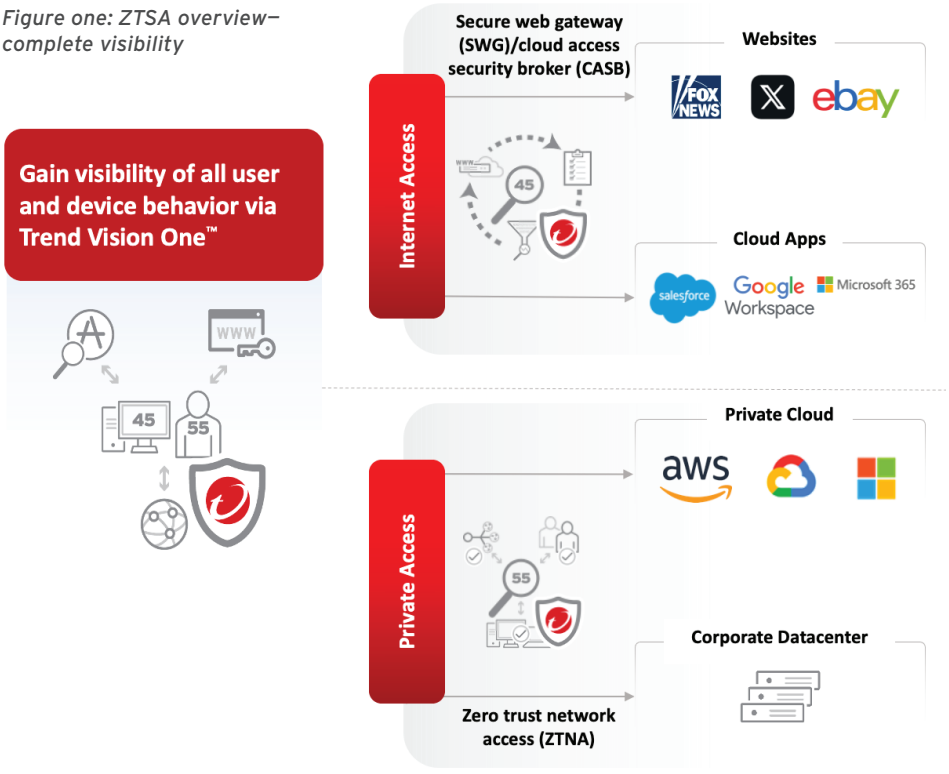
Trend Vision One™ – Zero Trust Secure Access (ZTSA)

Centralize your digital security management with integrated policies, risk response, and visibility

In today's ever-connected world, many organizations are transitioning to—or have already adopted—hybrid or remote operations. With the widening of digital attack surfaces comes increased cyber risk, and so the adage of "trust, but verify" is no longer practical. Broad, implicit-trust methods and practices are insufficient for your operations in the face of today's stealthy, resourceful adversaries and an ever-changing threat landscape. Prioritizing effective verification helps to mitigate your cyber risk.

Harness Trend Vision One™ – Zero Trust Secure Access (ZTSA) to securely connect your users, devices, and applications no matter where they are or what they need to access. With an agile approach to access control, strengthen your protective measures with granular visibility, enhanced security, and continuous risk assessment. Safeguard your users' journey and engagement with generative AI (GenAI) capabilities driving zero-trust architecture that support your business objectives.

Figure one: ZTSA overview—complete visibility



Key benefits:

- Gain control over user and device network access
- Implement and manage strict access permission controls to safeguard data and users
- Boost your risk resilience while streamlining operations for security and network teams
- Expand visibility and response times with continuous risk assessment insights
- Confidently embrace AI into your business while securing the user journey

What is zero trust?

The zero trust security model drives change in how organizations develop and maintain networks.

Rather than implicitly trust subjects accessing resources from certain parts of the network, zero trust assumes that unconventional access represents an intrusion. As a result, all connections between subjects, devices, and assets are checked to verify authorization and authentication.

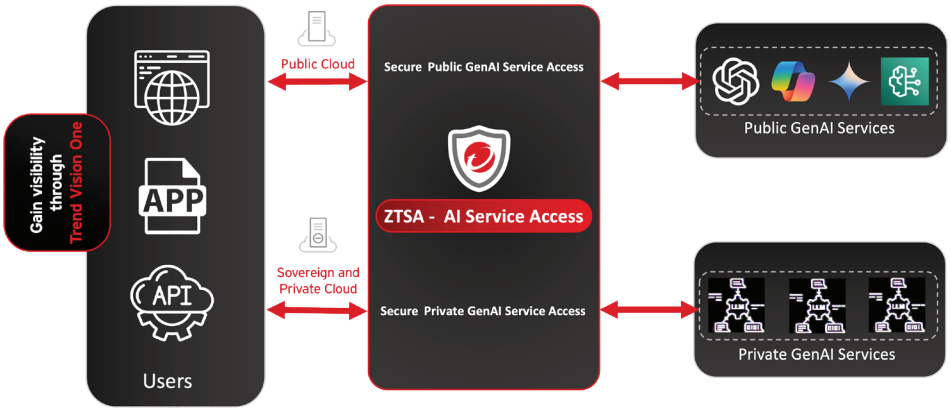
In addition, comprehensive evaluations are performed to determine the risk and security posture of the device in question before the connection is established with your network.

Integrated with our AI-powered Trend Vision One platform

Trend Vision One incorporates ZTSA alongside our dedicated attack surface risk management (ASRM) and extended detection and response (XDR) capabilities. Through Trend Vision One, enrich and inform your protection strategy with continuous adaptive risk and security assessment. In relation to SSE, ZTSA empowers you with SWG, CASB, and ZTNA capabilities. These enable you to secure user and device access across your network, web, cloud, and private applications in addition to AI services.

Strengthen your overall security posture by implementing strong access control permissions across your organization—all through a single unified platform.

Figure two: Trend Vision One™– Zero Trust Secure Access (ZTSA) – AI Service Access overview



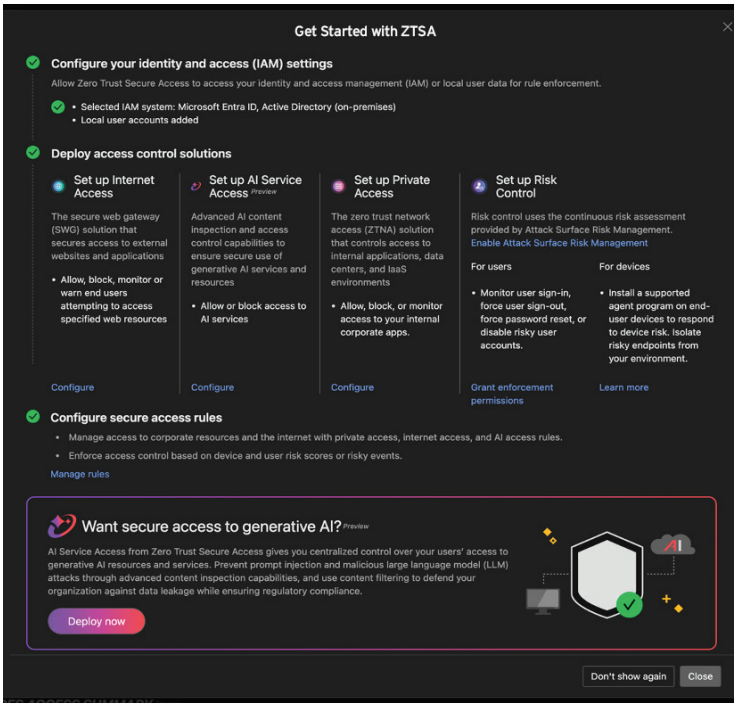
Bridge the gap between GenAI services and secure access

Organizations can harness AI for their business and security operations while defending against its adversarial uses. Access control can be enforced with zero trust principles when accessing public or private GenAI services.

ZTSA – AI Service Access can control AI usage as well as inspect GenAI prompt and response content. Use it to identify, filter, and analyze content to avoid potential sensitive data leakage or unsecured outputs in public and/or private cloud environments. Boost visibility to better monitor and manage your organization's AI usage, helping you prevent potential data exfiltration and attacks using prompt injection detection during the user access journey. In turn, this reduces the risk of potential manipulation of GenAI services by threat actors.

With ZTSA – AI Service Access, protect your user journey with enhanced security, streamline operations, and help enable safer, more seamless user interaction with GenAI—all while maintaining compliance. Improve your overall security posture, business resilience, scalability, operational excellence, and user experience.

Figure three: Guide to getting started with ZTSA



Trend Vision One and ZTSA capabilities

Cloud-native and risk-aware, Trend Vision One gives you access to ASRM, XDR, ZTSA, and multi-layered security capabilities in a unified platform. Empower your network and security teams with enhanced visibility and expanded risk awareness, helping them focus on strategic security measures rather than managing complex infrastructures.

Enable ZTSA to help secure your access to the internet, software-as-a-service (SaaS) applications, and/or GenAI tools. Leverage XDR-powered advanced analytics and ASRM-driven continuous risk assessment to dynamically allow—or revoke—access as user risk profiles change.

> A streamlined, integrated offering with a single agent for XDR, CASB, and ZTSA, along with straightforward pricing could help customers avoid the standard complexity with SASE deployments.

451 Research
S&P Global
Market Intelligence

Gain insight. Improve controls. Reduce risk.

Leverage continuous risk assessment

Risk is always changing and must be continuously assessed to be useful as a mechanism to improve security posture. For this reason, our Trend Vision One™ – Attack Surface Risk Management (ASRM) solution provides continuous risk assessment for ZTSA. ASRM gathers telemetry and data to automate decisions by leveraging our endpoint agent and network solutions.

At regular intervals and dynamically in real-time, risk rating data from ASRM is used to evaluate current connections between your users, devices, and applications. Should the risk rating exceed customizable thresholds, the connection is blocked and your network is protected against exposure. When the risk returns to within tolerance, the connection can be re-established, enabling your operations to continue securely.

Figure four: User access journey overview

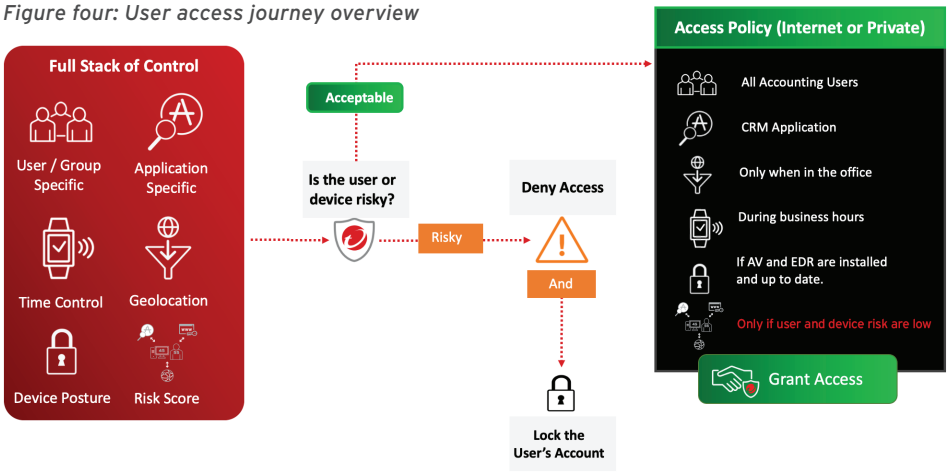
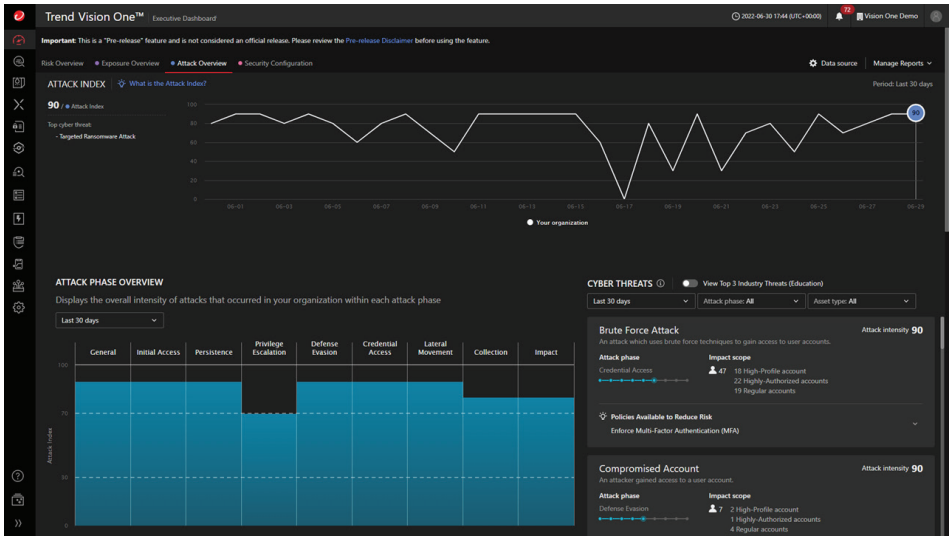


Figure five: Attack phase overview within Trend Vision One Executive Dashboard



> 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

Rethinking trust in your organization

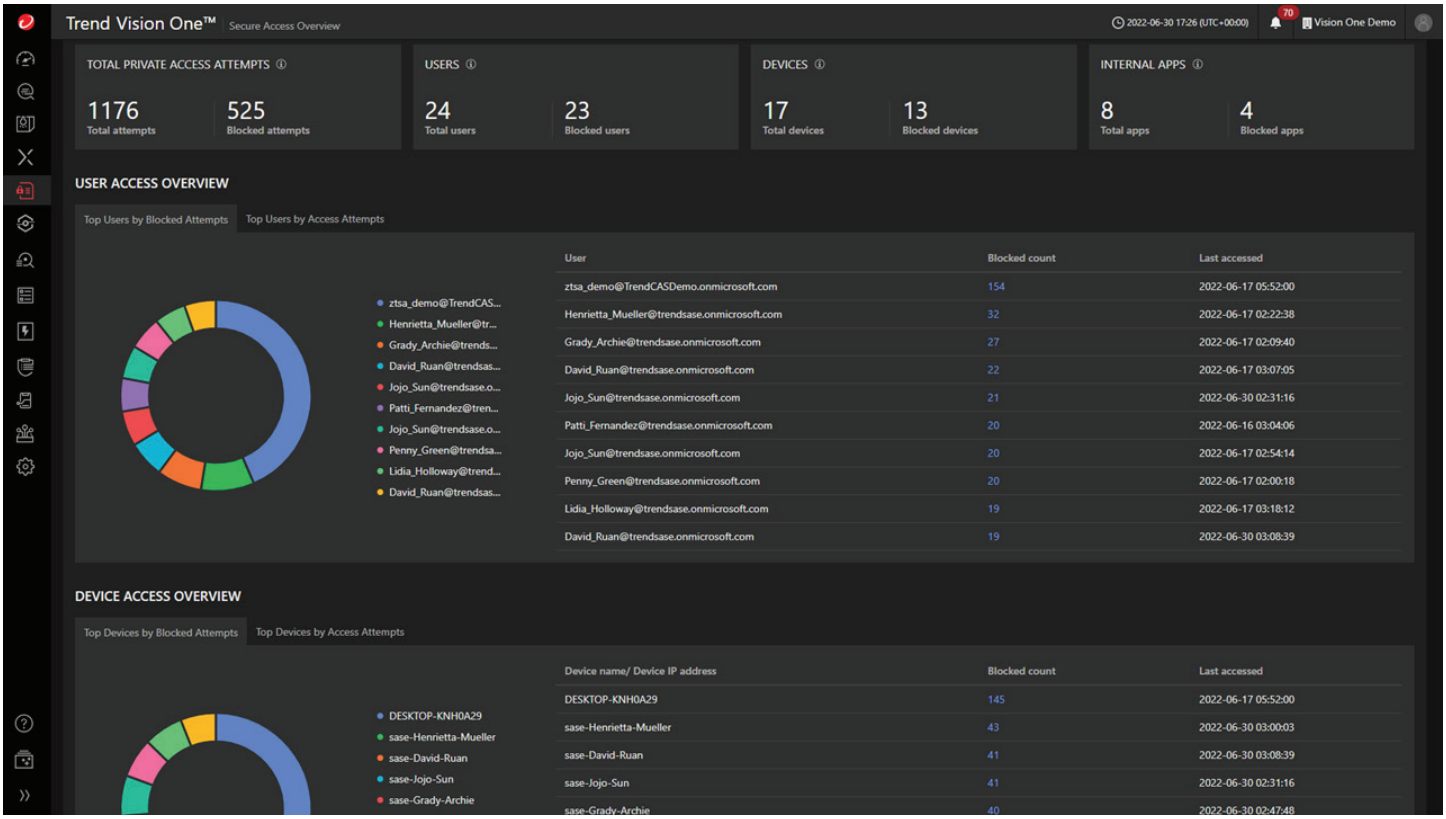
In many organizations, implicit trust is the standard. However, this exposes your business to considerable risk, in which case a single compromised identity could begin to wreak havoc in your environment and move throughout your network.

Much like digital transformation, your path toward zero trust is a journey rather than a solution. There are four important steps that can be taken depending on the highest-priority risk in your organization and current security posture. While more use cases exist, which can be implemented over time as your organization moves towards zero trust architecture, these initial steps include the following:

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

- Provides agent and agentless protection for secure web browsing and unsanctioned application 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
- Integrates natively within Trend Vision One
- Powered by Trend Micro™ Web Reputation Service, Trend™ Research, and ASRM

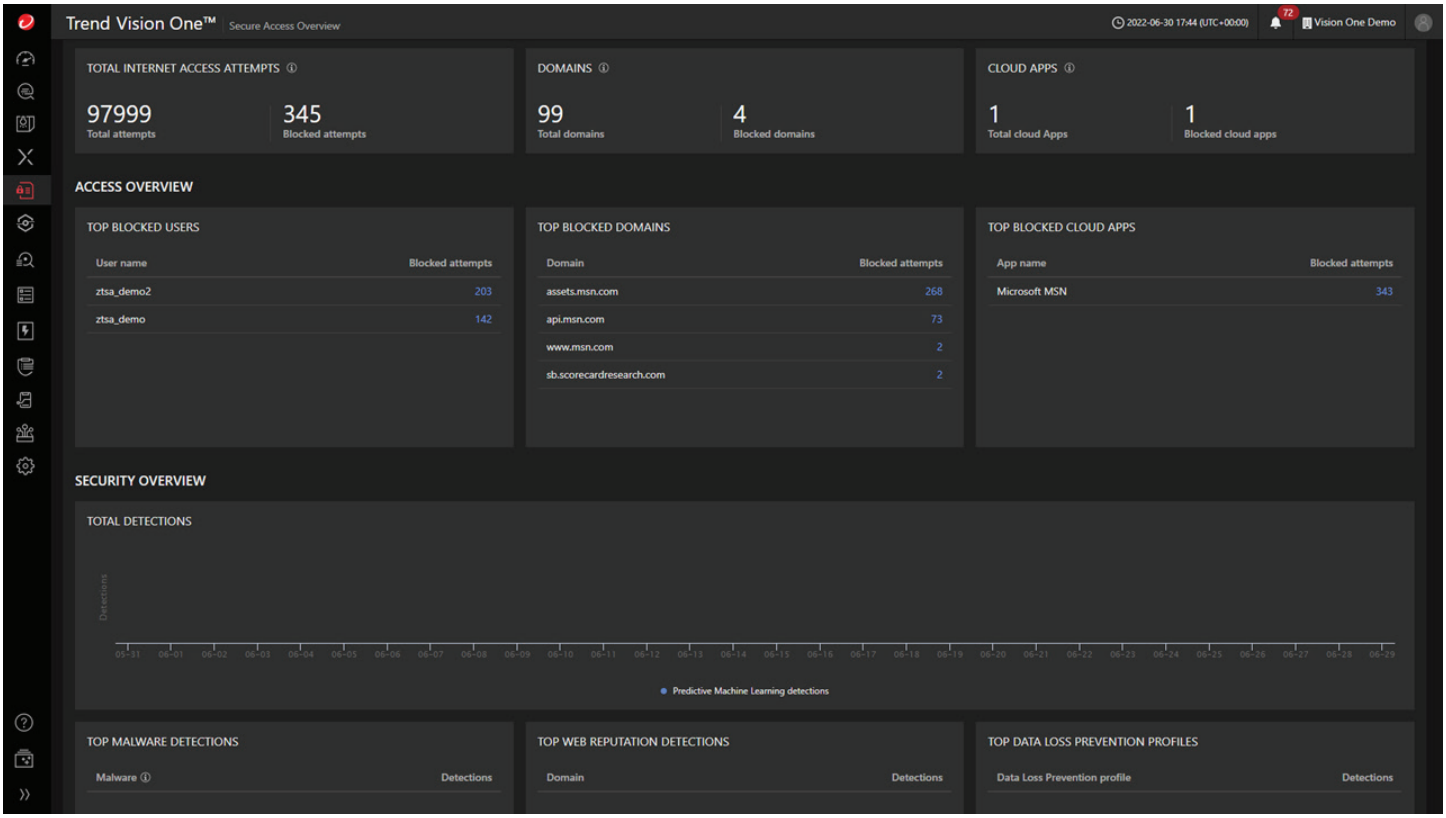
Figure six: ZTSA overview within Trend Vision One



2. CASB: Secure cloud application access and control

- Features agent and agentless protection to sanctioned SaaS applications
- Delivers secure access to SaaS applications, checking for policy violations and security risks
- Reduces the risk of unauthorized access to data and critical information
- Monitors application activity through granular cloud application action control
- Provides continuous risk assessment, powered by ASRM
- Leverages a simple-to-manage interface within Trend Vision One

Figure seven: ZTSA internet access control overview within Trend Vision One

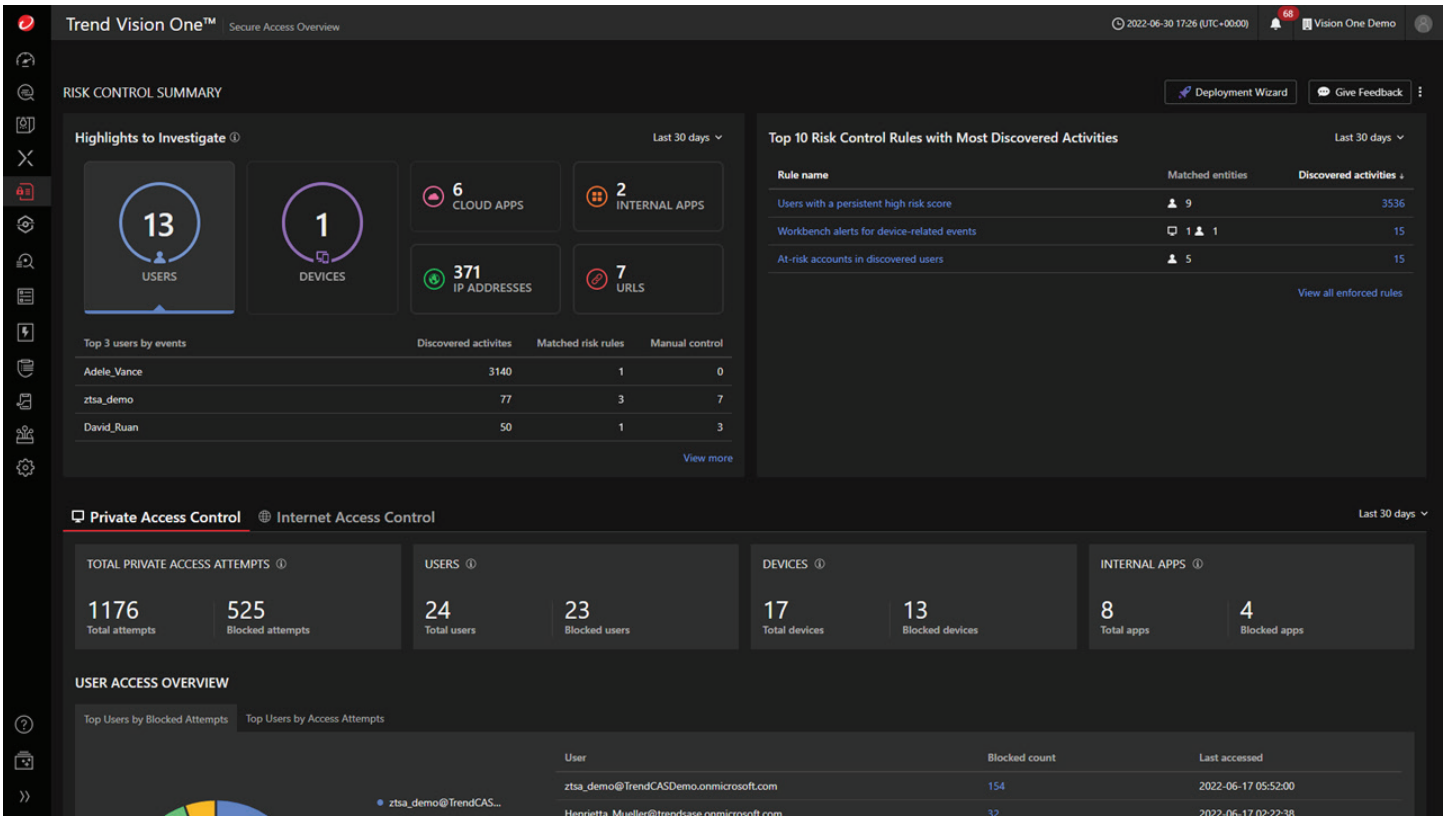


3. ZTNA: Secure access to business-critical resources with a modern approach

- Provides agent and agentless access with detailed control options for easy end-user access to corporate applications and resources
- Reduces the implicit trust of virtual private networks (VPNs) for greater risk assessment
- Delivers authenticated and secure just-in-time access to applications 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 ASRM
- Controls connections to applications 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, ZTSA provides you with a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. This way, should valid user credentials be stolen, the level of access they will grant to the organization will be limited and contained, effectively reducing the "blast area" of any cyberattack.

Figure eight: ZTSA private access control within Trend Vision One



4. ZTSA – AI Service Access: Secure the user journey to GenAI services

- Controls AI application usage by applying continuous risk-based access rules with granular visibility
- Inspects GenAI services' prompt and response to help avoid potential data leakage and unpredictable responses
- Detects prompt injection attacks to mitigate risk of potential manipulation from GenAI services
- Avoids the private model denial of service threats
- Delivers secure access to GenAI applications, checking for policy violations and security risks
- Reduces the risk of unauthorized access to data and critical information

Figure nine: ZTSA – AI Service Access within Trend Vision One

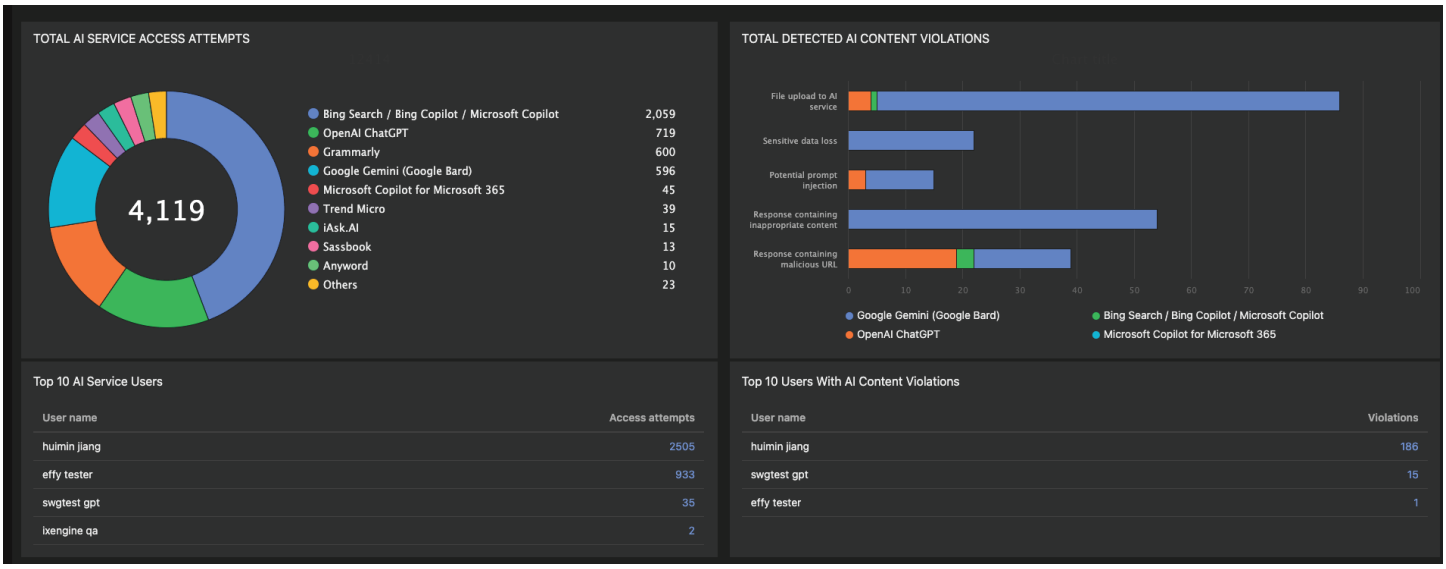
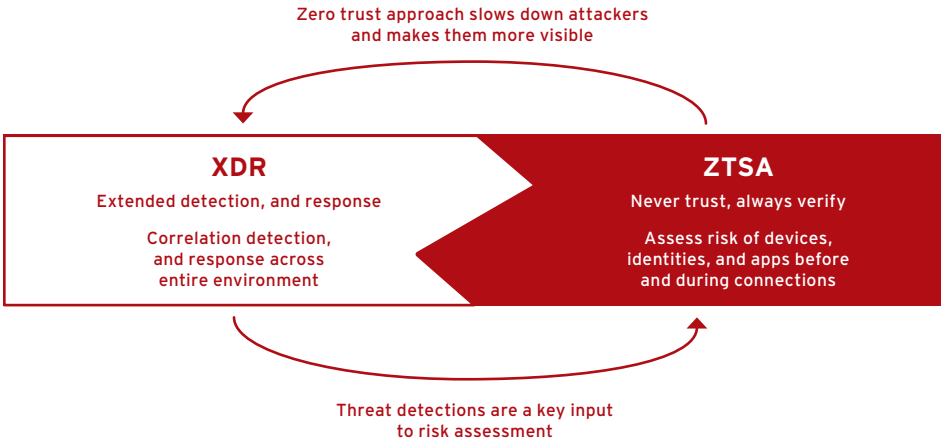


Figure 10: The connection between XDR and SSE using ZTSA



› Access platform trial