DATA SHEET

PREVENTATIVE SECURITY FOR IDENTITY EXPOSURE

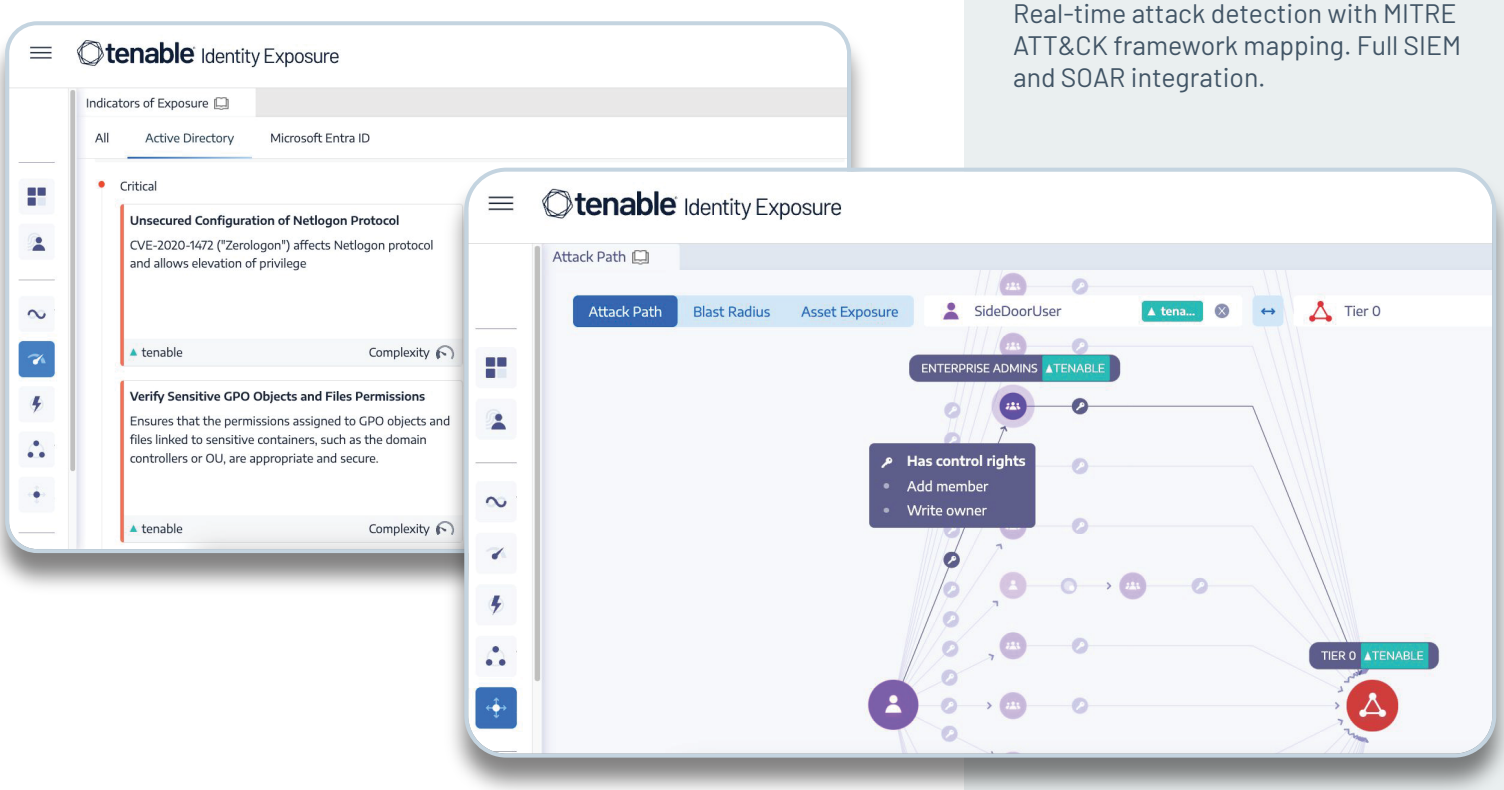
tenable Identity Exposure

Compromised identities are at the center of nearly every successful cyber security attack. Active Directory and Entra ID (formerly known as Azure AD) are common targets for attackers who 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 continually assesses 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 with an AI-driven risk score, and provides attack path visualization.



KEY BENEFITS

Predict and Prioritize

Rank each identity with a risk score and prioritize remediation of insecure configurations where it matters most.

Comprehensive Visibility

Eliminate long-standing, risky configurations. Visualize complex domain and forest relationships.

Visualize Attack Paths

Eliminate attack paths with real-time mapping of paths that lead to domain domination.

Frictionless

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 AI-Driven Risk Scoring

Unify Active Directory, hybrid, and Entra ID accounts all in a single view. Gain control of identities dispersed between multiple directory services, domains and forests in one place. Each identity is scored by our data science and AI engine, which ranks identities based on the level of risk should that identity be compromised.

Continually Assess Directory Services Security In Real-Time

Assess the security posture of your directory services and uncover vulnerabilities, risky configurations and permissions creep. 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

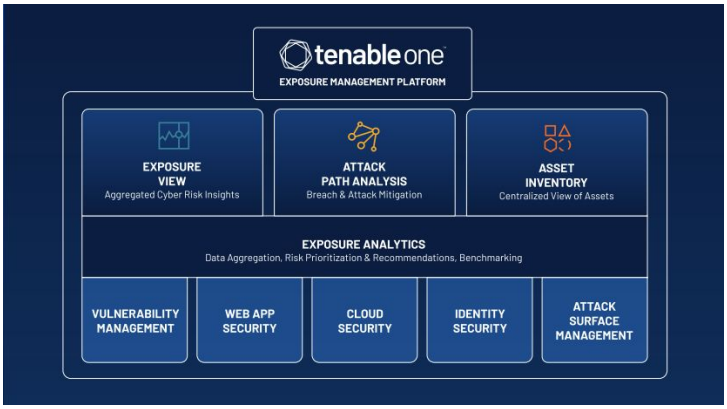
Make sense of the complex interrelationships between objects, principals and permissions, and eliminate attack paths that lead to domain dominance. Attack path analysis surfaces all the possible steps that attackers could take to move laterally, escalate privileges and gain control over your enterprise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

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.



Tenable One: Identity Aware Exposure Management

Tenable Identity Exposure enables identity-aware exposure management and is an essential part of the Tenable One Exposure Management Platform. Identity-aware exposure management helps you understand where to focus your preventative efforts to reduce the risk of a successful breach. Break down silos between enterprise data systems and correlate identity risk and vulnerability information across the entire enterprise with the power of Tenable.

Backed by Tenable Research

New attack detections and indicators of exposure are regularly added to Tenable Identity Exposure by our world-class research team, which discovers zero-day vulnerabilities, develops security advisories and remediation steps, and publishes intelligence briefs and insights.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.