Proofpoint Shadow

Stop privilege escalation and lateral movement in real time

Key Benefits

- Ensures early attacker detection and comprehensive threat investigations
- Reduces false positives in the SOC by providing high-fidelity alerts
- Agentless technology deploys easily with little IT involvement
- Provides continuous defence by dynamically adjusting as the IT environment changes
- Proven to scale across networks of more than a million endpoints
- Fills the gaps left by signature and anomaly-based threat detection

More than 90% of cyber attacks involve risky identities. Attackers have adapted their strategies by targeting privileged identities instead of trying to breach systems directly. This shift has led to a surge in successful ransomware attacks and data breaches. By focusing on vulnerable identities, attackers can shorten their attack timeline from months to days, or even hours.

Proofpoint can help. Our powerful Proofpoint Shadow solution transforms your endpoints into a web of deceptions that make it next to impossible for attackers to move laterally in your environment undetected. Part of the Proofpoint Identity Threat Defense platform, Shadow deterministically catches threat actors based on their interactions with what appear to be legitimate pathways on your endpoints but are actually deceptions that we employ.

Unlike other tools, Shadow doesn't rely on analytics based on signatures or behaviours. It also doesn't use agents or honeypots that can be exploited. Instead, Shadow's agentless architecture allows the deceptions to operate quietly, hiding from attackers. Shadow has successfully defended against more than 160 red team exercises with some of the top security organisations in the world, including Microsoft, Mandiant, the U.S. Department of Defence and Cisco.

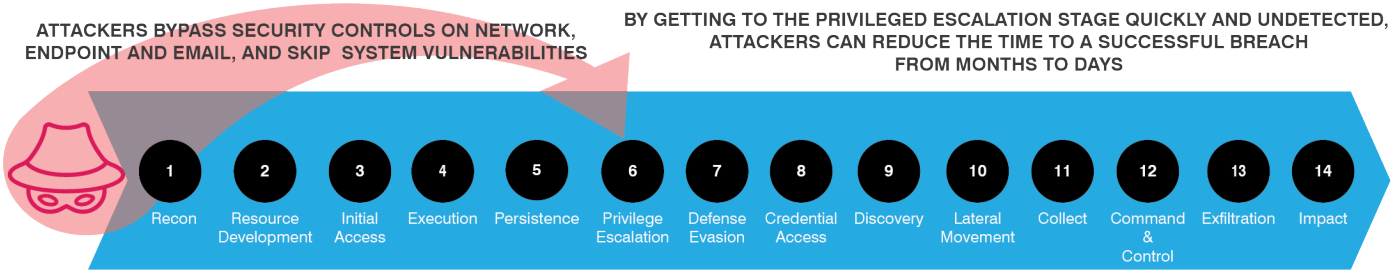

Figure 1. Attackers now focus on vulnerable identities as a key path through the attack chain.

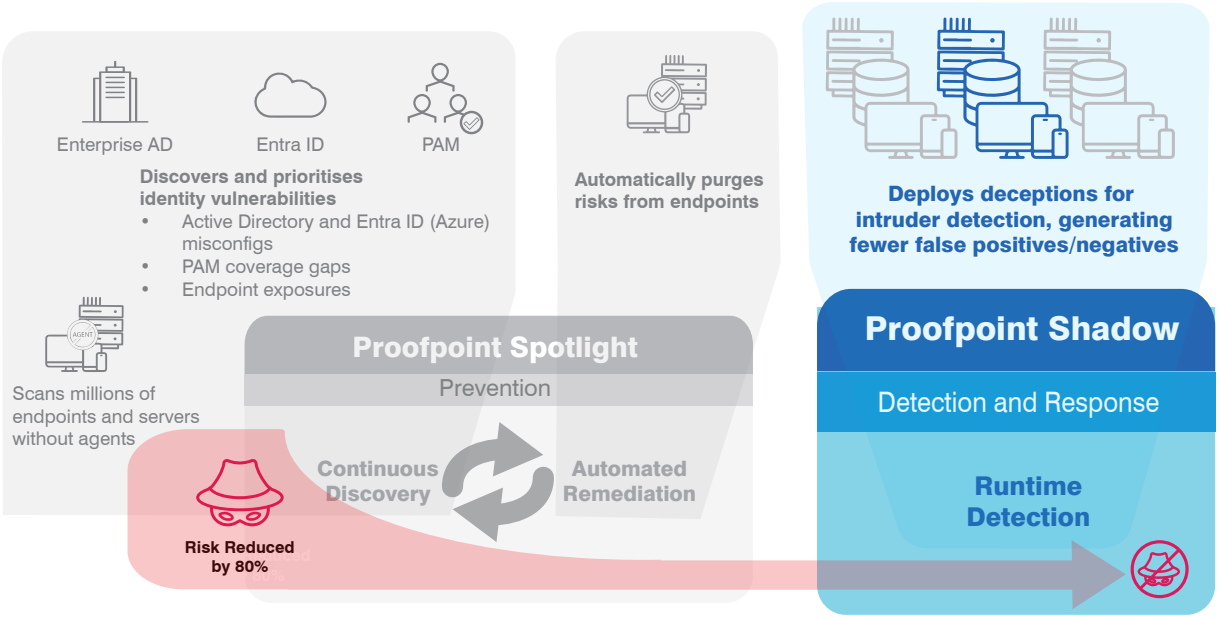

Figure 2. Part of the Proofpoint Identity Threat Defense platform, Shadow creates a web of deceptions that detect and alert on an attacker's lateral movement in your networks.

Probabilistic to Deterministic Detection

You can detect and respond to threats in many ways. You can look for very specific patterns, or signatures, for example. Or you can analyse how a potential threat actor behaves. Conventional tools often fail to catch serious attacks such as when threat actors escalate privileges or move laterally around your network undetected. And these detection failures can lead to the threat actors taking over accounts, spreading ransomware or stealing data. Security teams need a more advanced and reliable approach to stay ahead of these kinds of attacks.

Shadow provides a deterministic approach. It uses widely distributed deceptions to actively engage attackers across the attack chain and keep track of their activities. These deceptions are hidden deeply within the company's endpoints. They look and act like real files, RDP sessions, database connections, emails, scripts and more that attackers want to find. When an attacker engages with one, Shadow sends a real-time alert with forensics to the security team. The team can then use this information to make intelligent choices to stop the attack and protect the business from harm.

Agentless Detection and Protection

Shadow's unique agentless dissolving binary approach helps both IT admins and security teams. Intelligent automation and a light operational footprint minimise the impact on IT. And unlike security tools that rely on software agents, attackers can't turn off or circumvent Shadow.

More Than 75 Deception Techniques

Shadow employs more than 75 active deceptive techniques. It creates fake files and file shares, database connections, FTP and RDP/SSH connections, browser histories and URLs, Windows credentials, network sessions, emails, scripts and even historical Teams chats that serve as hidden tripwires that appear to be truly valuable to attackers. These techniques work together to catch the attackers in the act, no matter where the compromise begins–inside or outside the environment.

With Shadow, security teams can automate the creation of hundreds of customised fake Word and Excel files that look just like the real ones; they can even include your company logo and letterhead. Fake data within the documents sets off alarms for security admins if an attacker tries to use it to gain further access.

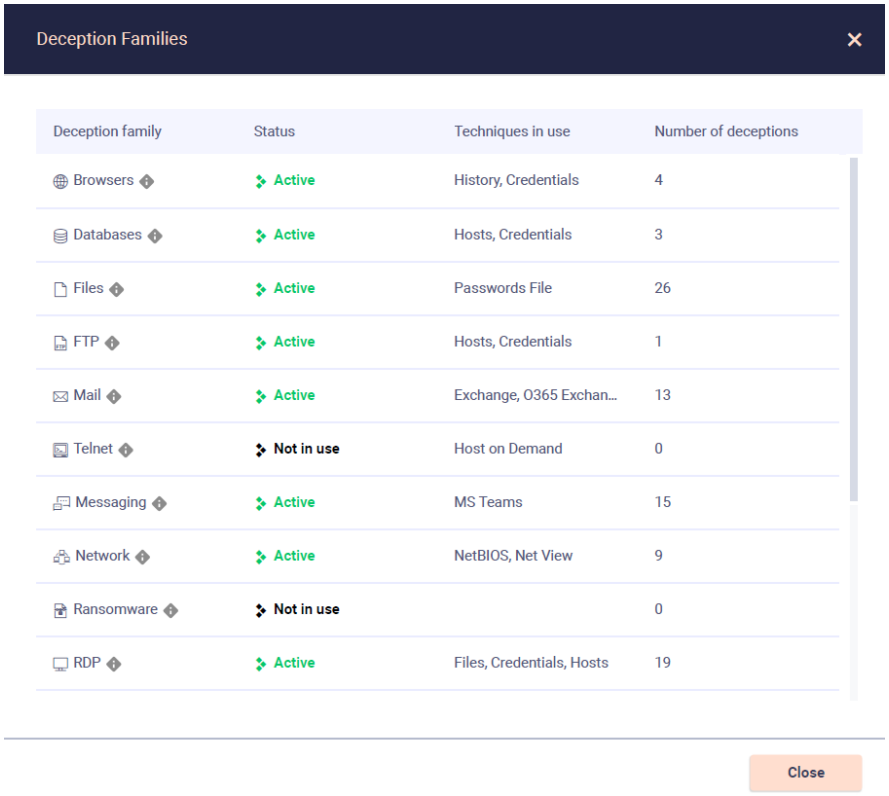

Figure 3. The Proofpoint Shadow user interface.

Automated Deception Customised to Each Endpoint

Shadow's intelligent automation system creates realistic and believable deceptions for attackers. It can easily adapt and scale without burdening the security team. Shadow analyses the endpoint landscape, designs tailored deceptions for each machine and deploys them with just one click. The solution also takes care of the ongoing process of adjusting and managing the deceptions over time.

A View From the Attacker's Perspective

Shadow's management console provides a wealth of forensics on attacker activity. It gives security teams important data about how close attackers are to your critical assets. It can also display a full timeline of what they were doing when they fell for the deceptions. And it can show security analysts what the deceptions look like from the attackers' point of view.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations 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**.