tripwire

WHITE PAPER

A Tripwire Zero Trust Reference Architecture

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The concept of Zero Trust Architecture is fairly straightforward. Networks and systems have been traditionally designed with the assumption that everybody inside a defined perimeter can be trusted and that everybody outside that perimeter is hostile. With that assumption, the idea of building an impenetrable wall around that perimeter makes perfect sense. Over time, and as technology has advanced, the assumption that there's a clear, defined perimeter has eroded. Zero trust is access control for the modern enterprise, built around the principle that trust must be continuously verified. Every person, device, or entity in a zero trust system is treated as hostile until their trustworthiness has been verified for the specific action or connection in question.

At its most basic level, zero trust shifts the basis of trustworthiness from one's place in the network to one's posture relative to a trusted state, and assumes the possibility of frequent changes eroding a previously-checked status such that continuous re-validation is necessary. In other words, the only way to maintain trustworthiness is to continually assess posture against a known, trusted state, and to monitor changes to ensure the integrity of that person, device, or entity. Security is based on trust, and trust is based on integrity.

Much of the technology for zero trust isn't new; it's the aggregation and use of the technology that ultimately creates a zero trust architecture. In practice, zero trust implementations vary greatly. This paper will briefly explore three evolutionary examples of a zero trust architecture, and then outline a reference architecture for Tripwire controls utilized within zero trust.

Basic Network Access Control

While a complete zero trust architecture considers verifying trust at multiple levels, the most basic, and earliest, approach is to apply enforcement at the network. The foundational technology for this approach is Network Access Control (NAC). Early versions of NAC were very capable at enforcement, but provided relatively little depth in terms of validation. Modern NAC, as part of zero trust, offers the ability to limit access to the network based on risks such as identity, vulnerability risk, and configuration.

NAC is important because it addresses the erosion of the network perimeter. If your network no longer has a "hard shell" keeping attackers firmly on the outside, then the process for validating access needs to adapt. Using NAC to validate every connection to the network, regardless of where they're coming from, is a strong first step towards zero trust.

Micro-Segmentation

While network access control provides a response to the eroding perimeter, it doesn't fully eliminate the network attack surface. Once an attacker compromises an asset with access to the network, they are able to move freely throughout the portion of the network to which that asset has access. The attacker now has access to highly valuable targets. Micro-segmentation is a response to this threat model. By segmenting and isolating workloads, organizations can secure them individually, according to their sensitivity,

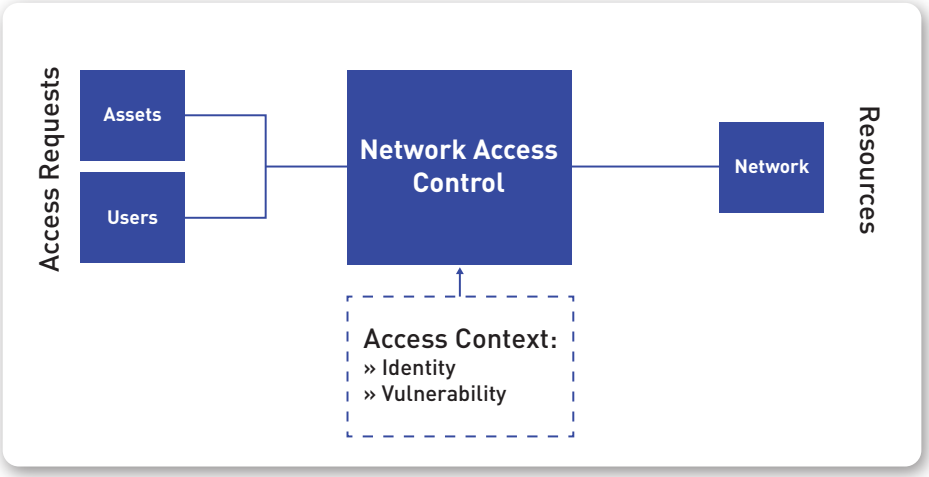

Fig. 1 Network Access Control

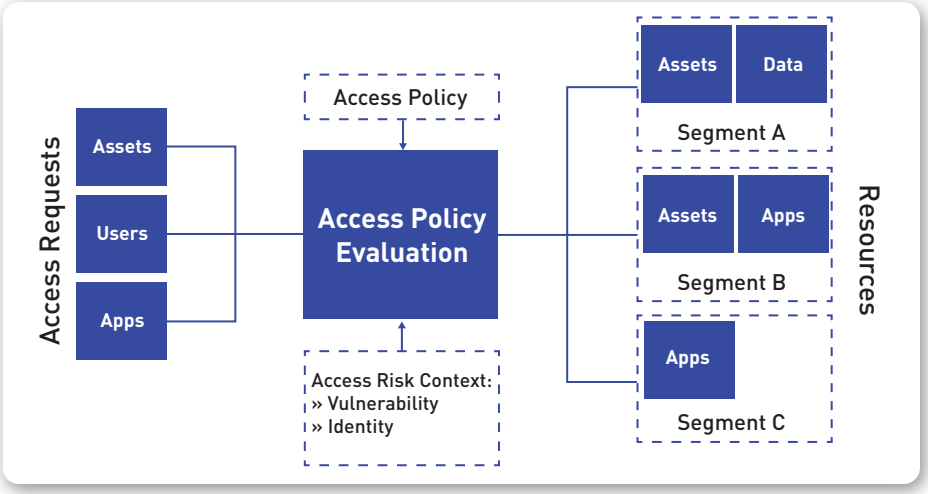

Fig. 2 Micro-segmentation

compliance requirements, or simply a principle of least privilege. Micro-segmentation generally introduces the concept of using policy to make access decisions as well, which is an important aspect of zero trust.

In Figure 2, the devices authenticating to the network are limited by policy to only specific zones or systems. Their ability to access other assets in the environment is limited at the network layer.

Micro-segmentation provides significant advantages over basic network access control, but it's still, ultimately, a control applied at the network layer. Limitations are ultimately placed on how network traffic can flow, leaving room for risk.

Trust Policy

The final architectural improvement that zero trust employs is a Trust Policy Engine. While the authentication checks done at the network will eliminate some threats, this evaluation does little to establish a durable trust. Trust and risk are, after all, opposite sides of the same coin. If you are risky, you are not trustworthy. So, in order to verify trust, we must measure risk.

Every possible attack vector that a hacker can exploit represents a risk vector. In an ideal world, one would measure every new communication for every form of risk, an approach which is generally not practical.

What is possible is to use existing security posture management tools to measure risk. Vulnerability assessment, configuration, unauthorized change, malware, and user behavior are a few.

When a connection is requested, both ends of the connection are evaluated for trustworthiness. Each of the assets involved will be presented a trust score for their proposed partner. Each asset will have a policy that states what kind and volume of risk they are willing to accept. If the partner is judged to be too risky, the connection request is rejected.

As an example, a device that has a non-compliant configuration, unpatched vulnerabilities, and has not had a malware check recently will have a higher risk score. This may be of little consequence if a PC is trying to communicate with a fax server (resulting in a lax policy requirement) but may be very important if a PC were trying to access customer databases or other sensitive information. The result would be that the customer database would have a policy with stricter risk requirements.

In Figure 3, a policy evaluation engine evaluates the risk scores of the devices that have been proposed to communicate.

Tripwire Controls in a Zero Trust System

The controls that are provided through Tripwire's products can play a key role in creating a robust zero trust system. Whether monitoring the security and compliance posture of entities requesting access or assets being accessed, Tripwire provides robust data to validate trustworthiness.

Security Configuration Assessment

One of the key components for determining the trustworthiness of either the entity requesting access or the resource to which access is being requested, is security configuration. If an asset is configured securely and according to policy, then the risk of interacting with that asset is well understood and appropriate risk-based access decisions can be made by the trust policy engine that's enforcing zero trust. Tripwire® Enterprise provides the broadest combination of platforms and policies for security configuration assessment, giving organizations the ability to determine how their assets are configured. This assessment of security policy is available for integration via APIs and apps connected to Tripwire Enterprise. Summary data about compliance to a policy and detailed data about specific configuration elements are available for making access decisions. Tripwire Configuration Manager provides assessment of cloud infrastructure such as cloud accounts, storage, and SaaSes, allowing for zero trust to extend beyond on-premise assets.

Policy Compliance

In addition to specific security posture requirements, some resources may be in scope for compliance standards. Zero trust policy can enforce compliance standards on entities accessing those resources. Tripwire can provide compliance assessment results to inform trust policy decision making. For example, assets connecting into a cardholder data environment can be allowed or denied

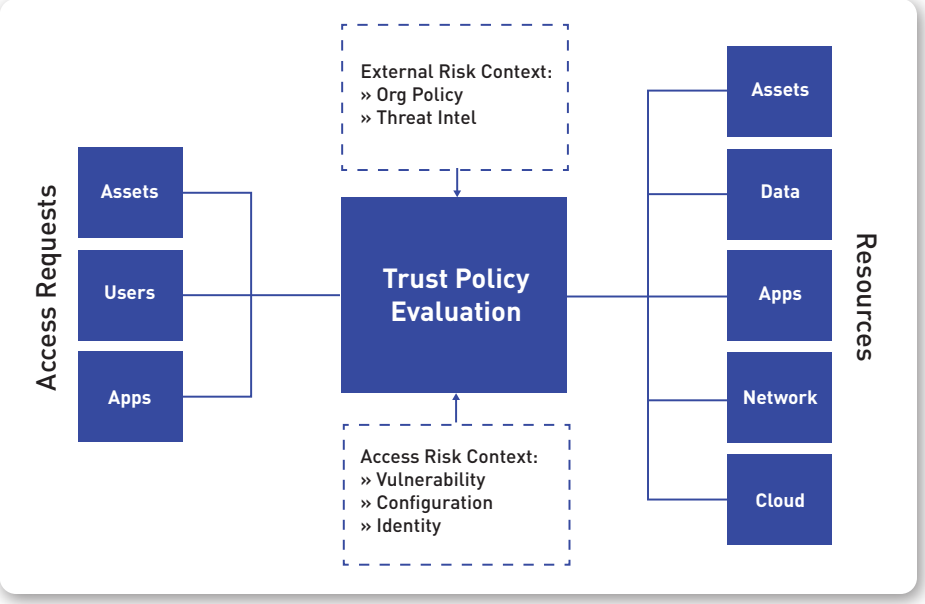

Fig. 3 Trust Policy

based on their own compliance with the PCI Data Security Standard. Where it can be difficult to assign a static asset scope to a compliance requirement, zero trust using compliance results from Tripwire can provide assurance that all entities involved in a particular system are compliant. Compliance assessment and file integrity monitoring are provided by Tripwire Enterprise.

Vulnerability Assessment

Tripwire IP360™ provides both agentless and agent-based vulnerability assessment across a variety of asset types, including servers, workstations, network devices, containers, and cloud workloads. Assessment includes vulnerabilities in the operating systems and applications on these devices. Tripwire IP360 results are applicable to both access requesters and resources in a zero trust architecture. Tripwire IP360 provides results in a robust REST API, including vulnerability details, CVSS scores, Tripwire Vulnerability Score, and other attributes. A zero trust policy might specify, for example, that assets with vulnerabilities providing remote privilege access should not be able to connect to specific data sets. Or, the policy might specify vulnerability score thresholds for access to specific sets of resources. Alternatively, company executives might be prevented from accessing resources that exhibit too much vulnerability risk. The granularity of risk data provided by Tripwire IP360 can support increasingly granular trust policies.

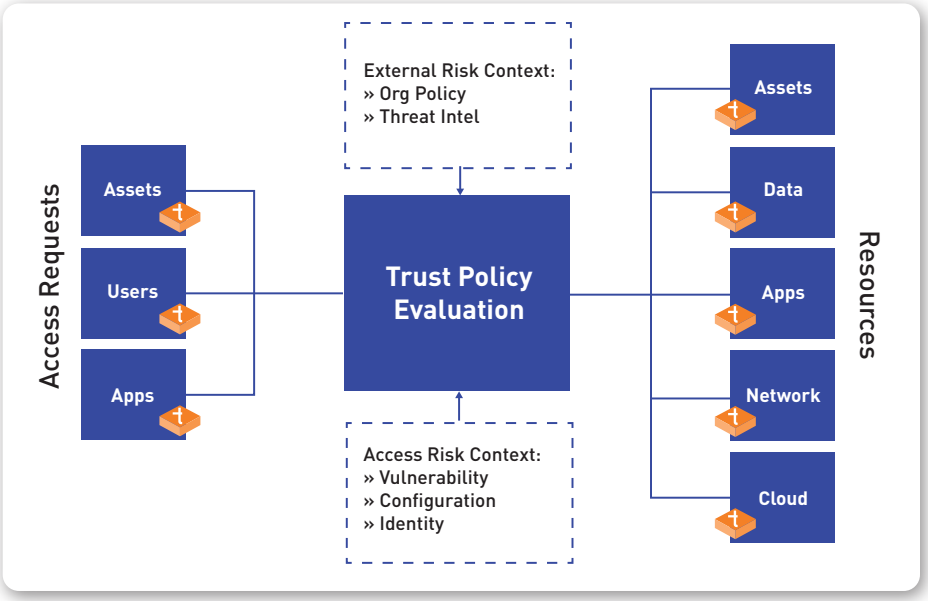

Fig. 4 Tripwire Controls in zero trust

Integrity Monitoring

While point-in-time assessment of security configuration, policy compliance, and vulnerability risk are key components of a zero trust architecture, they represent a methodology that leaves gaps for attackers to exploit. Integrity monitoring is the process of establishing a baseline state for an object, then monitoring that object for deviations from that baseline state. In the example of security configuration, that would mean establishing a baseline configuration and then monitoring that configuration for changes. By implementing integrity monitoring in a zero trust architecture, organizations can identify and address risk proactively, before the trust policy engine needs to make a decision about access. Additionally, integrity monitoring applies to the zero trust infrastructure itself. A change in the configuration of the zero trust policy, the policy engine, or any of the supporting components can change how zero trust is being enforced. Change is a constant in any IT infrastructure, and without integrity monitoring, even a perfectly configured zero trust system will drift and create unacceptable risk over time.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPTZTRA1a 2109