Proofpoint Identity Protection

Take a defense-in-depth approach to account takeover across your hybrid enterprise

Key Benefits

- Defend against account takeover across the entire attack chain
- Discover, prioritize and automatically remediate identity vulnerabilities across the organization's identity infrastructure
- Detect compromised accounts by applying threat intelligence and behavioral analytics
- Stop attackers attempts at lateral movement before they can reach the organization's critical IT assets
- Automatically quarantine compromised accounts and reverse malicious mailbox rule changes, manipulations of third-party apps and block data exfiltration

When threat actors compromise a user's accounts and credentials, they take control of that user's digital identity. If they succeed, they will then attempt to exploit even more user accounts. They will also seek to escalate their privileges and move laterally across cloud accounts, platforms, applications and network endpoints. At that point they can launch phishing and ransomware attacks, exfiltrate sensitive data and establish persistent access. But with Proofpoint Identity Protection, you can defend against account takeovers with a solid defense-in-depth approach that covers the entire attack chain.

The account takeover problem is a widespread concern. Our research shows that threat actors targeted 98% of all organizations in 2023, 62% of which experienced a compromise. The research also shows that nearly one-third of these compromised organizations had a multifactor authentication (MFA) solution in place. This indicates, unfortunately, that MFA is not a silver-bullet defense against account takeovers. Meanwhile, attackers have standardized their tactics and techniques to focus on identity. According to the Verizon DBIR Report, 94% of successful attacks used Active Directory and privileged identities to escalate their privilege so they can drive deeper into target organizations.

Proofpoint research also shows that 1 in 6 enterprise endpoints—both clients and servers—contain identity vulnerabilities. These are easily exploitable, and attackers target them to gain admin privileges. Many of the vulnerabilities arise from normal business and IT operational procedures. For example, user apps, such as browsers and client-side utilities, regularly cache usernames and

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

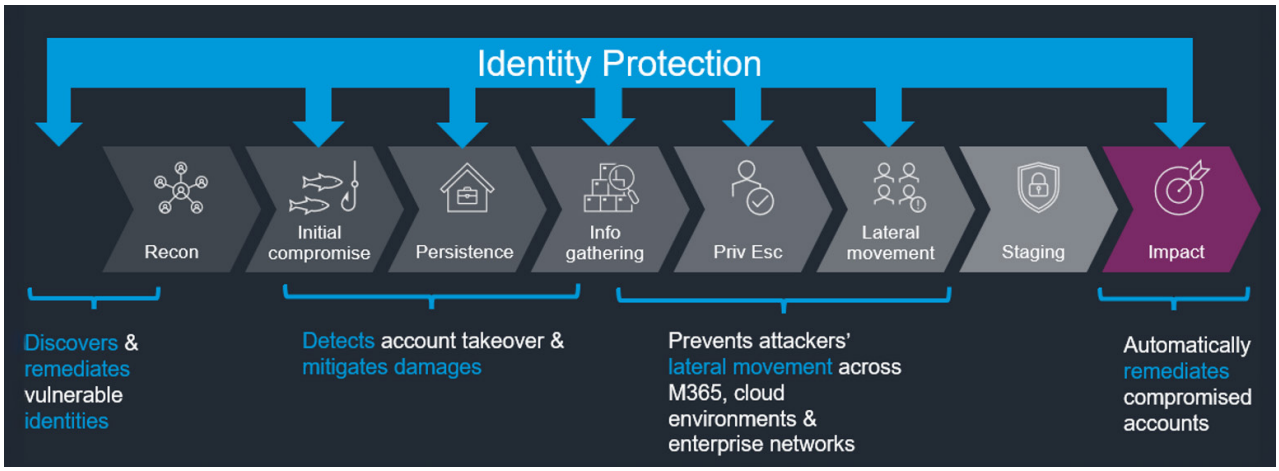

Figure 1. Identity Protection offers multiple security controls covering the entire attack chain.

passwords that can be extracted easily. Domain admin credentials are also often cached in system memory after a remote support session. And many times, non-IT users are granted admin privileges by mistake through Active Directory misconfigurations.

No single security system is perfect. That is why Identity Protection provides multiple layers of controls. Having more than one layer of controls helps you better defend against account takeovers and protect your IT systems. This defense-in-depth approach is even more relevant in today's hybrid enterprise, which depends on both cloud and on-premises assets. And identity management systems, such as Active Directory, PAMs and cloud-based identity provider services, are increasingly being targeted.

Discover, Prioritize and Remediate

Identity Protection discovers, prioritizes and remediates vulnerable identities prior to an account takeover attack.

- **Discovers—**It continuously discovers vulnerable identities in Active Directory, Entra ID, AWS Identity Center, PAMs, endpoints and other identity repositories
- **Prioritizes—**It prioritizes identity vulnerabilities based on risk and maps available attack paths relative to the organization's IT crown jewels
- **Remediates—**You can enable automated remediation directly from the dashboard and set up exception rules that are consistent with your security policies

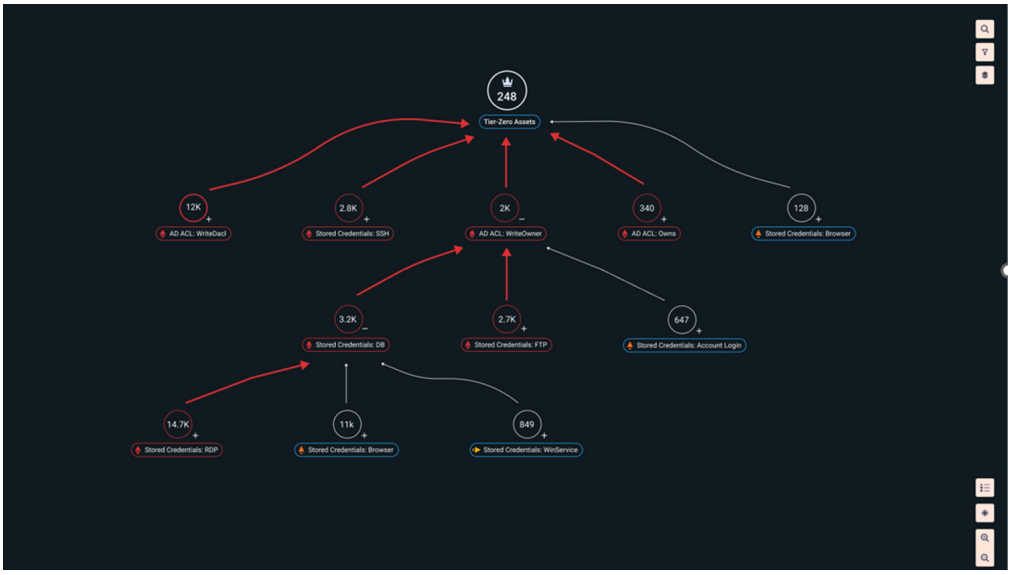

Figure 2. The attack path management view shows exploitable paths to an organization's crown jewels.

Figure 3. The Attack Sequence report displays threats across the attack chain.

Detect Compromised Accounts

Identity Protection reveals compromised accounts in your Microsoft 365 and Google Workspace email accounts. If left unchecked, these accounts can lead to broad compromises of entire cloud application environments. The solution correlates threat intelligence and data from Proofpoint Targeted Attack Protection with artificial intelligence (AI) and behavioral analytics to detect malicious events that can indicate an account takeover. This approach provides you with complete visibility. You can see the accounts that are compromised as well as what the threat actors have been doing. It also provides high-fidelity verdicts.

Identity Protection displays an attack sequence timeline of the threat actor's activity. This helps with investigations, as it can tell you how attackers accessed the account as well as what they did after they logged in and took control.

Detect and Respond to Active Threats

Identity Protection helps you detect and respond to attackers' activities post-compromise. It does this by deploying agentless deceptions throughout the enterprise. These look authentic. But they are, in fact, deceptive resources such as emails, cached credentials and stale RDP sessions. And when threat actors engage with them, you can detect their attempts at privilege escalation and lateral movement. When tripped, the deceptions collect forensic data to help guide your response to the active threats.

The timeline view of activity provides insights into accounts that have been taken over. All data is clickable. This allows analysts to drill down and investigate each incident post-compromise. When an attacker changes mailbox rules, Identity Protection automatically detects and remediates the action. Attackers often change these rules to hide their activity before staging a BEC or other type of attacks. Identity Protection will also detect and revoke access to exploited third-party cloud apps that have a trust relationship with the compromised account. If attackers have manipulated MFA settings to gain persistent access, Identity Protection will restore the original settings. These responses help reduce attackers' dwell time. They also help to minimize the potential business impact of the incident. And if an attacker attempts to exfiltrate data from your environment, Identity Protection will block the action.

LEARN MORE

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