



**EBOOK**

# Prioritize Zero Trust for Better Cloud Security

Trend Micro and Amazon Web Services (AWS) Work Together to Enable a Zero Trust Approach

# Table of contents

What Is Zero Trust? .....3

The Vital Need for Zero Trust .....4

Trend Micro’s Perspective on Zero Trust.....5

If You Can’t See It, You Can’t Protect It.....6

Trend Micro’s Cyber Risk Index (CRI) .....7

Trend Micro in Cooperation with AWS .....8



# What is Zero Trust?

Businesses are always in need of the most robust security possible. As more organizations move to the cloud and given the new distributed, connect-from-anywhere approach to work, tighter security mechanisms are vital. Traditionally, enterprises have relied upon a specific perimeter security paradigm that trusts users and devices once authenticated, granting them access to the entire network while leaving enterprise assets vulnerable to cybercriminals.

In contrast, Zero Trust prompts enterprises to take into account identity, authentication, and other context indicators such as device state and health in order to make real and meaningful security improvements over the status quo. In an ideal world, Zero Trust is a security model where access to your computing resources and data are not granted solely based on network location. Levels of trust are clearly and continuously evaluated and amended in real time to enable secure access to enterprise resources. The Zero Trust architecture approach assumes that no connection, user, or asset is trustworthy until verified.

In fact, Zero Trust has gained such prominence that in May 2021, President Biden signed an [executive order](#) mandating that all federal agencies establish plans to drive adoption of Zero Trust architecture.<sup>1</sup> This has spurred organizations to speed up their adoption of Zero Trust principles. Now, the need for products that support Zero Trust is growing so fast that the global Zero Trust security market is expected to grow from \$27.4 billion in 2022 to \$60.7 billion by 2027.<sup>2</sup>

The National Institute of Standards and Technology (NIST) developed an entire Zero Trust architecture, detailed in [Special Publication 800-207](#), which defines Zero Trust as a set of cybersecurity principles when planning and implementing an enterprise architecture. It has become known as the gold standard of Zero Trust in the cybersecurity industry.

<sup>1</sup> The White House. "[Executive Order on Improving the Nation's Cybersecurity](#)." May 12, 2021.











<sup>2</sup> MarketsandMarkets. "[Zero Trust Security Market](#)." 2021.



# The Vital Need for Zero Trust

Organizations often begin their Zero Trust journey when faced with new security considerations as they move to the cloud. Migrating on-premises resources to the cloud entails monitoring a growing digital attack surface, which equals all possible entry points for unauthorized access into any system that is typically complex, massive, and constantly evolving.

## Potential Threat Entry Points

-  User accounts
-  Endpoints
-  Mobile devices
-  Domains and subdomains
-  Servers
-  Cloud workloads
-  Cloud containers
-  Cloud storage
-  Applications
-  IoT

Legacy security practices have proved difficult to scale and adapt to increasingly complex modern-day attacks that exploit distributed workforces, remote work, and bring-your-own-device policies for employees. For example, it can be complex to deploy role-based access control (RBAC) in the cloud to ensure employees access only information they need to do their jobs and are unable to access information that doesn't pertain to them. The once wildly popular virtual private network (VPN) approach is slowly declining due to the latency issue created when users have to move from their endpoint to the VPN and then to the cloud; with remote working now the norm, users want to access the cloud directly and quickly.

Zero Trust starts with a set of principles that each enterprise implements according to its business and security needs. While each organization's reason for adopting Zero Trust may be different, Zero Trust should always be viewed as an evolving concept and ongoing journey that leverages various products and solutions to keep organizations protected.



# Trend Micro's Perspective on Zero Trust

Trend Micro, an [Amazon Web Services](#) (AWS) Advanced Technology Partner, has an approach to Zero Trust that enforces and maps directly to NIST principles, again, believing that Zero Trust is a philosophy, not a single product. Trend Micro views it as an ongoing cadence where organizations continuously evaluate and manage risks and threats. While NIST lists security controls on which an enterprise can base their Zero Trust progress, technology needs to be put in place to implement such a posture. Security in the cloud age also requires policies that automate risk assessment in cloud environments because it's a vastly different scale of velocity.

To address the complexity of risk, the process needs to be treated like a lifecycle, in which continuous visibility and assessment are used to discover an organization's attack surface, assess the risk, and then mitigate the risk. Trend Micro advises customers to take Zero Trust implementation one step at a time.

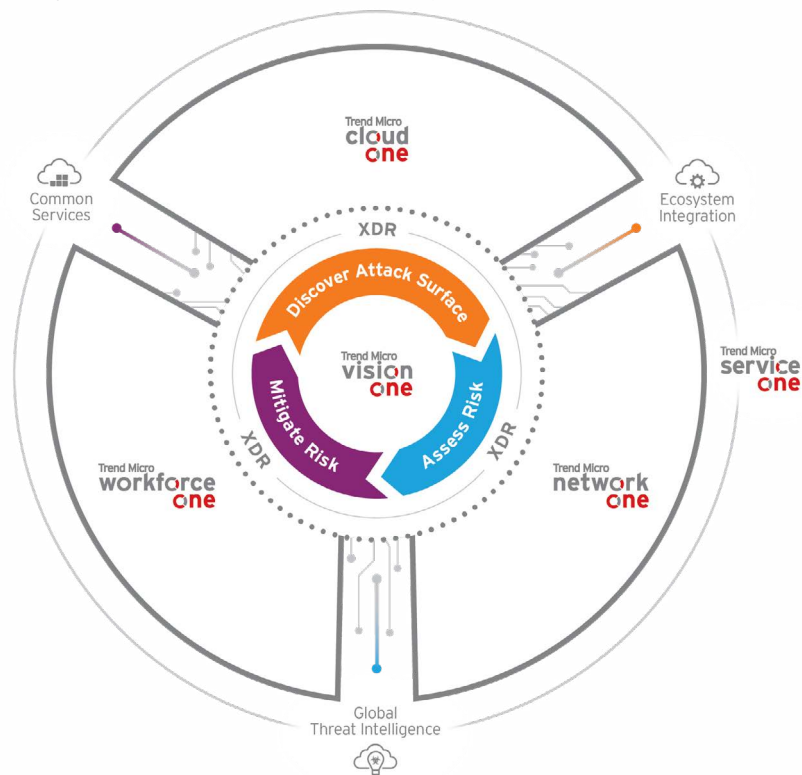
In practice, Trend Micro's Zero Trust posture could focus on helping an organization discover its attack surface on cloud workloads and then providing a list of common vulnerability exposures (CVE), typically endpoints that could be exploited. Or it might be helping with application access control. Or, drilling down, ensuring that a developer doesn't have access to an AWS resource in such a way that he or she could exploit a compromised account and take down the entire organization.



# If You Can't See It, You Can't Protect It

Often times, by implementing a Zero Trust posture, attackers are taken out of their comfort zone and perform in ways they normally wouldn't, which triggers an alert. This is when extended response and detection (XDR) comes into play, providing holistic protection against cyberattacks, unauthorized access, and misuse.

Trend Micro integrates XDR information into its Trend Micro One network solution, a unified cybersecurity platform that enables organizations to be resilient and understand, communicate, and mitigate cyber risk across the enterprise.



**Trend Micro One** enables business agility through the delivery of market-leading security capabilities for protecting multiple environments across the enterprise. It includes capabilities for:

- **Trend Micro Vision One™**, the core of Trend Micro One, gathers detailed telemetry from native sensors from all Trend Micro's protection layers as well as other data sources from across an enterprise, performing both big data analytics to power XDR and risk insights in support of risk assessment and a better security posture.
- **Trend Micro Cloud One™** protects cloud deployments with a security services platform for cloud builders.
- **Trend Micro Workforce One** secures users on any device, any application, and anywhere. It is a portfolio of products that can apply multiple layers of protection across endpoint, email, web, and SaaS applications to defend users regardless of device, application, network, or location.
- **Trend Micro Network One™** protects networks, including enterprise, remote, and industrial networks, by delivering powerful network security capabilities that detect the unknown and protect the unmanaged, including IT and OT resources.
- **Trend Micro Service One™** supports the entire platform, augmenting security teams with 24/7/365 managed detection and response, incident response, targeted attack detection, and expert support.

The platform is powered by common services (RBAC, security engines, etc.), global threat intelligence, and deep integration into the ecosystem to ensure Trend Micro fits into any organization's environment.

In essence, there is no one silver bullet for Zero Trust. It requires Trend Micro's far-ranging security solutions platform, AWS, and customers working in tandem.



## Trend Micro's Cyber Risk Index (CRI)

Trend Micro offers a well-known, comprehensive Cyber Risk Index (CRI) that helps assess where the gaps are in an organization's security posture so it can measure its progress toward implementing Zero Trust principles and, thus, its readiness to respond to different types of cyberattacks. The CRI's findings can help an organization thwart serious threats against data, applications, and IT infrastructure. Since risk score is calculated different ways by different companies, Trend Micro will measure it over time. That way, organizations can determine whether or not they are improving with Zero Trust and what additional steps to take.

The CRI assesses top risk factors across five key areas:

- Infrastructure risk
- Data risk
- Human capital risk
- Cyber risk
- Operational risk



# Trend Micro's Cyber Risk Index (CRI)

The CRI also shows an organization how it compares with its industry peers as well as regionally. Updated regularly, the CRI was created by Trend Micro Research and Ponemon Institute and surveys organizations globally to investigate their level of cyber risk, including North America, Europe, Asia-Pacific and Latin/South America.



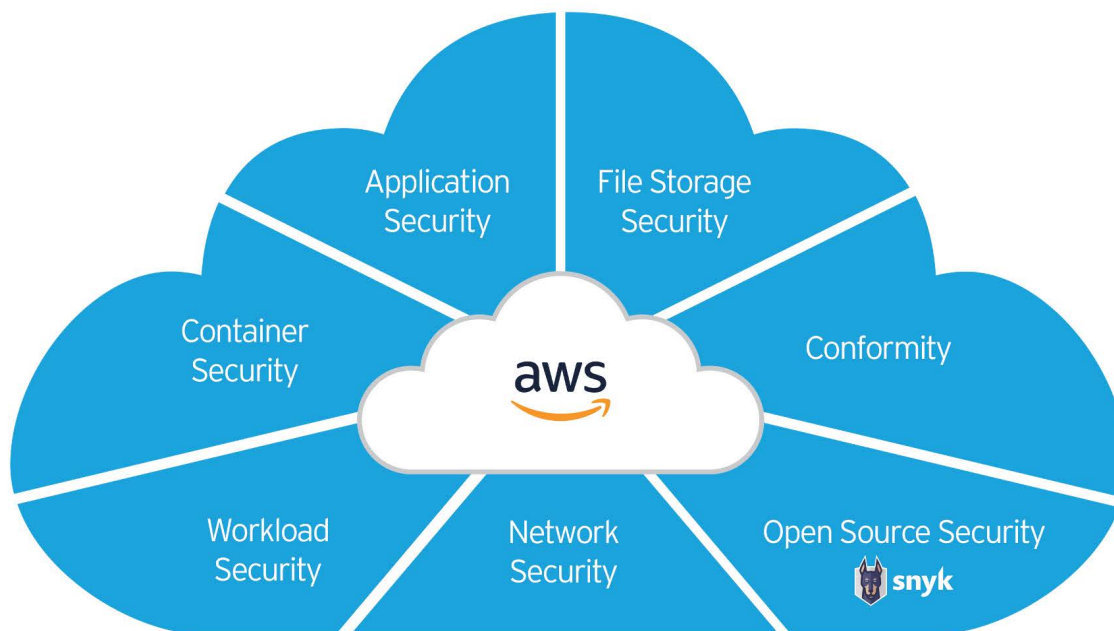




## Trend Micro and in Cooperation with AWS Partnership

Trend Micro has been an AWS advanced partner since 2012. With more than 15 AWS competencies and designations, Trend Micro continuously innovates jointly with AWS and AWS Marketplace to deliver leading cloud security solutions to support AWS customers. In fact, Trend Micro is rated [five stars by customers on AWS Marketplace](#).

Trend Micro and AWS share the same intense focus on satisfying customers, resulting in Trend Micro's track record of "firsts" with AWS. For example, AWS has released a number of products in concert with Trend Micro as a release partner. There is considerable alignment between the two development organizations. In fact, Trend Micro currently has more than 200 employees whose sole responsibility is to work with AWS.



### Talk to an expert now

Want to learn more? [Book a meeting with Trend Micro.](#)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Copyright © 2022 by Trend Micro Incorporated. All rights reserved.

Trend Micro, and the Trend Micro t-ball logo, Deep Security, Trend Micro Deep Security AntiVirus for VDI, Trend Micro Deep Security Virtual Patch, Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

