tenable | Data Sheet

Identity Exposure

Essential security for identity exposure

Identities are the new perimeter - compromised identities are at the center of nearly every successful cybersecurity attack. Active Directory and Entra ID are common targets for attackers who can achieve domain domination by using off-the-shelf tools to exploit the complex relationships between objects, permissions and entities.

The constant changes in directory services also limit visibility into the entire attack surface and continually introduce new attack pathways. Few security teams have enough visibility and context to secure the large attack surface of directory services, and the tools they often use only provide a snapshot in time, making security a moving target.

Worst yet, according to IBM’s 2022 Cost of a Data Breach Report, the average time to discover a breach involving compromised credentials is 243 days and the average time to contain it is 84 days. That means a successful attacker may have nearly a year to disrupt the most critical service in the modern enterprise.

Tenable Identity Exposure is an agentless security solution that delivers end-to-end protection against identity-based attacks. It continually validates the security posture of your directory services and instantly alerts you when your directory services are under attack. Tenable Identity Exposure also provides prioritized step-by-step mitigation guidance, ranks your riskiest identities by a risk score, and provides attack path visualization. By isolating and eradicating identity security gaps, Tenable Identity Exposure strengthens your overall security posture for an identity-intelligent enterprise.

Key benefits

- **Predict and prioritize**
  Rank each identity with a risk score to discover where your riskiest identities reside and prioritize remediation where it matters most.
- **Comprehensive visibility**
  Look deeper, evaluating all your human and machine identities and prioritizing preventive security with risk scoring to discover where your riskiest identities reside. Visualize complex domain and forest relationships.
- **Visualize attack paths**
  Eliminate attack paths with real-time mapping of paths that lead to domain domination.
- **Agentless**
  Get instant results with quick, frictionless deployment that requires no agents and no administrative privileges.
- **Instant attack detection**
  Real-time attack detection with MITRE ATT&CK framework mapping. Full SIEM and SOAR integration.

Key capabilities

- **Identity unification and risk prioritization**
  Break down enterprise identity siloes and unify all identities across Active Directory, hybrid and Entra ID to reveal your identity reality. Gain control of identities dispersed between multiple directory services, domains and forests in one place. Prioritize remediation with our data science-backed identity risk score that ranks identities by level of risk to the environment. Optimize team efficiency and focus efforts on business risk mitigation and preventing attacks.

- **Continuously validate directory services security in real-time**
  Assess the security posture of your directory services and uncover longstanding configuration and permission issues that make identities a central part of most attacks. Tenable Identity Exposure provides a step-by-step tactical guide that identifies affected objects, eliminating the need for time-consuming manual reports or scripts.

- **Eliminate attack paths that lead to domain domination**
  Make sense of the complex interrelationships between objects, principals and permissions, and eliminate attack paths that lead to domain dominance. Attack path analysis surfaces all the possible steps that attackers could take to move laterally, escalate privileges and gain control over your enterprise directory services.

- **Access real-time attack detection**
  Receive instant alerting against attacks including credential dumping, Kerberoasting, DCSync, ZeroLogon and many more. Respond to attacks in real-time by integrating Tenable Identity Exposure with your SIEM and SOAR. Tenable's research team regularly updates indicators of attack as new identity based exploits are discovered.

- **Investigate and inform**
  Reduce incident response time and capture all changes to Active Directory using Trail Flow. Inform your incident response teams and enrich your security operations processes with real-time prioritization and detailed remediation steps.

- **Increase password strength**
  Boost your organization's password hygiene and slash the risk of password-related attacks. Check for passwords that have been compromised, shared, or that do not meet complexity requirements

- **Tenable One: Correlate identity risk across your environment**
  Tenable One, with the power of Identity Exposure, provides vital context from identities across the entire enterprise attack surface to help prioritize your preventative security efforts to reduce the risk of breaches. Reduce the time and effort required for patch management, gain a better understanding of the attack surface, eliminate blind spots, and build a baseline for effective exposure management.

- **Backed by Tenable research**
  Our world-class research team regularly adds new attack detections and indicators of exposure to Tenable Identity Exposure. The team discovers zero-day vulnerabilities, develops security advisories and remediation steps, and publishes intelligence briefs and insights.

About Tenable

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact