proofpoint.

SOLUTION BRIEF

Proofpoint Spotlight

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

Key Benefits

- Discover identity risk across multiple categories in the attack chain
- Gain identity visibility across a single pane of glass: Active Directory, Azure AD, PAMs, Endpoints, LAPS
- Automatically get a prioritized list of identities and address the most urgent needs first
- Remediate or auto-remediate risks and threats discovered
- Gain risk visibility across subsidiaries and M&A 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 now a pervasive and growing concern. Attackers are shifting their focus from system-based threats to attacks based on identity. These attacks can be completed in days. And they can leave no trace of compromise or malware.

Even with privileged account management (PAM) and multifactor authentication (MFA) in place, one in six enterprise endpoints still has a vulnerable identity. And these are primary targets for cyber criminals. Ransomware and other targeted cyber attacks focus on privileged identities in particular.

Proofpoint Spotlight can help. Our solution prevents identity threats by addressing risks before they can become more serious. It provides continuous and comprehensive discovery of identity vulnerabilities in various categories across the attack chain, including:

- Shadow admin threat
- Unsecure stored credential on endpoints
- Password misconfiguration

Spotlight offers discovery, risk prioritization and automatic remediation of such identity and misconfigurations. It was developed by national defense engineers who saw the need to help CISOs prioritize threat autoremediation tasks when handling alerts. This is because the growing volume of these alerts often means they generate a lot of noise rather than prevent impact to business.

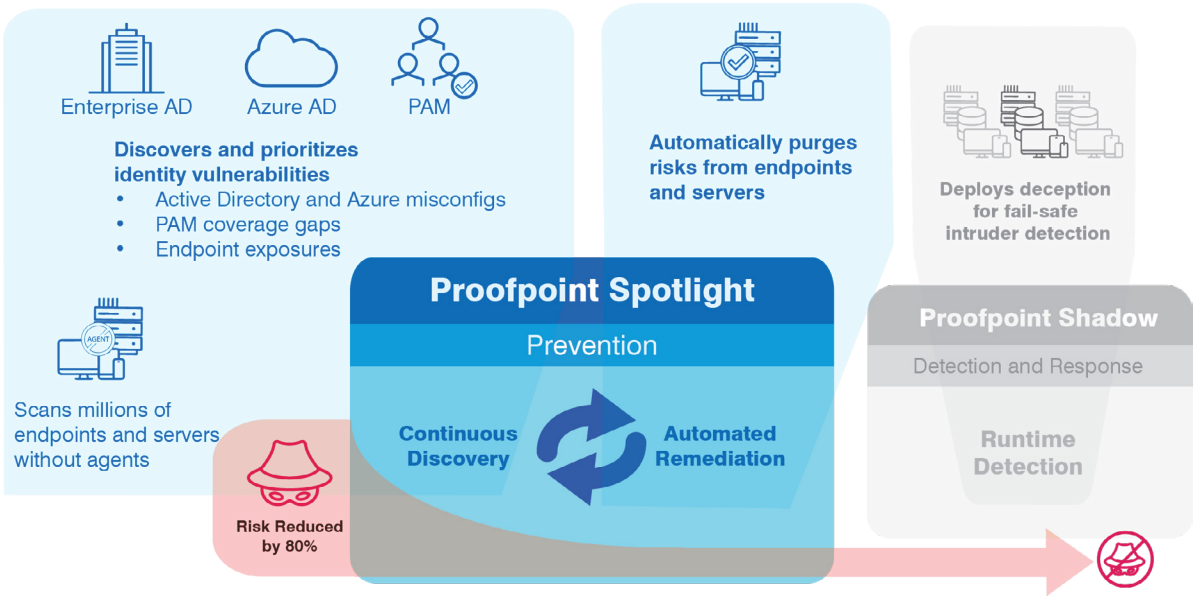

Figure 1. Part of Proofpoint Identity Threat Defense, Proofpoint Spotlight provides continuous discovery and remediation of privileged identity vulnerabilities and policy violations.

How Threat Actors Abuse Privileged Identities

When attackers first land on a host, the point of entry is usually not their final target. They often escalate privilege. And then they move laterally in a system to reach their goal. They use tools like Bloodhound, Cobalt Strike, Mimikatz and ADFind to quickly exploit privileged credentials and make it a challenge for you to detect them.

More than 90% of organizations have had an identity-related breach in the past year. And ransomware attacks have reached record-breaking levels. There are many reasons for this rise. One is that identity and access management system deployments are very complex. Identities are also always changing. And there is a lack of continuous visibility into the gaps in the environment.

Other reasons include:

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

Real-World Example: Attack at CNA Insurance

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

From there, he escalated privileges to Domain Admin. Then he encrypted critical data, exfiltrating some of it. The customer paid a ransom of $40 million to recover from the attack.

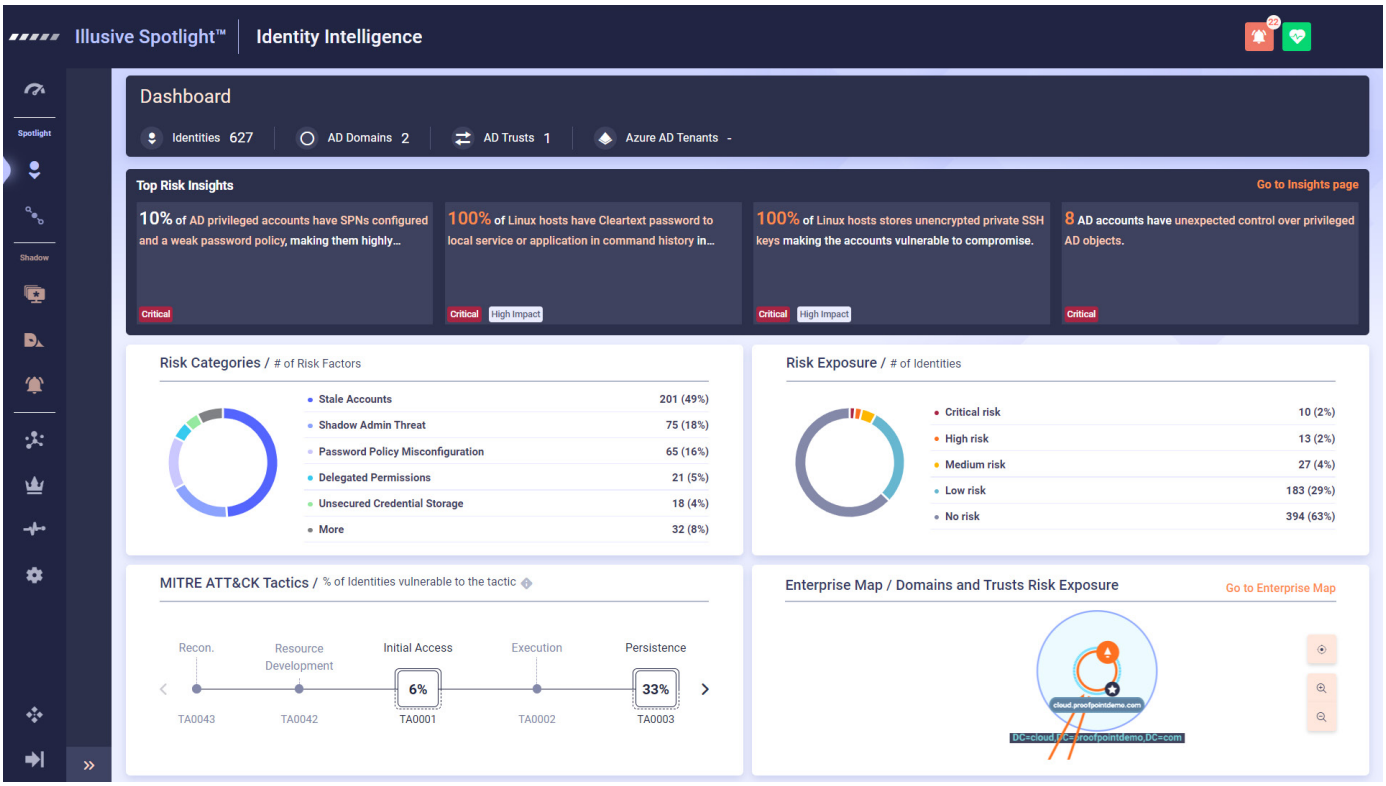

Figure 2 The Proofpoint Spotlight Identity Risk dashboard.

Find, Prioritize and Fix Vulnerable Identities

Spotlight, along with Proofpoint Shadow, is part of the Proofpoint Identity Threat Defense platform of offerings. Spotlight reveals all of the gaps between your existing identity security policies and your actual environments, including endpoints. It provides complete visibility into identity vulnerabilities and risks by scanning:

- Directory structures, such as Active Directory and AzureAD
- PAM solutions, such as CyberArk and Delinea
- Endpoints
- Servers
- Services

Proofpoint Spotlight helps prevent potential attacks by taking away what attackers need to further their crime before it can escalate into actionable threats.

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.