Proofpoint Spotlight

Automatically discover, prioritise and remediate identity vulnerabilities before attackers exploit them

Key Benefits

- Discover identity risk across multiple steps in the attack chain
- Gain identity visibility covering: Active Directory, Entra ID (formerly Azure AD), PAMs, Endpoints, LAPS
- Automatically get a prioritised list of identity vulnerabilities exposed on endpoints
- Manually or automatically remediate vulnerabilities such as Shadow Admins
- Gain risk visibility across subsidiaries and newly acquired entities with a domains and trusts enterprise map
- Intelligent reporting on risk trends over time to enhance your identity security posture

Credential theft and abuse is a pervasive and growing concern. Attackers are shifting their focus from system-based threats to attacks focused on identity. They can complete these attacks in hours or even minutes. And they can leave no trace of compromise or malware.

Even with privileged account management (PAM) and multifactor authentication (MFA) in place, 1 in 6 enterprise endpoints still has vulnerable identities. These are primary targets for cyberattackers. Ransomware and other targeted threats focus on privileged identities as a means to an end.

Proofpoint Spotlight can help reduce the risk of your identities being used against you. The solution is part of the Proofpoint Identity Threat Defense platform. It provides continuous and comprehensive discovery of identity vulnerabilities and automatically remediates these threats. Spotlight addresses identity threats before they can become full-scale breaches.

National defence engineers developed Spotlight to help security teams prioritise threat autoremediation tasks. Alerts are meant to prevent impact to business. But the rising numbers of these alerts has led to increased volumes of noise, which security teams must take the time to sort through.

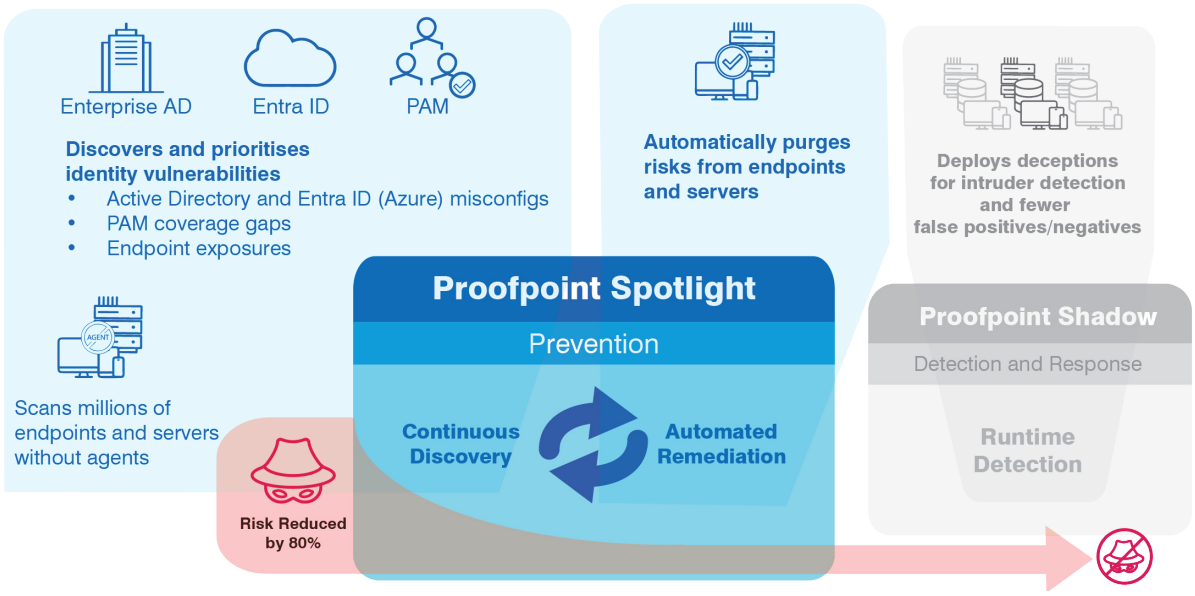

Figure 1. Part of Proofpoint Identity Threat Defense, Proofpoint Spotlight provides continuous discovery and remediation of privileged identity vulnerabilities and policy violations.

How Threat Actors Abuse Privileged Identities

When attackers first land on a host, this is usually not the final target. In most attacks, the threat actors try to escalate privilege. Then they move laterally through the environment to reach their real goal without being detected. They use tools such as Bloodhound, Cobalt Strike, Mimikatz and ADFind to quickly exploit privileged credentials and hide their presence.

In our research, more than 90% of organisations have had an identity-related breach in the past year. And ransomware attacks have reached record levels. There are many reasons for this rise. One is that identity and access management system deployments are very complex. Identities are also continuously changing. And organisations lack complete visibility into the gaps in their environment.

Other reasons include:

- Insufficient or improper PAM configuration and management of service-account, local-admin and privileged-domain credentials
- Unintentional creation of shadow admin accounts that have excessive privileges
- Improper termination of RDP sessions
- User applications–including browsers, SSH, FTP, PuTTY and databases–that cache credentials and cloud access tokens on endpoints

Real-World Example: Attack at Insurance Company

A threat actor used credential stuffing to access a network via remote desktop protocol (RDP). The attacker used stolen credentials for the initial access.

From there, the attacker escalated privileges to Domain Admin. Critical data was encrypted, and some of it was exfiltrated. The organisation paid a ransom of $40 million to recover from the attack.

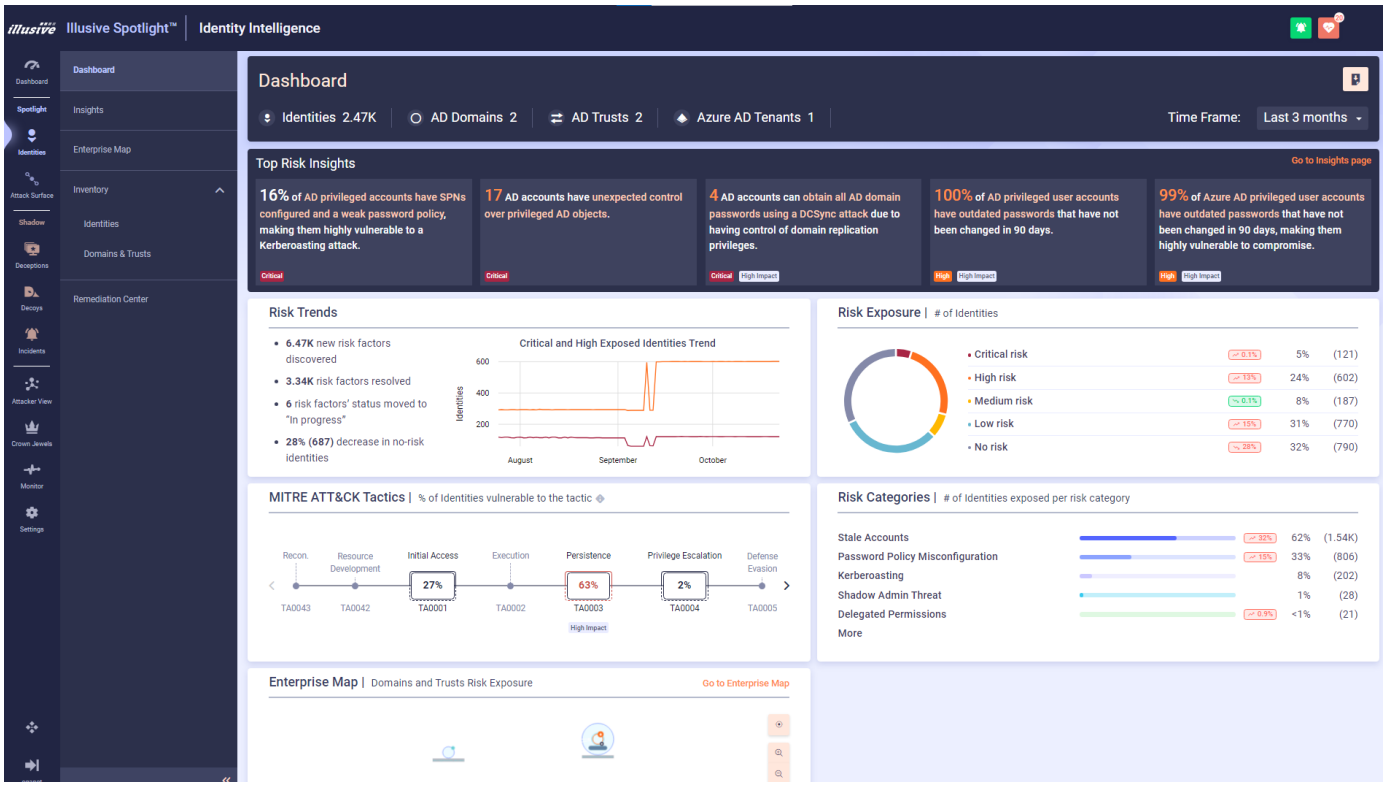

Figure 2. The Proofpoint Spotlight Identity Risk dashboard.

Find, Prioritise and Fix Vulnerable Identities

Spotlight reveals the gaps between your identity security policies and your actual environments. It scans the following systems to provide complete visibility and prioritisation of current identity vulnerabilities:

- **Directory structures.** Active Directory and Entra ID (formerly Azure AD).
- **PAM solutions.** CyberArk and Delinea Centrify.
- **Endpoints.** Clients and servers.
- **Tasks.**

Proofpoint Spotlight helps prevent attacks by taking away the identity vulnerabilities attackers need to further crimes that can escalate into significant breaches.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.