EBOOK #3

The Where of the World

The current state of Zero Trust technology

GUIDEPOINT
SECURITY

The Where of the World

The current state of Zero Trust technology

Much progress has been made in positioning technology and tools to support Zero Trust implementations. But there is still further to go before end-to-end Zero Trust can be enforced.

New ideas to improve the ability to detect and respond to cyber security incidents have been introduced, which are critical to improving overall security posture. Due to the variety of vendor solutions organizations have deployed across various infrastructure layers, current orchestration capabilities will need to mature, as this will play the most critical role in end-to-end Zero Trust implementation. In a true Zero Trust Architecture, multiple infrastructure layers will need to share risk information with policy enforcement points to allow enforcement of real-time dynamic access policies, which will require orchestration to pull contextual information from every relevant infrastructure layer. In the end, this means that standards must be developed to create a common understanding and interpretation of risk scoring, so that various vendors' solutions can share security posture and trust-related information for making access decisions with policy enforcement points. These distributed risk evaluation and orchestration capabilities will continue to mature and develop over the next few years.

In addition, existing standards such as SAML 2.0 and OIDC will likely change, as they currently do not provide provisions for inserting contextual information outside of user identity information. For example, SAML 2.0 does not have a provision for including endpoint health information in the SAML assertion.

Preparing for Blast-Off

Get started

As technology capabilities continue to evolve, organizations need to focus on the following key aspects to position them for the journey to implement Zero Trust Architecture:

KNOW AND MANAGE YOUR USERS

Implement automated Identity Governance and Privileged Access Management capabilities first. They are key foundations.

KNOW AND MANAGE YOUR CRITICAL INFORMATION ASSETS

Implement a robust asset management capability. Define associated processes to catalog the most critical information assets that need to be protected, including an inventory of the APIs in the environment that share critical information.

BUILD OUT FOUNDATIONAL CAPABILITY AND AUTOMATE PROCESSES AT EACH LAYER OF INFRASTRUCTURE

There are many existing capabilities that will improve security posture on your journey to Zero Trust, such as MFA, EDR, XDR, and SASE.

START EDUCATING YOUR BUSINESS ON THE BENEFITS OF A ZERO TRUST APPROACH

Explain the benefits of a Zero Trust Architecture to your business. Get executive buy-in.

START IDENTIFYING USE CASES FOR PILOT IMPLEMENTATION

Zero trust principles will need to be implemented on a case-by-case basis. Focus on protecting the most critical information assets. Partner with your business to identify those use cases.

RE-EVALUATE AND UPDATE YOUR SECURITY POLICIES

Zero trust approaches will likely make enforcement of various access controls more streamlined and may remove exceptions.

Equip Your Starship

Technology recommendations

As technologies evolve and new standards for interoperability emerge, organizations should keep the following considerations in mind during ongoing developments and maturity in vendor offerings.

TAKE AN AGILE APPROACH

As orchestration and authorization capabilities improve, SaaS solutions will scale better than on-premise offerings. Think about using cloud solutions for access management. Adding threat intelligence feeds for your network and endpoint will provide quick access to new capabilities as vendors offer more ongoing maturity and interoperability.

LOOK OUT FOR CHANGES TO EXISTING STANDARDS

Some existing standards such as SAML 2.0 will likely go through changes to introduce additional contexts, such as endpoint health, in access decision making for federated connections.

FOCUS ON API-BASED INTEGRATIONS

No single technology solution will handle a complete Zero Trust implementation. End-to-end Zero Trust implementation requires information sharing between multiple solutions to gather context from different parts of the infrastructure for access-related decision-making. The solutions deployed must have a robust API to facilitate sharing of information with policy enforcement points for continuous, real-time enforcement of access decisions.

BALANCE SECURITY, USABILITY, AND COST-EFFECTIVENESS

Not all use cases will require the implementation of Zero Trust principles. Zero Trust implementations must be evaluated based on the criticality of information assets and the access scenarios for each. Evaluating suitable use cases for implementation of Zero Trust principles will be critical to get business buy-in.

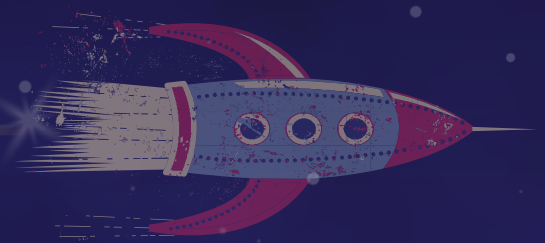
THINK ABOUT USER FRICTION

As Zero Trust principles are implemented, it will likely have an impact on the end-user experience and may even cause pushback. The changes in user experience must be thoroughly evaluated before making changes to how access decisions are made. The key to success for Zero Trust adoption will be reduced friction for business users as the transition takes place.

And finally...

...remember that no single solution will address all use cases for Zero Trust. Any steps taken towards implementing Zero Trust must be able to co-exist with other solution providers. Organizations must focus on automating various business processes and introduce foundational capabilities to position themselves for success in the implementation of a Zero Trust model. As the cybersecurity technology landscape continues to evolve toward Zero Trust frameworks and methodologies, it is critical that organizations stay on top of ongoing advances and evaluate new capabilities for incremental coverage of Zero Trust use cases.

Get started on Zero Trust adoption today with the help of GuidePoint Security. Take a look at the comprehensive consulting Zero Trust workshops or contact us for more information.



GUIDEPOINT
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
06.2022