tenable

SOLUTIONS OVERVIEW

RETHINKING YOUR SECURITY WITH A ZERO TRUST APPROACH

Zero Trust is more than just the newest buzz phrase. It's a strategy for implementing cybersecurity in a business world without perimeters. The sudden increase in remote working has added layers of complexity, with users and data operating outside of traditional IT defenses. The attack surface can no longer be defined by a logical perimeter.

Organizations with increasingly complex infrastructures are turning to Zero Trust as a model for controlling and securing their networks, applications and users.

Traditional perimeters no longer exist

With the rise of cloud services and the remote workforce, traditional perimeter security is dead and the attack surface is expanding. Frequently, cybercriminals are able to log into your network simply using weak, stolen or otherwise compromised credentials. Once inside, they expand their attack and move laterally across the network trying to gain access to the organization's most critical and sensitive data. As such, perimeter-based security models that assume if an asset, user or application is on your network it is "secure and compliant" are no longer adequate and provide limited protection against identity and credential-based threats.

Never trust. Always verify.

Zero Trust security is not a product or solution. It is a broader strategy for modern security that adapts to the complexity of today's business environment. Zero Trust assumes that untrusted actors already exist both inside and outside of your network and follows the mantra "Never trust, always verify". It replaces the belief that everything behind the corporate firewall is safe, and instead assumes that users, assets and applications are breached and should not be trusted regardless of where they are located, or what resources they have access to. Zero Trust requires that organizations continuously monitor and validate assets to understand how they move around, their interdependencies, level of access and how they interact with the network in order to spot anomalies and suspicious behavior.

DISRUPT ATTACK PATHS AND START YOUR ZERO TRUST JOURNEY WITH TENABLE

- **Prevent Identity-Based Vulnerabilities**
  Identify misconfigurations and vulnerabilities on your network, including Active Directory, and get recommended fixes for each issue
- **Catch Every Change in AD**
  24/7 automatic analysis of AD modifications to spot attacks and risky behavior
- **Monitor and Evaluate Users' Rights**
  Deliver built-in controls to enforce least-privilege on your users' identities
- **Disrupt Attack Paths**
  Prevent lateral movement by detecting privilege escalation and trust rights abuse
- **Gain Full Visibility into Your Assets and Vulnerabilities**
  Continuously assess all assets- including IT, cloud resources, OT devices and remote endpoints- to understand their security posture
- **Incorporate Asset Criticality**
  Automatically calculate the business criticality of your assets based on device type, capabilities and importance to the organization
- **Establish a solid foundation**
  Get full and continuous visibility into all assets and their vulnerabilities

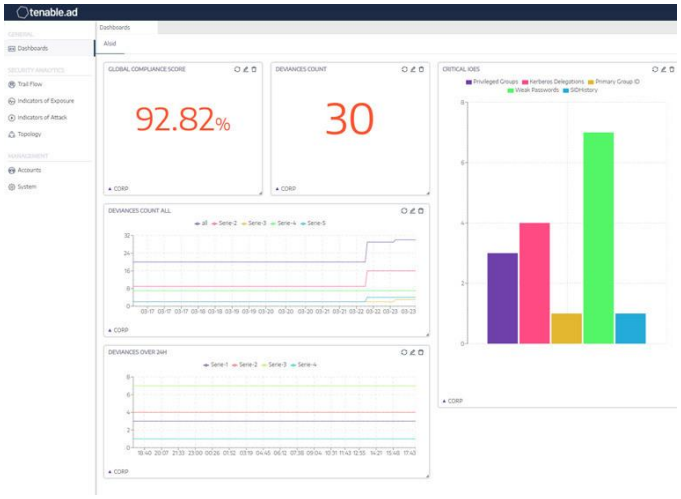
Tenable Helps you Evolve Risk-Based VM to Support Zero Trust

Zero Trust is a powerful security model designed to prevent breaches and limit internal lateral movement by threat actors. With the traditional network perimeter disappearing, you need to validate users' rights, detect lateral movement and employ foundational cyber hygiene as critical components to achieving Zero Trust security. Tenable solutions play an integral part in your Zero Trust Architecture from Risk-based Vulnerability Management to ensure complete visibility, continuous monitoring and vulnerability prioritization to Active Directory security to disrupt attack paths and monitor for risky user behavior.

Active Directory is at the center of trust

With a trust no one, validate everything approach, Zero Trust security relies on the systematic and continuous evaluation of users and their permissions. Active Directory (AD) is a fundamental tool used to achieve Zero Trust security by enabling the evaluation of users' rights. Therefore, it's critical that organizations track and alert on asset state changes and evolutions, and continuously detect lateral movement and privilege escalation. With Tenable.ad organizations can:

- Evaluate users rights with built in control to enforce least privileges on identities
- Track asset state evolution and alert on changes made to an Active Directory asset
- Detect lateral movement with built in detection of privilege escalation and right abuse
- Continuously monitor for risky user activities that could indicate a compromise



Trust is just another type of vulnerability

Just as software vulnerabilities are routinely exploited in cyber attacks, trust is no different in perimeter-based defenses. Attackers frequently exploit privileges and trust to perform lateral movement as part of the attack path. While identity and access management technologies are essential for enabling Zero Trust security, it's critical that those platforms are themselves secure and hardened. With Tenable, you can:

- Find weaknesses in AD before attackers can exploit them and get recommended fixes for each issue
- Dynamically monitor user databases, like Active Directory, for misconfigurations and lateral movements
- Audit and assess every configuration setting and entry relationship with Active Directory
- Assess all assets for vulnerabilities, misconfigurations and missing updates and prioritize patching to decrease the likelihood of compromise

Trust is dependent on asset state

Gaining visibility into all assets and exposures is foundational for developing Zero Trust policies and enforcement. Zero Trust builds off of risk-based VM practices, such as performing continuous discovery and assessment of assets, defining asset criticality, and implementing risk-based prioritization, as key inputs in determining whether to grant, restrict or deny access to resources. Using Tenable.io or Tenable.sc organizations can:

- Identify and continuously monitor all assets and exposures on your network, from IT and cloud devices, to remote worker endpoints and OT devices
- Remediate like there is no perimeter with vulnerability prioritization based on risk
- Identify critical assets and ensure they have the highest level of protection and monitoring
- Establish a variety of preventative measures such as two factor authentication, identity and access management and encryption

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

For More Information: Please visit **tenable.com/solutions/zero-trust**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**

tenable®