Proofpoint Identity Threat Defense Platform

Stop privilege escalation and lateral movement

Products

- Proofpoint Shadow
- Proofpoint Spotlight

Key Benefits

- Discover, prioritise and remediate identity-based vulnerabilities
- Understand the privileged identity risks and available attack paths in your environment
- Gain visibility into identity vulnerabilities covering Active Directory, Entra ID, AWS Identity Center, Okta, PAMs, Endpoints, LAPS
- Automatically remediate identity vulnerabilities exposed on endpoints
- Ensure early attacker detection and accelerate threat investigations
- Use agentless technology that attackers cannot bypass
- Fill the gaps left by signature- and behaviour-based threat detection
- Leverage integration with Proofpoint TAP, TAP ATO and NPRE
- Available for SaaS deployment

Attacks have become much more sophisticated and targeted. And the solutions that are meant to defend against them are not keeping up with the threat.[1] The trends suggest that attackers are standardising their tactics, techniques and procedures to focus on identity. But organisations have not yet been able to break the attack chain reliably. Identities are a critical part of the attack surface that requires increased focus.

The Proofpoint Identity Threat Defense platform provides end-to-end protection against identity threats. It includes component products Proofpoint Shadow and Proofpoint Spotlight. It features the discovery and remediation of identity vulnerabilities as well as agentless deception-based detections and forensic data collection. The platform enables you to discover, prioritise and remediate vulnerable identities. It also helps you detect and respond to active threats.

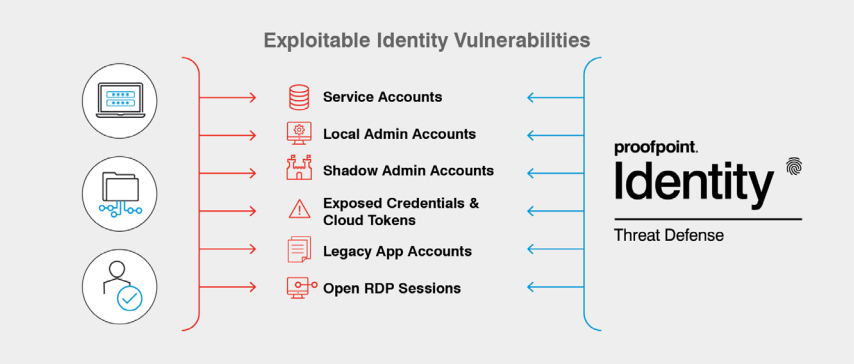

Figure 1: Proofpoint Identity Threat Defense and exploitable identity vulnerabilities.

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

1 Some of these solutions include identity and access management (IAM), multifactor authentication (MFA), endpoint detection and response (EDR), security information and event management (SIEM) and extended detection and response (XDR).

An Identity Crisis

Most organisations deploy Active Directory. Unfortunately, 79% have had an identity-related breach in the past two years. According to the Verizon DBIR Report, 94% of successful attacks used Active Directory and privileged identities to escalate their privileges. The attackers use a wide range of tools. Bloodhound, Cobalt Strike, Mimikatz and ADFind are just a few of them. These tools help them exploit privileged identities quickly. They also make it hard to detect their attacks.

Proofpoint research shows that 1 in 6 enterprise endpoints, both clients and servers, contain identity vulnerabilities. And this is even when traditional identity and access management (IAM) solutions are in place. Attackers exploit these vulnerabilities to gain access to admin privileges. When they first land on a host, that host is rarely their end target. They seek to move laterally within the network as they search for the most critical, or Tier 0, IT assets. Once there, they can exfiltrate data. They can also launch ransomware attacks.

Figure 2: Proofpoint Identity Threat Defense platform.

Many identity vulnerabilities arise from normal business and IT operational procedures, such as:

- **Usernames and passwords.** User apps often cache these on endpoints such as browsers, SSH, FTP, PuTTY and databases. PAMs do not protect these credentials.
- **Domain admin credentials.** These are sometimes retained in system memory after a remote support session. They are also often cached in an unprotected service account.
- **Shadow privileges.** Configuring identity directory objects and groups in Active Directory can be very complex. Because of this, some users can be inadvertently assigned excessive, shadow privileges.

An End-to-End View of Identity Security

Successful attacks exploit management and protection gaps. Our platform helps security leaders see and defend against these gaps. It enables them to:

1. **Discover.** Get continuous discovery and visibility of identity vulnerabilities in AD, Entra ID, AWS Identity Center, Okta and endpoints.
2. **Prioritise and Remediate.** See a list of vulnerabilities prioritised by the ones that need attention first. These risks appear on a spectrum that ranges from non-critical to urgent. Enable automated remediation of identity vulnerabilities straight from the platform. You can set up exception rules that are consistent with your security policies.
3. **Detect and Respond.** See when attackers are active in your environment. With agentless deceptions, you can detect activity such as kerberoasting, password spraying, privileged account abuse and much more. You can use automated forensic data collection to help guide your organisation's response to active threats.

LEARN MORE

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