



PRIVILEGED ACCESS SECURITY

PAS INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: **Proofpoint**

Website: <https://www.proofpoint.com/>

Name of Product: Proofpoint Spotlight (Previously Illusive Spotlight)

Version: 3.1.183

Date: April 25, 2023

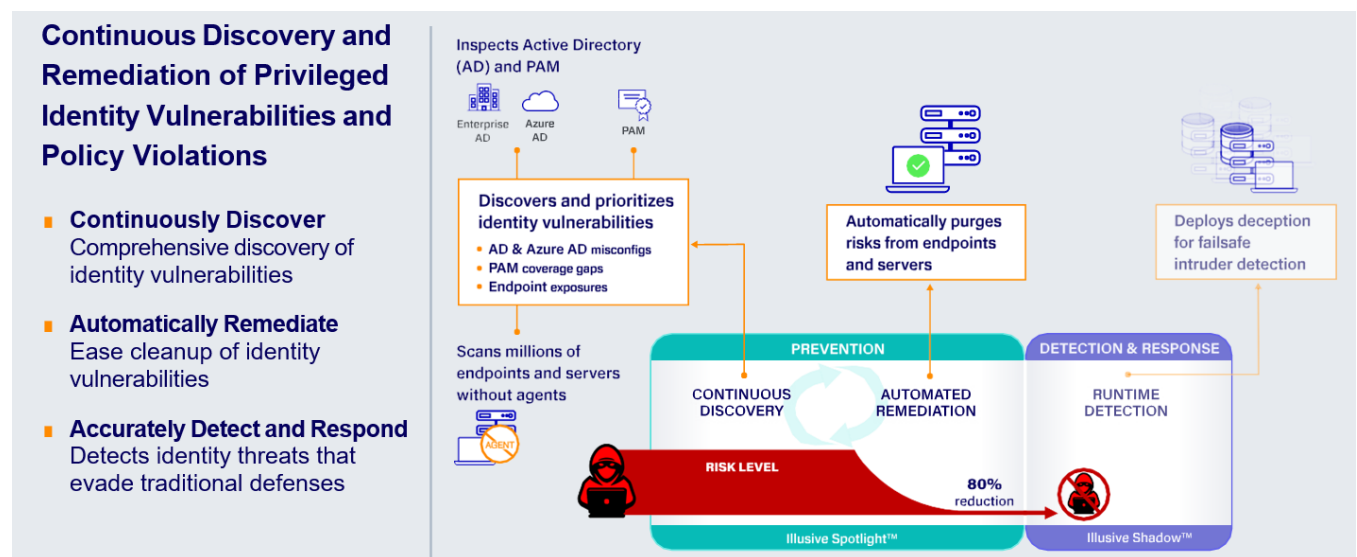
PROOFPOINT SPOTLIGHT SOLUTION OVERVIEW

Identity Threat Detection & Response (ITDR) is Critical to Protect Against the #1 Vector for Attack.

The global increase in cyberattacks has been enabled by attackers shifting their focus from system to identity-based attacks, such as account takeover attacks (ATOs). These attacks are often completed in only days and go undetected without leaving any indicators of compromise or evidence of malware.

To execute a targeted cyberattack, attackers typically need to establish themselves on an endpoint and gradually find their way into an organization's high-value systems. Rather than detecting malware or monitoring anomalous network traffic or user behavior, Proofpoint anticipates and manipulates the behavior of the actual people behind the attack. As an agentless, automated solution that deters and detects their reconnaissance and lateral movement, Proofpoint solution protects critical systems and operations by stopping high-impact attacks very early in the attack process.

On each endpoint, Proofpoint Shadow plants false bits of information (deceptions) that appears real and valuable to the attacker. Simultaneously, the **Proofpoint Spotlight** module preemptively reduces the availability of real credentials and connections that an attacker could use. Together, these capabilities ensure that, from the first point of entry, the attacker is confronted with extremely high odds of choosing a false path. The first wrong move an attacker conducts triggers an alert. Detailed, real-time forensics are captured from the system where the attacker is operating. From the Proofpoint Attacker View console, defenders are armed with knowledge of the attacker's position in relation to critical assets and are provided the information they need to prioritize triage and choose the best course of action.



KEY BENEFITS

Proofpoint key benefits:

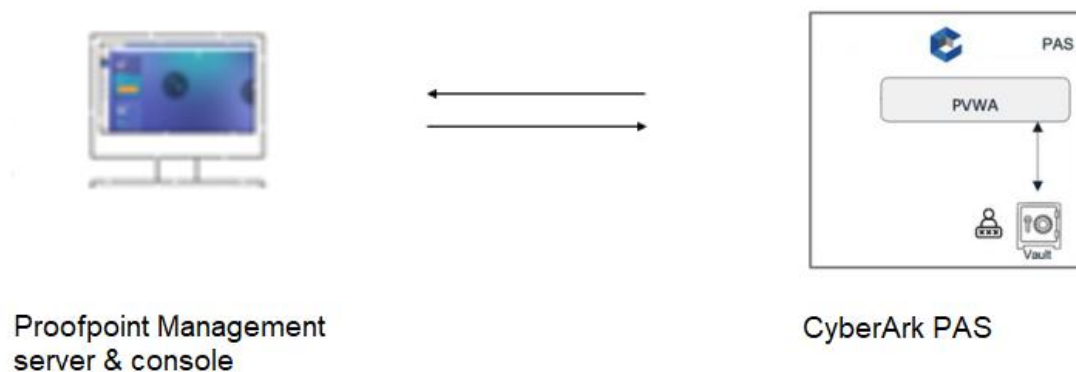
- **Uncovers and removes high-risk connectivity** that enables lateral movement
- **Forces attackers to reveal themselves** early in the attack process by disorienting and manipulating their decision-making process
- **Provides real-time insight** when attackers are present, for rapid remediation and future improvements

Key benefits of integrating Proofpoint Spotlight with CyberArk PAS:

- **Track unmanaged users**- users that do not have their password managed in CyberArk Vault
- **Track unmanaged service accounts**- service accounts that do not have their secret managed in CyberArk Vault

Accounts not managed by a PAM (Privileged Access Management) tool increases the risk of attackers gaining access without detection and exploiting privileged identity accounts in an organization. With PAM, it is possible to reduce this risk by managing the access and passwords of privileged identities and constantly monitoring their sessions and activities.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



1. Proofpoint Spotlight and PAS integration

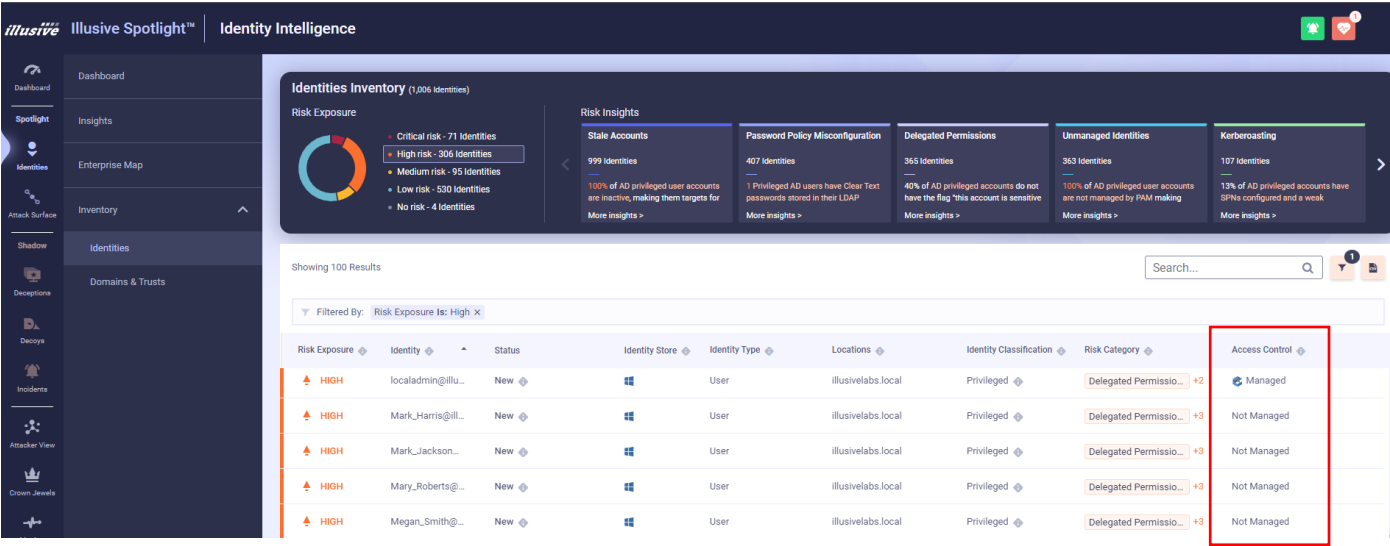
The Proofpoint Spotlight Management Server is a central server which is installed with the Credentials Provider Client and connects to PAS.

To get the list of managed accounts from CyberArk, the Proofpoint Management Server periodically connects to the PAS server to pull these accounts.

2. How It Works

Proofpoint periodically queries CyberArk's REST API to get the list of managed accounts, using this URI: `"/PasswordVault/api/Accounts"`.

Proofpoint Spotlight then compares the CyberArk managed accounts with the accounts Proofpoint pulled from onboarded identity stores such as Active Directory. Proofpoint Spotlight highlights accounts which have been found unmanaged in CyberArk.



PAS INSTALLATION

Refer to “Credential Provider and ASCP Implementation Guide” for CyberArk Credential Provider installation.

PAS CONFIGURATION

- The CyberArk PAS user for this integration requires List Accounts permissions in the Safe to query the "/PasswordVault/api/Accounts" resource.
- The CyberArk PAS user must be a local CyberArk account in order to authenticate to the web API.

PROOFPOINT SPOTLIGHT PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to the **Proofpoint Spotlight Installation Guide** for Partner Product installation.

To configure the CyberArk PAS server in Proofpoint Spotlight:

This portion of the integration allows Proofpoint to pull managed accounts from CyberArk using the PAS interface.

To configure CyberArk PAS in the Proofpoint Console:

CyberArk PAS Integration  **Inactive**

This configuration integrates with CyberArk Privileged Access Security™ allowing Illusive to identify user accounts managed by CyberArk and enrich data presentation in Attack Surface Manager [Domain User Credentials](#) and [Local User Administrators](#)

Configure the following credentials to enable Illusive to identify user accounts managed by CyberArk. The [following prerequisites](#) must be met for Illusive to identify CyberArk managed accounts.

Hostname

Port

Username

Password

 **Disconnect PAS Integration**

 **Check Connectivity**

 **Connect PAS Integration**

1. In the Proofpoint Management Console, navigate to **Settings > Third Party Integrations > CyberArk**.
2. In the **Password Management Identification** section, specify the following details:
 - a. Hostname – PAS Webserver hostname
 - b. Port – PAS Webserver port
 - c. Username – PAS user username
 - d. Password – PAS user password
3. The following options are available when configuring PAS integration:
 - To save the configuration, click **Connect PAS Integration**.

Note: After saving, an **Active** or **Inactive** status will appear whether the integration is successful or not.

- To discard changes, click **Discard**.

Important: No undo option will be available after disconnecting the integration.

- To check the connectivity status in real time, click **Check Connectivity**.

4. Click **Save**.

PARTNER CONTACT INFO

Business Contact	Name	D.j. Long
	Email	dlong@proofpoint.com
	Tel	
Technical Contact	Name	Omer Ganot
	Email	oganot@proofpoint.com
	Tel	
Support Contact	Name	Uri Polsky
	Email	upolsky@proofpoint.com
	Tel	
Marketing Contact	Name	Jasmine Wu
	Email	jawu@proofpoint.com
	Tel	