General Report

What is **Zero Trust?** *(Really)*

Written by Greg Young, VP Cybersecurity, Trend Micro
and William Malik, VP Infrastructure Strategies, Trend Micro

July 2023

Contents

Published by
Trend Micro

Written by
Greg Young and William Malik

1. How We Got Here

A decade in the making

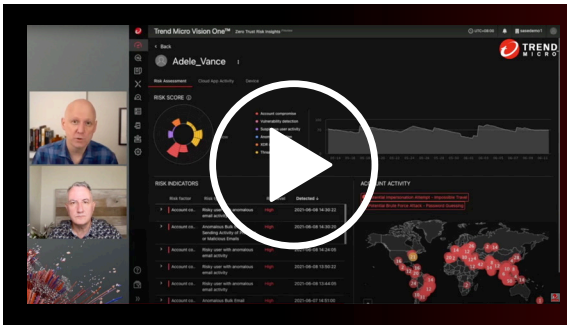
Although it can seem like zero trust (ZT) is a new evolution, the strategic approach and many factors driving it have been present since the early 2010s. IT and business have undergone transformative shifts, especially during the last decade, but security fundamentals have not. Cloud, increased digitalization, remote work, as-a-service solutions, and dozens of other shifts change how enterprises engage with technology. Security, instead, has attempted to increasingly scale the same approaches or add on narrow safeguards without any foundational change. New enterprise, old security.

Security has tried scaling old approaches

Networks started off as wide open. If you were in a virtual private network (VPN) or an office, you could typically access your network after providing a valid user ID and password. Security has attempted to scale this by carving the network up into increasingly smaller zones. However, this was just a method of scaling, or creating smaller "buckets", of the same basic fundamentals. This scaling, in turn, has introduced new challenges related to manageability and visibility, which paradoxically can create new opportunities for more advanced attackers. The Internet of Things (IoT) introduced a large number of semi-intelligent devices that needed to be trusted, while the use of shadow IT left organizations with less visibility into data usage and applications.

Identity

The fundamentals of identity and credentials have not changed. Scaling hasn't worked, with many identities and more complex password rules. Too many identities and continuous password resets hasn't worked out well. When an attacker compromises a user's credentials, they can then move laterally across the network, spreading ransomware, gaining additional privileges, or exfiltrating data for extortion or spying. One remedy was multi-factor authentication (MFA). MFA has increased credential strength in one regard, however the "multi" means that there is only a second channel of authentication. The trust is binary. You are trusted if you are authenticated, and nothing more. Trust is still only based on the credential authentication, and maybe some limited risk factor such as geolocation. And that trust is continuous until the next logout.



Gain important insight into Trend's industry perspective on zero trust

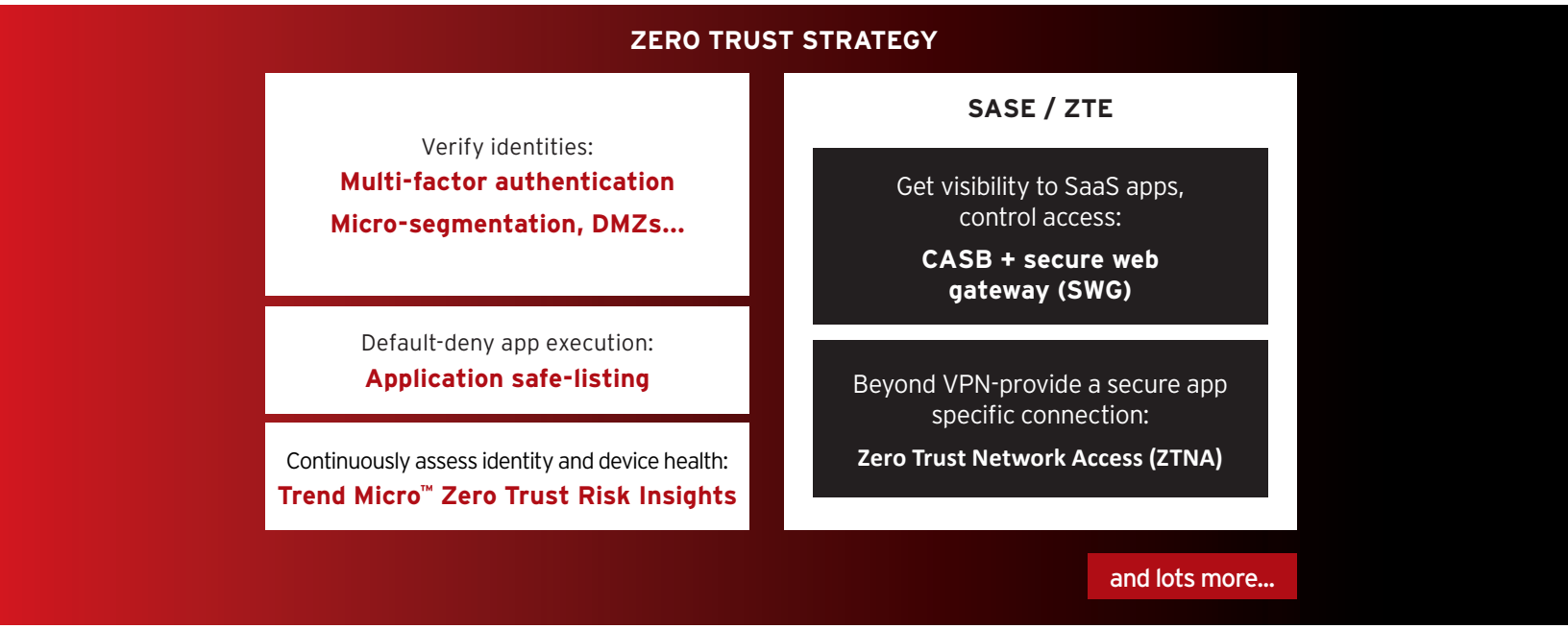
2. What is Zero Trust?

ZT is an architectural approach and goal built on a foundation of every transaction, entity, and identity being untrusted until some basis for that trust is established and maintained continuously. Getting to zero is the ultimate goal and it needs to be maintained with future infrastructure and business changes.

On this foundation, ZT initiatives have several widely identified pillars that specific sub-projects will help establish, including:

- Verifying identities
- Restricting network access
- Default-deny of application execution
- Visibility for continuous assessment

Many potential paths to zero trust...



Although each pillar can typically be connected to a common security task (for example, MFA for identity, microsegmentation for restricting network access, etc.), visibility for continuous assessment is the least discussed pillar yet the most critical. Without proper visibility, the overall level of ZT can slide back into complexity, wiping out all previous effort.

Across the pillars there are three key functions that are fundamental to ZT:

1. Posture 2. Continuous assessment 3. Assumed compromised

1. Posture is much like a person's health, as it is qualitative. It is granular and refers to the unique quality of all things and identities. Having ZT in an identity means that not only should the authentication take place, but the posture of that identity must be assessed. Pre-ZT identity health was infrequent or binary. Posture means assessing identities, devices, applications, and data usage for both potential and active risks. This is based on threat risks and detection and response findings. For an endpoint, a potential risk may come in the form of an unpatched vulnerability, while an active risk might be the detection of a suspicious lateral movement. For an identity, a potential risk may come from an incorrect assignment of admin privileges and an active threat activity may include suspicious login behavior or detection of phishing emails originating from this identity. As with personal health, one's security posture can change over time. How often the zero trust architecture requires a posture assessment should be risk-driven, given a solid baseline set of controls.

2. Continuous assessment, as opposed to a scheduled or intermittent evaluation, looks at all transactions. Network Admission Control (NAC) helped with this, but it was limited. ZT expands greatly on NAC concepts in terms of what is in scope for posture, where it applies, and the continuous nature. NAC is not equal to ZT because after the initial check on a limited number of criteria, trust was then granted thereafter. Rather than being a single chokepoint, a ZT architecture treats all access attempts as chokepoints, while all transactions are validated and all entities have a trusted posture. The frequency of these assessments should be driven by a risk assessment, while all elements (people, devices, entities on the network) must conform to the architecturally defined baseline.

3. Assumed compromised embodies the anti-ZT paradigm of "verify then trust." Although security operations center (SOC) teams often operate within this principle—before investigation begins—the assumption is that all is well in the architecture until an alert is issued. ZT means nothing should proceed until an "all clear" is established: an anti-alert. The assumption of compromise applies to all entities, including identities and credentials.

These three elements once again flip the security paradigm upside down: Visibility of these key elements with enforcement points drafted into the ZT architecture, while decisions to block and prevent are continuously made based on risk. Threats are stopped before they become attacks—before a SOC team investigates them. This leaves SOC teams free to investigate the most serious incidents, and gives operations teams a chance to remedy problems that led to denying or blocking the threat.

3. What Zero Trust Isn't

ZT isn't a standard or a certification. Yes, there is a NIST document regarding ZT, but it is a Special Publication (SP) and not a Federal Information Processing Standard (FIPS). NIST SP 800-207 is a valuable document and discusses the architecture level goals that are covered here. But there is no such thing as "certified NIST SP 800-207 compliant."

ZT isn't a product. Yes, products can form a part of your ZT architecture, but it can't be "bought by the pound." Implementing a microsegmentation product may be an effective strategy, but only if done with the goals and principles of your ZT architecture.

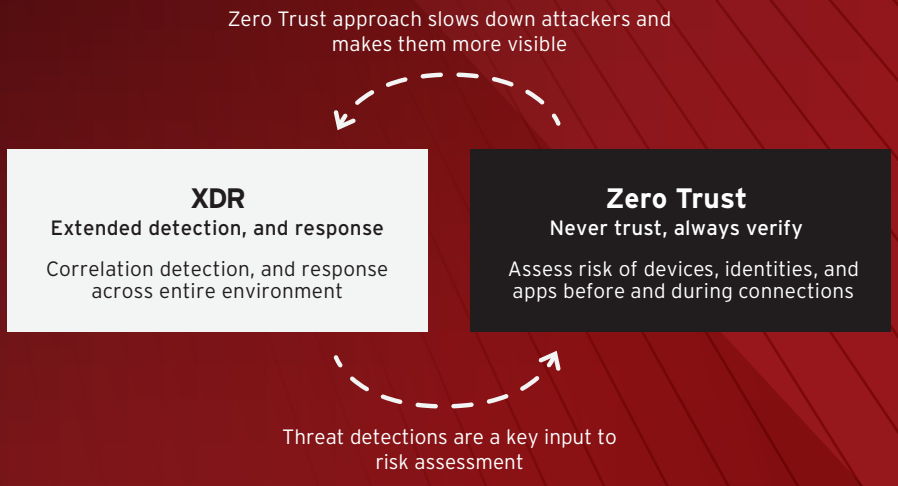
Vendors who are labeling unchanged legacy security products as ZT only add to the complexity of ZT. This "zero trust washing" attempts to capitalize on potential confusion regarding ZT and links it with the "buy by the pound" paradigm. Legacy products can be part of a ZT architecture, but they must be deployed specifically in a way to support the ZT goal. The greatest impact is having an overall ZT architecture that is progressively implemented and continuously enforced. The overall ZT implementation will be multi-year and likely incorporate multiple projects focused on specific pillars.

4. XDR and Zero Trust

Extended detection and response (XDR) is a new threat-focused security approach. An advancement and broadening of endpoint detection and response (EDR), XDR collects large volumes of telemetry across an organization's security data sources. This solution looks for clues across an organization's environment to see more and respond faster to attacks. XDR on its own is highly valuable in stopping threats, however it has usually been deployed to secure existing infrastructure, not immediately change it. SOC teams equipped with the resulting rich telemetry of XDR will often identify weaknesses in the organization's architecture, and CIO and CISO teams often respond with tactical changes to a non-ZT architecture. This has resulted in organizations having a high correlation between deploying XDR and implementing a ZT strategy.

XDR has two significant assets that can propel a ZT architecture: strong endpoint controls and organization-wide telemetry from across IT. A strongly secured endpoint provides a solid basis for trust establishment by providing the SOC with the knowledge that the endpoint is free from malware, what transactions it has engaged in, valuable information about its posture, and that a single agent is imbedded with ZT capabilities such as Zero Trust Network Access (ZTNA). The telemetry in the XDR data lake provides visibility, the most challenging ZT pillar to establish. This telemetry can give insight into the posture of elements beyond endpoints, especially across silos and the gaps between them that attackers usually exploit. ZT decisions can factor in XDR detections when granting access to resources, and this data provides an already-collected primary source for continuous assessment.

After using XDR to advance the architecture, ZT returns the favor by making XDR more effective. A strong security architecture makes it more difficult for attackers to move laterally or access resources, causing attackers to generate more noise and thus, can be easier to detect. ZT removes many architectural weaknesses that are usually exploited and detected and/or blocked by XDR. By eliminating a large amount of the vulnerabilities through better architecture thanks to ZT, XDR and the associated SOC staff can better focus on the most advanced attacks or portions of the organization that are furthest from achieving ZT.



5. Zero Trust Journey

Identity and access management (IAM)

IAM governs user identification. Users would prefer to not repeatedly authenticate themselves, so they ask for single sign-on. Administrators would like to deal with all the access rights and requests for an individual, so they ask for consolidated user administration. Those two disciplines together are the technical basis for IAM. An IAM project in itself is a substantial undertaking. This brief discussion of the key elements will help with planning.

Users—and key devices and services—should authenticate themselves to gain access to resources. To do so, it is important to map out the users requiring access to specific resources and provision them through the IAM service, with as much information regarding their use profile as appropriate. Sensitive resources should use MFA. In all cases any MFA tool is vastly superior to a single static password.

Privileged access management (PAM)

For truly sensitive resources, consider a PAM tool, such as those provided by CyberArk, BeyondTrust, or Thycotic. This adds logging of privileged account activity to robust authentication, allowing detailed forensic assessment in the event of a breach.

Passwords

Recently, the National Institute of Standards and Technology updated their password guidance. They performed a mathematical analysis of password strength and found that a longer password is far better than a password requiring a mix of special characters, numerals, and upper- and lowercase letters. The longer the password is, the stronger it is. Users find that long passwords consisting of a few familiar words are much easier to remember than an elaborate string of meaningless characters.

Frequent password changes are security theater, Bruce Schneier's phrase for actions that look good to the uninitiated but have no cybersecurity value. When a password is compromised the bad actors use it within hours. Changing the password every 90 days will have no impact of risk remediation. Use MFA instead of only a password.

Continuous health assessment

Maintaining the integrity of the IT environment is a core mission of information security. As part of that mission, the organization must monitor key elements for potential breaches and indicators of compromise (IoC).

6. Zero Trust Networking

Microsegmentation

Flat networks are a significant risk, as any malicious code could traverse the network unimpeded. Readying the network for ZT will require segmentation. The goal is to balance the degree of isolation among subnets with the complexity of managing the profiles for each sub-segment. It is important to understand the locality of data references across critical processes to develop zones and place a boundary around each zone, to limit unwanted traffic. There must be a balance between the vulnerability inherent in a flat network versus the resulting vulnerability from the complexity of managing hundreds of segment rule sets.

Isolate vulnerable technology

It is recommended to isolate all technology sharing a particular vulnerability, such as ICT devices with a fixed OS release which cannot be patched. As manufacturers of certain OT (operational technology) devices—such as industrial robots or medical equipment—typically build in a specific OS release, changing the release by patching or upgrading the software can void the warranty or decertify the device. These devices should be segregated with tight policy rules to minimize the possibility of intrusion.

Limiting external physical and remote access to sensitive zones is also suggested, as is building a DMZ to filter remote access from vendors or "as a service" products.

Instrument network segments

Subnets should be instrumented with information security tools to detect and stop malware—cryptomining, rogue encryption, data exfiltration, unauthorized programs, and malicious tools launching DDoS attacks or spam emails and messages. Correlate the alerts and logs for analysis and action via a consolidated console.

Collectively, these measures will define and secure your network topology.

Zero trust Network Access

As ZT architectures progressed, it was recognized that organizations often found themselves deploying certain recurring elements. This instilled less trust in communications at the edge for incoming VPN connections and outgoing requests to software as a service (SaaS), cloud workloads, and web server connections. Secure Access Service Edge (SASE) or Zero Trust Edge (ZTE) are two labels being applied to this family of services occurring at the edge, and which have grown increasingly challenging as employees have become increasingly mobile.

Pre-ZT we relied upon VPN, CASB (cloud access security broker), and SWG (secure web gateway) safeguards. But VPNs were limited and tended to terminate at the edge, connections after that were over-trusted, they were not able to mesh the security with software defined networks. SWGs didn't easily service remote employees, and CASBs were relatively static and trust was a fixed concept. Networks were increasingly software defined, entities were mobile, and security was fixed in stone. Unmanaged endpoints, unsanctioned SaaS, SD-WANs and the ramp-up of remote employees during COVID-19 applied pressure to pre-ZT security architectures and increased the need for SASE.

SASE falls inside the envelope of ZT and employs ZT principles for a specific segment of the organization. The third level in this solution is ZTNA, which is within the envelope of SASE and is the basis on which all other SASE security services lean on. As ZTNA is a smarter VPN that employs ZT principles, this initial connection can enable SWG and CASB to proceed with ZT enablement. While ZTNA connections support posture, continuous assessment, and assume compromise, the ZTNA connection should link the initiating entity with the target entity from end to end and be aware if entities and paths change. These changes would be due to their software defined nature; an employee now on the road connecting to a server that has been orchestrated elsewhere.

A request to connect to a SaaS application or a web request from a remote worker via ZTNA in SASE suddenly has greatly limited the risk surface. More about SASE and ZTNA are available here.

Note that these definitions are evolving.

https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

https://en.wikipedia.org/wiki/Secure_Access_Service_Edge

Zero trust networking implementation

The challenge with traditional VPNs is that it offers a simple solution that doesn't solve the complex, central problem. A VPN creates an encrypted path from a user's device to a firewall at the edge of a corporate network. All traffic traversing that path is encrypted. (Note that this only applies to a company-provided VPN—third-party VPNs encrypt traffic between the user's device and the third-party's firewall; after exiting there, the traffic proceeds, unencrypted, to its final destination.) This broad, general solution means that once connected, the user has access to everything behind the firewall. The VPN exists to create a perimeter.

If the user's machine contains malware, that malware can access everything behind the firewall, too. This is an illustration of the failure of the perimeter as a security concept.

ZTNA can replace the conventional VPN to establish a ZT environment, consider which resources rely on a firewall for protection, and map out alternative solutions providing greater granularity. For instance, rather than have all email reside on a server behind a firewall, you can secure each user's account with multifactor authentication and only allow authenticated users to access the email server.

Zero trust networking implementation

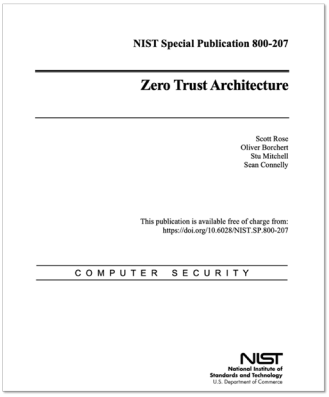
Most organizations' first discussions about zero trust are often about segmentation or identity. This is focused on the outcome, which makes sense, however it turns out that to get these outcomes there are precursor capabilities that are required: visibility and continuous monitoring. Attackers use lateral movement and neglected parts of the infrastructure because they know that visibility is normally centered only on parts of the infrastructure–they fear being detected. Like a locked door without an alarm or a camera on it, wide visibility and the associated telemetry must be in place for moving to zero trust. Additionally, that monitoring must be continuous. Infrequent scans do not translate to zero trust. Continuous monitoring means a nearly real time flow of telemetry being analyzed, unlike so many of the current security regimes today where assessments are made either on demand or in very long intervals, sometimes days. A VPN connection should not be allowed to continue if the risk profile of the endpoint, server or identity suddenly becomes a high risk. Additionally, that connection should be severed rather than only checking for risk on the next login attempt.

7. Zero Trust Frameworks

There are various approaches to understanding or describing ZT, however there are no certifications or practical standards. This can be frustrating as many domains in security have extensive ISO (International Organization for Standardization) standards and compliance frameworks. Frustration is added on top of confusion when it is intimated that products are "zero trust certified" or "are in compliance with the NIST (National Institute of Standards and Technology)." However, there are helpful frameworks and approaches to help understand and plan your ZT strategy.

NIST SP-800-207

The NIST special publication, "Zero Trust Architecture" describes the importance of ZT strategies and gives scenarios for how U.S. Federal Government programs are adapting to employing ZT and what kinds of technologies could be helpful. Unlike the FIPS (Federal Information Processing Standards), this is a special publication and not standard. It is intended to provide high-level guidance and discussion for the federal landscape.


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Analyst firm viewpoints

The high-level guidance from analysts is quite helpful when understanding the principles of ZT. Forrester, Gartner, IDC, ESG, and other analyst firms have, encouragingly, coalesced their ZT definitions and frameworks. There are not radical differences in their overall approaches, however there are some important and distinctive differences in the terminology—and especially scope of zero trust and related subdomains.

Gartner, Forrester, ESG, IDC, and most other firms are all using the term zero trust. To describe the combination of CASB, SWG, and more advanced VPN using zero trust principles, Gartner uses the term SASE (Secure Access Service Edge), and Forrester refers to it as ZTE (Zero Trust Edge). They all seem to agree that this can be used within a SD-WAN environment quite adeptly, however there are currently different opinions on whether SD-WAN and networking itself must be part of the security solution. It is most likely there will be agreement that the network is the target, and a more granular definition will arise that recognizes the role of SASE/ZTE as a part of defending SD-WAN and branch offices—but that the networking software and equipment need not be provided by the security vendor.

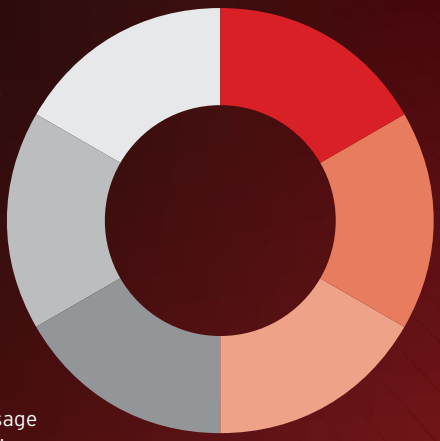
The bottom line is that the analyst firms provide valuable guidance, but they will not be prescribing a granular reference architecture or detailed standard model—your ZT and SASE/ZTE projects will be customized to your organization's needs.

8. How Can Trend Help with Your Zero Trust Journey?

Continuous health and posture assessment

To follow the ZT strategy, it is critical to continually assess the risk of identities, devices, applications, and data. This is achieved using telemetry from endpoints, email, directory services, XDR, and other sources. Within Trend Vision One™, the Zero Trust Risk Insights app helps decide how close the risk is to zero and prioritizes issues as well as tracks the organization's overall posture over time. This real-time risk assessment can be used to feed—via APIs—the automatic decision making in other ZT architecture components, including ZTNA, SASE, microsegmentation, and identity.

Factors used by Zero Trust Risk Insights to continually assess risk of users and devices



- **Threat detection**
  - High-risk website access
  - Known threats
  - Security policy violation
- **XDR detection**
  - Correlated threat data
- **Cloud app activity**
  - Unsanctioned cloud app usage
  - Cloud app risk level analysis
- **Account compromise**
  - Internal phishing
  - Credential dump
  - Suspicious user activity
- **Vulneravility detection**
  - Device with highly exploited CVE
  - Application with highly exploited CVE
- **Anomaly detection**
  - Unusual user/device activity
  - Anomalous web usage
  - Anomalous Microsoft-365 usage

Extended detection and response (XDR)

The XDR capabilities of Trend Vision One collect telemetry from endpoint, email, networks, and cloud to detect and respond faster to attacks. It uses cross-layer detection models to piece together the small clues related to attacker activity, giving organizations a graphical reply of events and multiple response actions. Optional managed detection and response service (Trend Micro™ Managed XDR) provides expert threat identification and investigation.

Strong endpoint and hybrid cloud workload controls

Core to protecting devices and hybrid cloud workloads are robust endpoint security. Products include application control to allow only the use of trusted applications, unknown malware protection, intrusion prevention system (IPS), and more. A single endpoint agent can be used for protection, for EDR/XDR, and to deliver telemetry and risk information to Zero Trust Risk Insights. In the future, it will also include ZTNA and SASE agent functionality.

Network controls for on-premises, IoT, and cloud

As a foundational item, network security can help segment and protect networks. Optimized products secure on-premises, Internet of Things (IoT), or cloud environments. Using leading vulnerability research from the Trend Micro™ Zero Day Initiative™ (ZDI), cybersecurity solutions can protect against undisclosed threats months before a vendor patch is available.

Cloud security

A broad collection of cloud controls are available to help achieve ZT. In addition to the previously mentioned cloud workload and cloud network security protection, security for containers, cloud file storage, applications, and open-source vulnerabilities are available alongside cloud security posture management.

SASE solutions

Trend Micro™ Zero Trust Secure Access enables secure connections between users and private and public applications. It uses CASB and ZTNA capabilities to automatically block connections based on machine learning, your custom policies, and the risk scores from Zero Trust Risk Insights.

9. Conclusion

Over the last decade, cybersecurity has been focused on the challenge of securing increasingly vulnerable and complex architectures. The industry has made great advances in spotting and blocking attackers, but much like a firefighter battling a blaze in a building built without fire retardant materials, the inherent security design of our IT infrastructure needs to change if we are to significantly reverse the war against attackers. ZT provides more inherent security and lower risk, multiplying the effect of security investments and activities.

These ZT initiatives are not interdependent. That is, you will improve your ZT posture by improving each of these elements independently. From an architectural perspective, the end state is similar; but from a deployment perspective, it does not matter which initiative you start with, or which order you perform them in. Let your organization's risk assessment drive the priorities for each.