proofpoint.

SOLUTION BRIEF

Proofpoint Spotlight

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

Key Benefits

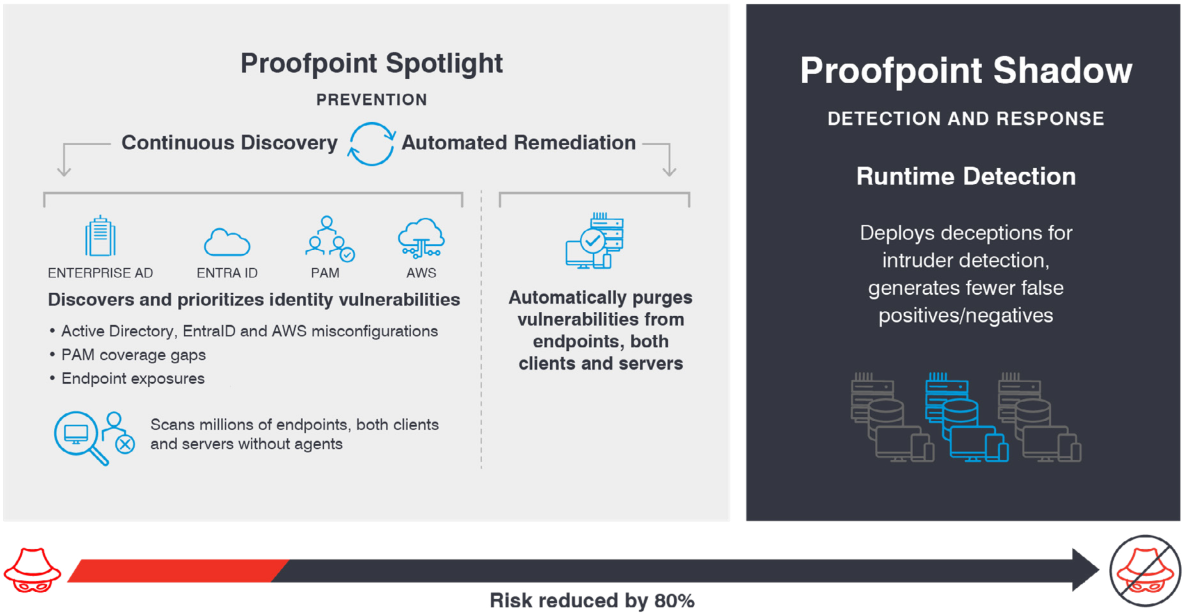
- Discover identity vulnerabilities, attack paths and blast radius
- Gain identity vulnerability visibility covering: Active Directory, Entra ID, AWS Identity Center, PAMs, Endpoints, LAPS
- Receive a prioritized list of identity vulnerabilities exposed on endpoints
- Manually or automatically remediate 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 to deliver identity vulnerability context against the organization's Very Attacked People (VAPs)
- Available for SaaS deployment

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 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.

National defense engineers developed Spotlight to help security teams prioritize vulnerability remediation tasks. Alerts are meant to prevent impact to business. But the rising numbers of these alerts has led to an increased volume of noise, which security teams must take the time to sort through.



Discovers and prioritizes identity vulnerabilities

- Active Directory, EntraID and AWS misconfigurations
- PAM coverage gaps
- Endpoint exposures

Scans millions of endpoints, both clients and servers without agents

Automatically purges vulnerabilities from endpoints, both clients and servers

Deploys deceptions for intruder detection, generates fewer false positives/negatives

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

How Threat Actors Abuse Privileged Identities

When attackers first 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.

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.

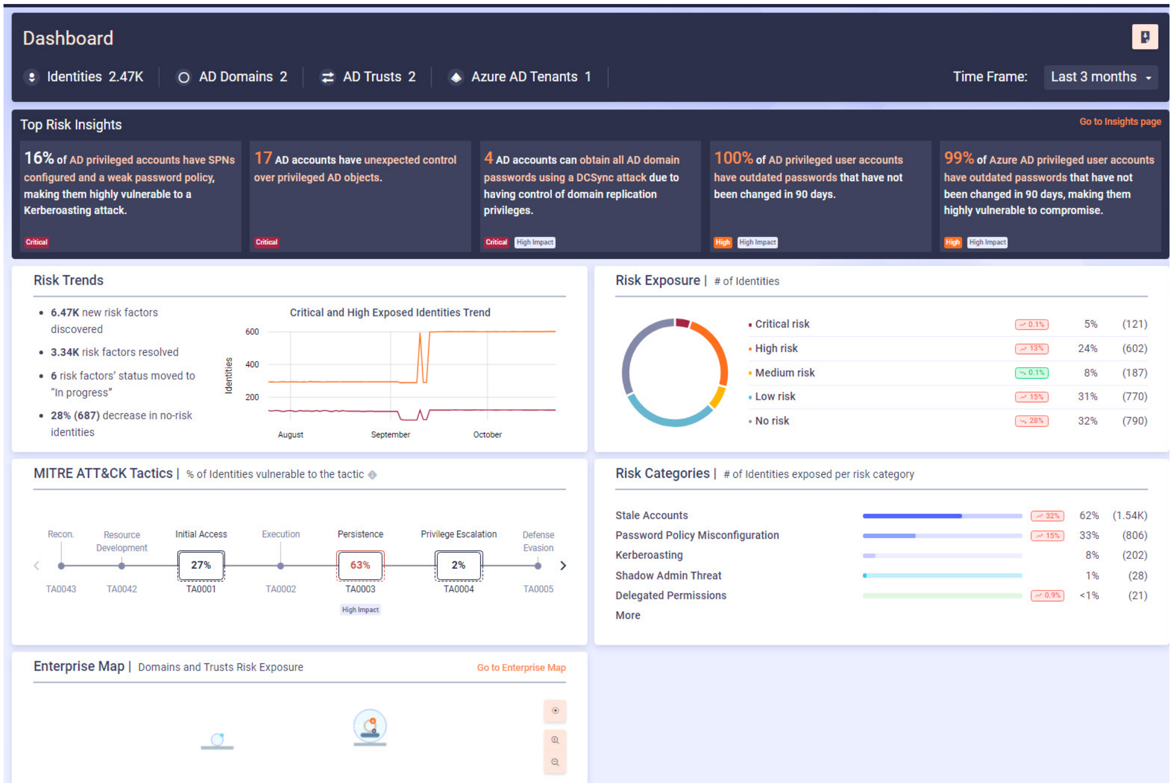
Other reasons include:

- Insufficient or improper PAM configuration and 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.



16% of AD privileged accounts have SPNs configured and a weak password policy, making them highly vulnerable to a Kerberoasting attack.

17 AD accounts have unexpected control over privileged AD objects.

4 AD accounts can obtain all AD domain passwords using a DCSync attack due to having control of domain replication privileges.

100% of AD privileged user accounts have outdated passwords that have not been changed in 90 days.

99% of Azure AD privileged user accounts have outdated passwords that have not been changed in 90 days, making them highly vulnerable to compromise.

- **6.47K** new risk factors discovered
- **3.34K** risk factors resolved
- **6** risk factors' status moved to "In progress"
- **28% (687)** decrease in no-risk identities

Critical risk	↗ 0.1%	5%	(121)
High risk	↗ 13%	24%	(602)
Medium risk	↘ 0.1%	8%	(187)
Low risk	↗ 15%	31%	(770)
No risk	↘ 28%	32%	(790)

Stale Accounts	↗ 32%	62%	(1.54K)
Password Policy Misconfiguration	↗ 15%	33%	(806)
Kerberoasting		8%	(202)
Shadow Admin Threat		1%	(28)
Delegated Permissions	↗ 0.9%	<1%	(21)

Figure 2. The Proofpoint Spotlight Identity Risk dashboard.

Find, Prioritize 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 prioritization of current identity vulnerabilities:

- **Identity Stores—**Active Directory, Entra ID and AWS Identity Center
- **PAM solutions—**CyberArk and Delinea
- **Endpoints—**Clients and servers, including stored credentials

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.