TREND MICRO

Trend Micro

TREND MICRO™ ZERO TRUST SECURE ACCESS

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.

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 evaluate the risk/security posture of the device before the connection is established.
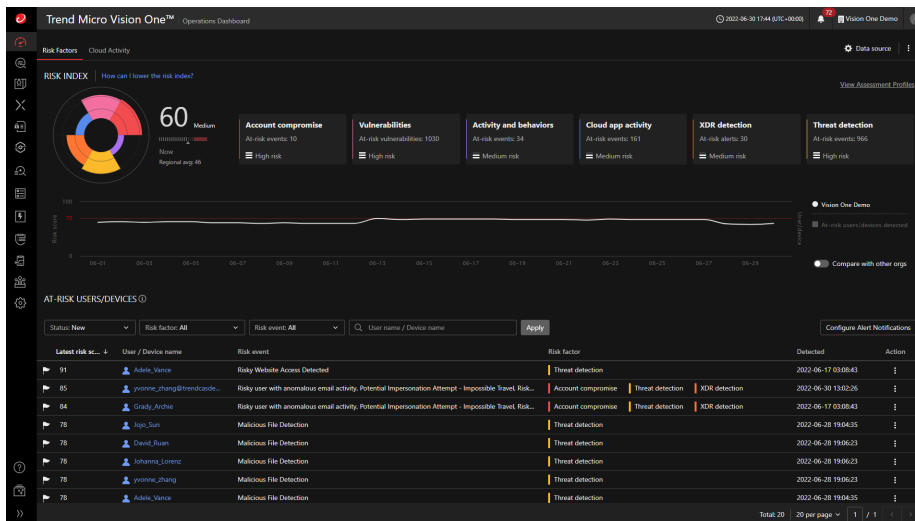
REVISING TRUST IN YOUR ORGANIZATION

In most organizations, implicit trust is the standard. This opens the organization to considerable risk, where a single compromised identity can begin to wreak havoc in the environment and largely move throughout the network unabated.
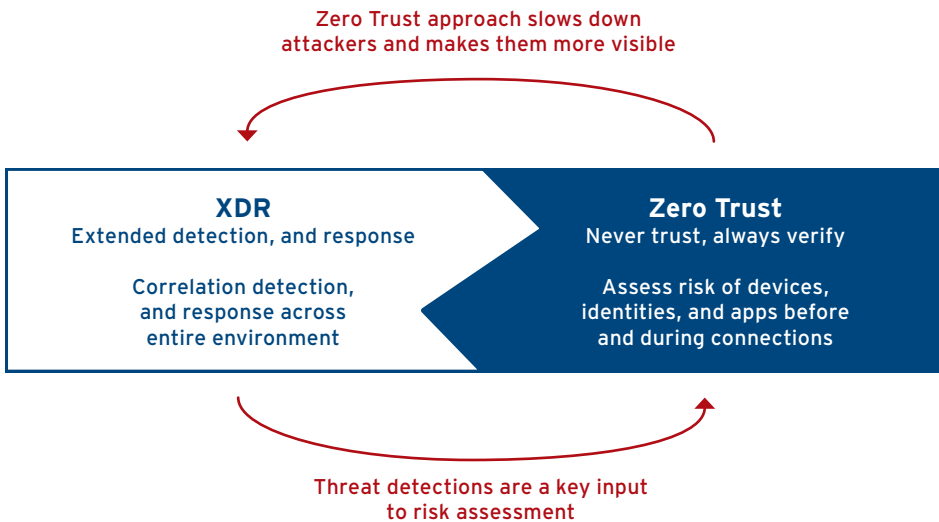
Much like digital transformation, the path toward Zero Trust is a journey, not a solution. There are a number of 'initial steps' that can be taken depending on the highest priority risk in your organization and your current security posture. While more use cases exist, which over time can be implemented as your organization moves towards Zero Trust architecture, the initial steps include:

1. **Securing access to the internet**

2. **Delivering fast and secure access to cloud applications**

3. **Transforming your remote access solution**

INTRODUCING TREND MICRO ZERO TRUST SECURE ACCESS

As part of Trend Micro Vision One™, Trend Micro Zero Trust Secure Access follows the principles of Zero Trust networking. This strengthens your overall security posture by enforcing strong access control permissions from multiple identity services across the organization.

Instead of granting access to the entire network, as a VPN does, Zero Trust 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.

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
Never trust, always verify

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

Threat detections are a key input to risk assessment

> "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

> "Among respondents with a broad zero trust initiative underway, 61% indicated they had begun to implement SASE."
>
> 2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG, published October 2021

SECURES ACCESS TO THE INTERNET

- Provides agent and agentless protection for secure web browsing and unsanctioned app access
- Presents highly contextualized data to Trend Micro 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 Micro Vision One
- Powered by Trend Micro™ Web Reputation Service, Trend Micro Research, and Trend Micro Vision One™ Risk Insights
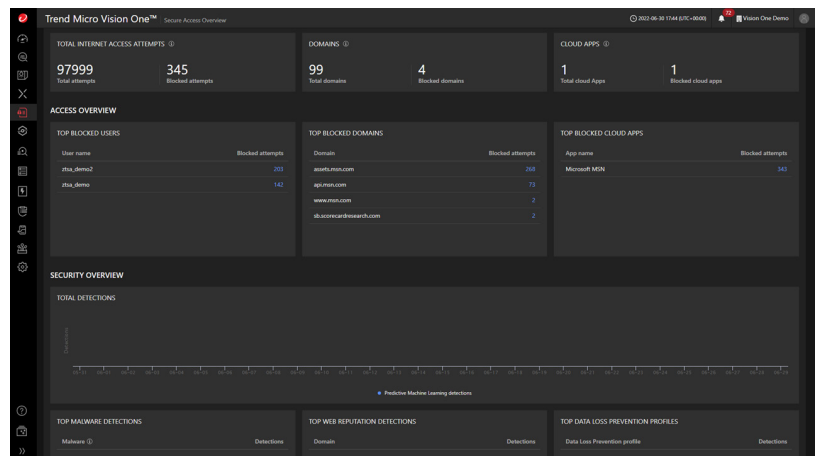
DELIVERS FAST AND SECURE ACCESS TO CLOUD APPLICATIONS

- Features agent and agentless protection to sanctioned software as a service (SaaS) apps
- Presents detection and activity reports into extended detection and response (XDR) for rapid response
- Delivers secure access to SaaS apps, checking for policy violations and security risks
- Powered by Trend Micro Vision One Risk Insights
- Provides a simple-to-manage interface, within Trend Micro Vision One
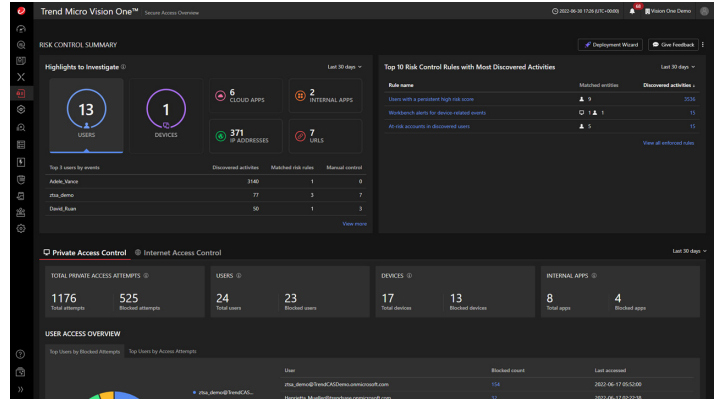
TRANSFORMS YOUR REMOTE ACCESS SOLUTION

- 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 Trend Micro Vision One Risk Insights
- Controls connections to apps and resources with continuous risk assessment – dynamically allowing and revoking access as risk profiles change
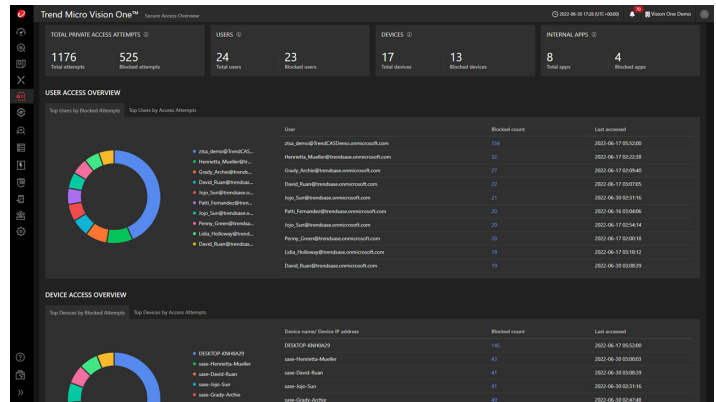
CONTINUOUS RISK ASSESSMENT

As we continue to measure cyber security 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 Vision One Risk Insights provides that function of continuous risk assessment for Zero Trust Secure Access.

At regular intervals and dynamically in real-time, risk rating data from Risk Insights 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.

TREND MICRO™
Securing Your Connected World