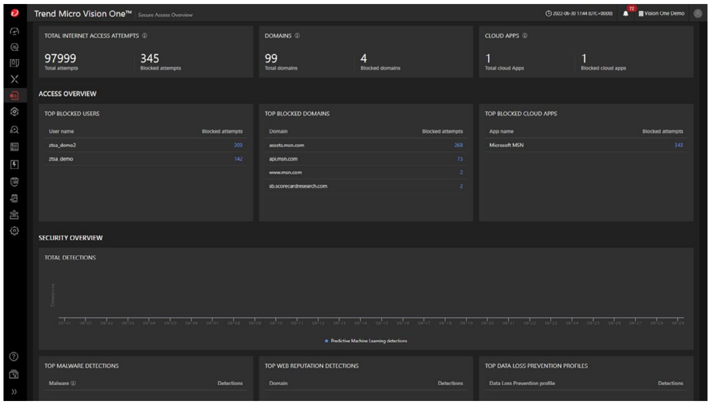
User	Blocked count	Last accessed
ztsa_demo@TrendCASDemo.onmicrosoft.com	154	2022-06-17 05:52:00
Henrietta_Mueller@trendsase.onmicrosoft.com	32	2022-06-17 02:22:38
Grady_Archie@trendsase.onmicrosoft.com	27	2022-06-17 02:09:40
David_Ruan@trendsase.onmicrosoft.com	22	2022-06-17 03:07:05
Jojo_Sun@trendsase.onmicrosoft.com	21	2022-06-30 02:31:16
Patti_Fernandez@trendsase.onmicrosoft.com	20	2022-06-16 03:04:06
Jojo_Sun@trendsase.onmicrosoft.com	20	2022-06-17 02:54:14
Penny_Green@trendsase.onmicrosoft.com	20	2022-06-17 02:00:18
Lidia_Holloway@trendsase.onmicrosoft.com	19	2022-06-17 03:18:12
David_Ruan@trendsase.onmicrosoft.com	19	2022-06-30 03:08:39

DEVICE ACCESS OVERVIEW

Top Devices by Blocked Attempts | Top Devices by Access Attempts

Device name/ Device IP address	Blocked count	Last accessed
DESKTOP-KNH0A29	145	2022-06-17 05:52:00
sase-Henrietta-Mueller	43	2022-06-30 03:00:03
sase-David-Ruan	41	2022-06-30 03:08:39
sase-Jojo-Sun	41	2022-06-30 02:31:16
sase-Grady-Archie	40	2022-06-30 02:47:48

Secure Access overview in the Trend Vision One platform



TOTAL INTERNET ACCESS ATTEMPTS
97999 Total attempts
345 Blocked attempts

DOMAINS
99 Total domains
4 Blocked domains

CLOUD APPS
1 Total cloud Apps
1 Blocked cloud apps

ACCESS OVERVIEW

TOP BLOCKED USERS

User name	Blocked attempts
ztsa_demo2	203
ztsa_demo	142

TOP BLOCKED DOMAINS

Domain	Blocked attempts
assets.msn.com	268
api.msn.com	73
www.msn.com	2
sb.scorecardresearch.com	2

TOP BLOCKED CLOUD APPS

App name	Blocked attempts
Microsoft MSN	343

SECURITY OVERVIEW

TOTAL DETECTIONS

TOP MALWARE DETECTIONS

Malware	Detections

TOP WEB REPUTATION DETECTIONS

Domain	Detections

TOP DATA LOSS PREVENTION PROFILES

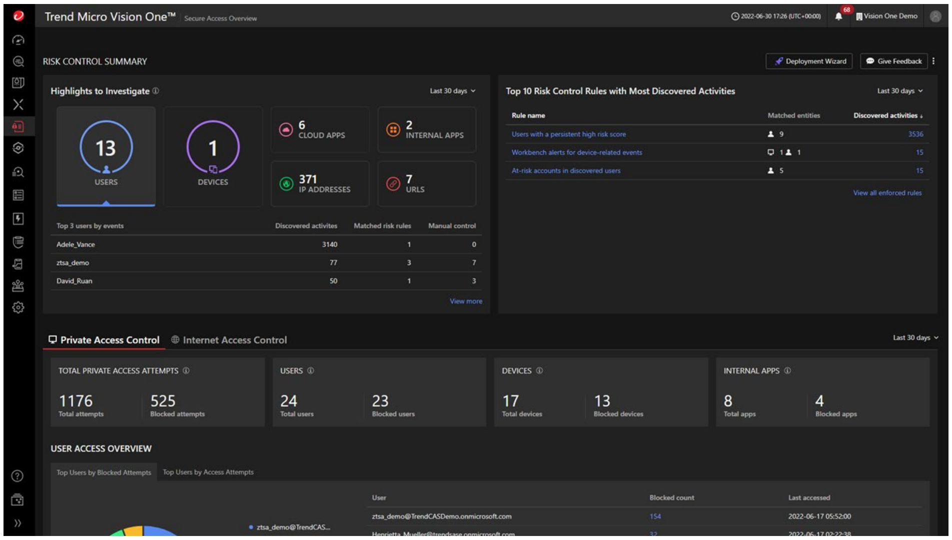
Data Loss Prevention profile	Detections

Secure Access Internet Access Control, part of the modern Trend Vision One platform
Includes SWG and CASB solutions.

3. ZTNA: Secure access to business-critical resources with a modern approach

- Provides agent and agentless access with detailed control options for easy end-user access to corporate apps and resources
- Reduces the implicit trust of VPNs for greater risk assessment
- Delivers authenticated and secure just-in-time access to apps and resources for greater protection
- Reduces the blast area if there is a threat by limiting access to only specific parts of the network
- Provides continuous risk assessment powered by our Operations Dashboard
- Controls connections to apps and resources with continuous risk assessment dynamically allowing and revoking access as risk profiles change

Instead of granting access to the entire network, as a VPN does, Secure Access provides a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. If valid user credentials are stolen, the level of access they will grant to the organization can be contained, effectively reducing the blast area of any attack.



Trend Micro Vision One™ | Secure Access Overview

2022-06-30 17:26 (UTC+00:00) | 68 | Vision One Demo

RISK CONTROL SUMMARY

Highlights to Investigate — Last 30 days

13 USERS | 1 DEVICES | 6 CLOUD APPS | 2 INTERNAL APPS | 371 IP ADDRESSES | 7 URLS

Top 3 users by events	Discovered activites	Matched risk rules	Manual control
Adele_Vance	3140	1	0
ztsa_demo	77	3	7
David_Ruan	50	1	3

View more

Top 10 Risk Control Rules with Most Discovered Activities — Last 30 days

Rule name	Matched entities	Discovered activities ↓
Users with a persistent high risk score	9	3536
Workbench alerts for device-related events	1 1	15
At-risk accounts in discovered users	5	15

View all enforced rules

Private Access Control | Internet Access Control — Last 30 days

TOTAL PRIVATE ACCESS ATTEMPTS: 1176 Total attempts, 525 Blocked attempts
USERS: 24 Total users, 23 Blocked users
DEVICES: 17 Total devices, 13 Blocked devices
INTERNAL APPS: 8 Total apps, 4 Blocked apps

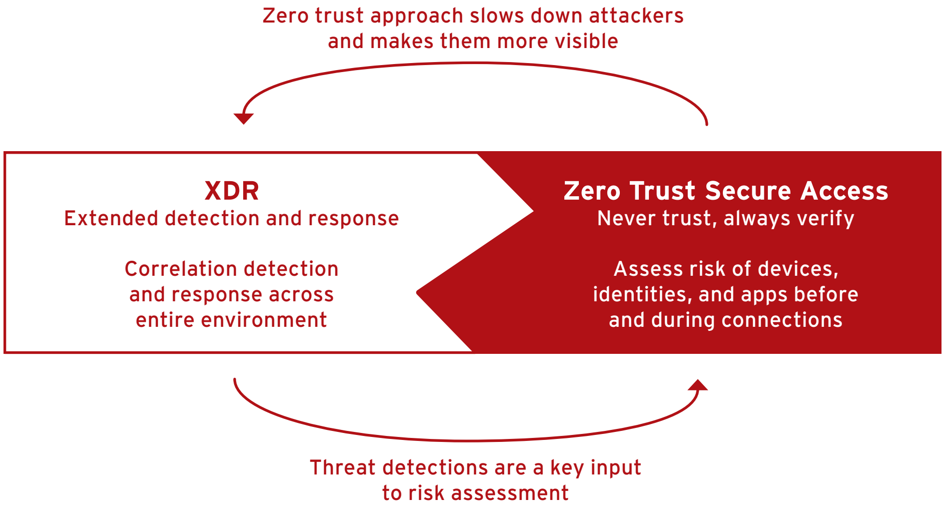
USER ACCESS OVERVIEW

Top Users by Blocked Attempts | Top Users by Access Attempts

User	Blocked count	Last accessed
ztsa_demo@TrendCASDemo.onmicrosoft.com	154	2022-06-17 05:52:00
Henrietta_Mueller@trendsase.onmicrosoft.com	32	2022-06-17 02:22:38

ZTSA Private Access Control, part of the modern Trend Vision One platform Includes ZTNA

Connection between XDR and SSE using Secure Access



Zero trust approach slows down attackers and makes them more visible

XDR
Extended detection and response

Correlation detection and response across entire environment

Zero Trust Secure Access
Never trust, always verify

Assess risk of devices, identities, and apps before and during connections

Threat detections are a key input to risk assessment

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy