Proofpoint Spotlight

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

Key Benefits

- **Discover identity vulnerabilities, attack paths and the blast radius of users**
- **Gain identity vulnerability visibility covering: Active Directory, Entra ID, AWS IAM Identity Center, Okta, PAMs (CyberArk and Delinea), endpoints, LAPS**
- **Receive a prioritized list of identity vulnerabilities exposed on endpoints without the dependence on agents**
- **Manually or automatically remediate vulnerabilities such as Shadow admins and cached credentials on endpoints**
- **Gain risk visibility across subsidiaries and newly acquired entities with a domains and trusts enterprise map**
- **Intelligent risk scoring and trends to enhance your identity security posture**
- **Integrate with the Proofpoint TAP Dashboard, TAP ATO and NPRE.**
- **Available for SaaS deployment**

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Credential theft and account takeovers are pervasive and growing concerns. 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), 1 in 6 enterprise endpoints still has vulnerable identities and most organizations have shadow administrators.. These identities 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 them. Spotlight addresses these vulnerabilities before threat actors can exploit them.

How Threat Actors Abuse Privileged Identities

When attackers first compromise an identity or land on a host, this is usually not their final target. In most attacks, they try to escalate privilege. Then they try to move laterally through the environment to reach their real goal. They use tools such as Bloodhound, Cobalt Strike, Mimikatz and ADFind to quickly exploit privileged credentials and hide their presence.

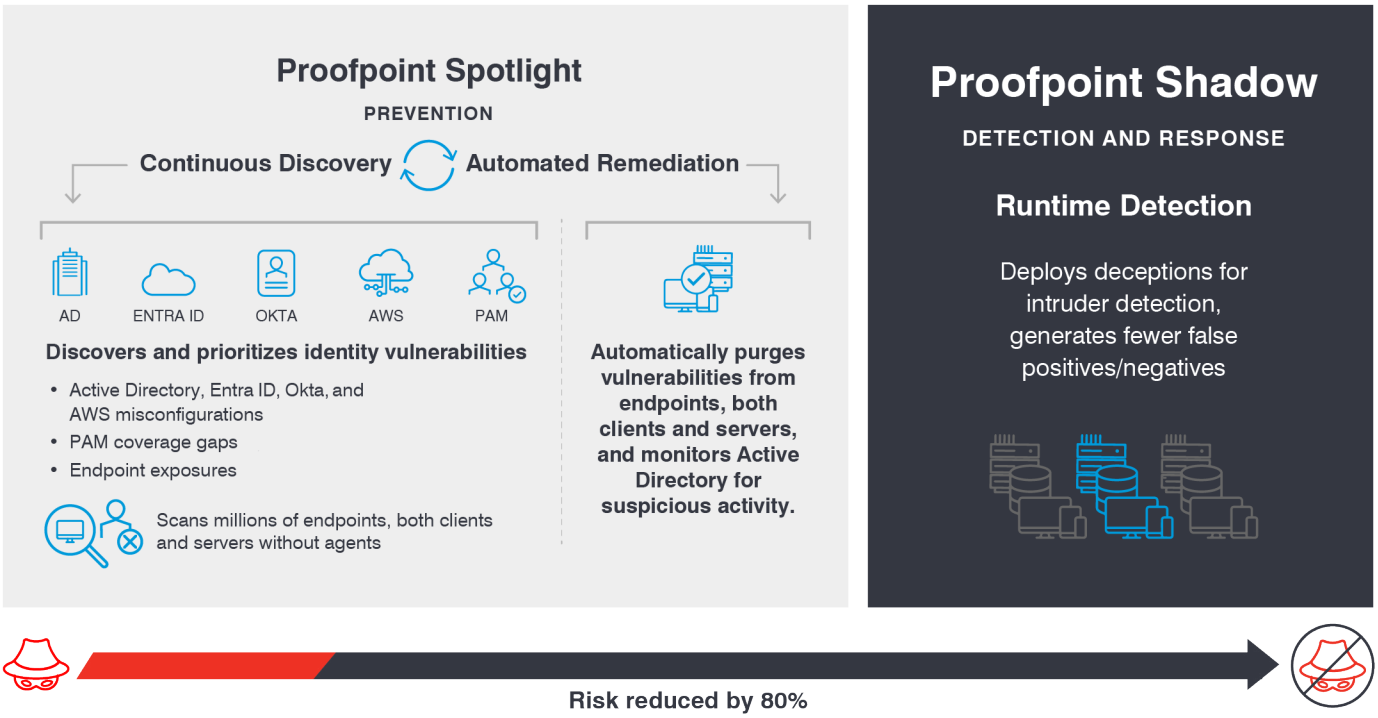

Figure 1. Part of the Proofpoint Identity Threat Defense platform, Proofpoint Spotlight provides continuous discovery and remediation of identity vulnerabilities and security policy violations.

In our research, more than 90% of organizations 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 deployments of identity and access management systems are very complex. Identities are also always changing. And organizations don't have complete visibility into the gaps in their environment.

Other reasons include:

- Insufficient or improper PAM configuration and complex 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—such as 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 organization paid a ransom of $40 million to recover from the attack.

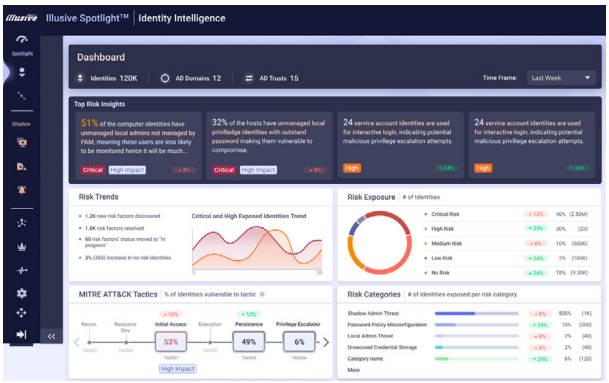

Figure 2. The Proofpoint Spotlight Identity Risk dashboard.

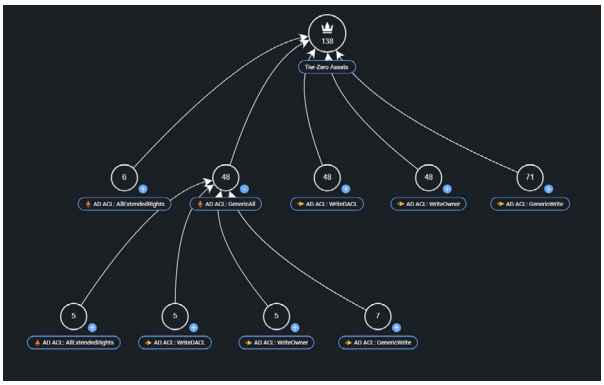

Figure 3. Attack Path Management.

Leverage integration with Proofpoint TAP, TAP ATO and NPRE to provide current identity vulnerability directly against your VAPs, accounts which have been taken over and as part of the overall risk scoring of your users.

Proofpoint Spotlight helps prevent attacks by taking away the identity vulnerabilities attackers need to move laterally, which can escalate into significant breaches. It can also prevent lateral movement by providing detailed identity-centric blast radius information.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' 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 organizations 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**.