Proofpoint Spotlight

Automatische Erkennung, Priorisierung und Behebung von Identitätsschwachstellen, bevor Angreifer sie ausnutzen

Wichtige Vorteile

- Erkennung identitätsbezogener Risiken in mehreren Phasen der Angriffskette
- Überblick über Identitäten für Active Directory, Entra ID (ehemals Azure AD), PAM-Lösungen, Endpunkte, LAPS
- Automatische Erstellung einer priorisierten Liste der Identitätsschwachstellen auf Endpunkten
- Manuelle oder automatische Behebung von Schwachstellen wie Schatten-Administratoren
- Risiko-Transparenz über Tochtergesellschaften und neu übernommene Entitäten dank einer Karte der Domains eines Unternehmens, einschließlich Vertrauensstellungen
- Intelligente Berichte über langfristige Risikotrends zur Verbesserung der Identitätssicherheit

Diebstahl und Missbrauch von Anmeldedaten ist ein allgegenwärtiges und wachsendes Problem. Angreifer haben ihren Fokus geändert und greifen nicht mehr Systeme an, sondern nehmen Identitäten ins Visier. Für ihre Angriffe benötigen sie teilweise nur Stunden oder Minuten und hinterlassen dabei kaum Spuren einer Kompromittierung oder Malware.

Selbst wenn Lösungen zur Verwaltung privilegierter Zugriffe (Privileged Account Management, PAM) und Multifaktor-Authentifizierung (MFA) implementiert werden, ist einer von sechs Endpunkten durch privilegierte Identitäten gefährdet. Und genau diese Identitäten sind das primäre Ziel von Cyberangreifern bei Ransomware- und anderen gezielten Bedrohungen.

Proofpoint Spotlight hilft Ihnen, sich vor dem Missbrauch Ihrer Identitäten zu schützen. Als Bestandteil der Proofpoint Identity Threat Defense-Plattform ermöglicht die Lösung die kontinuierliche und umfassende Erkennung von Identitätsschwachstellen sowie die automatische Behebung dieser Bedrohungen. Proofpoint Spotlight wehrt Identitätsbedrohungen ab, bevor sie sich zu ausgewachsenen Kompromittierungen entwickeln können.

Entwickler aus dem Bereich der nationalen Verteidigung haben Proofpoint Spotlight entwickelt, um Sicherheitsteams die Priorisierung automatischer Behebungsmaßnahmen für Bedrohungen zu erleichtern. Eigentlich sollen Warnmeldungen Unternehmen vor Schäden bewahren, doch die steigende Zahl der Meldungen führt zu immer mehr irrelevanten Informationen, die vom Sicherheitsteam erst durchkämmt werden müssen.

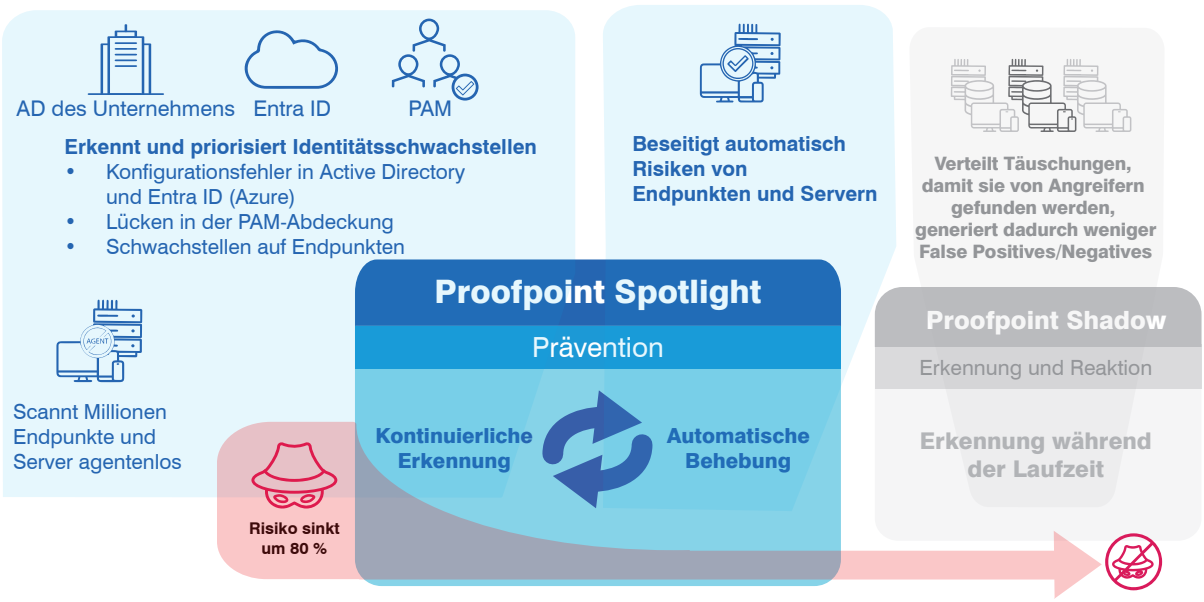

Abb. 1: Als Teil der Proofpoint Identity Threat Defense-Plattform ermöglicht Proofpoint Spotlight die kontinuierliche Erkennung und Behebung von Schwachstellen durch privilegierte Identitäten sowie von Richtlinienverstößen.

Wie Bedrohungsakteure privilegierte Identitäten missbrauchen

Wenn Angreifer zum ersten Mal einen Host erreichen, handelt es sich dabei selten um das eigentliche Ziel. Bei den meisten Angriffen versuchen die Bedrohungsakteure, ihre Rechte auszuweiten, damit sie sich lateral in der Umgebung bewegen und unbemerkt ihr Ziel erreichen können. Sie verwenden dabei Tools wie Bloodhound, Cobalt Strike, Mimikatz und ADFind, mit denen sie privilegierte Anmeldedaten schnell ausnutzen und ihre Präsenz verbergen.

Laut unseren Untersuchungen sind 90 % der Unternehmen im letzten Jahr Opfer einer identitätsbezogenen Kompromittierung geworden. Auch Ransomware-Angriffe haben ein neues Rekordniveau erreicht. Für diesen Anstieg gibt es viele Gründe. Einer davon ist, dass die Bereitstellung von Lösungen zur Identitäts- und Zugriffsverwaltung sehr komplex ist. Zudem ändern sich Identitäten laufend und vielen Unternehmen fehlt der Überblick über ihre Umgebung.

Dies sind weitere Gründe:

- Unvollständige oder falsche PAM-Konfiguration und Verwaltung von Anmeldedaten für Service-Konten, lokale Administratorkonten und privilegierte Domains
- Unbeabsichtigte Erstellung von Schatten-Administratorkonten mit übermäßigen Berechtigungen
- Nicht ordnungsgemäß getrennte RDP-Sitzungen
- Anwendungen (z. B. Browser, SSH, FTP, PuTTY und Datenbanken), die Anmeldedaten und Cloud-Zugriffs-Token im Cache von Endpunkten speichern

Reales Beispiel: Angriff auf ein Versicherungsunternehmen

Ein Bedrohungsakteur verschaffte sich mithilfe eines Credential-Stuffing-Angriffs über das Remote-Desktop-Protokoll (RDP) Zugang zu einem Netzwerk. Für den Erstzugriff nutzten die Angreifer gestohlene Anmeldedaten.

Anschließend erlangten sie Domain-Administrator-Berechtigungen. Kritische Daten wurden verschlüsselt und teilweise exfiltriert. Das Unternehmen zahlte ein Lösegeld von 40 Million US-Dollar, um seine Daten wiederherzustellen.

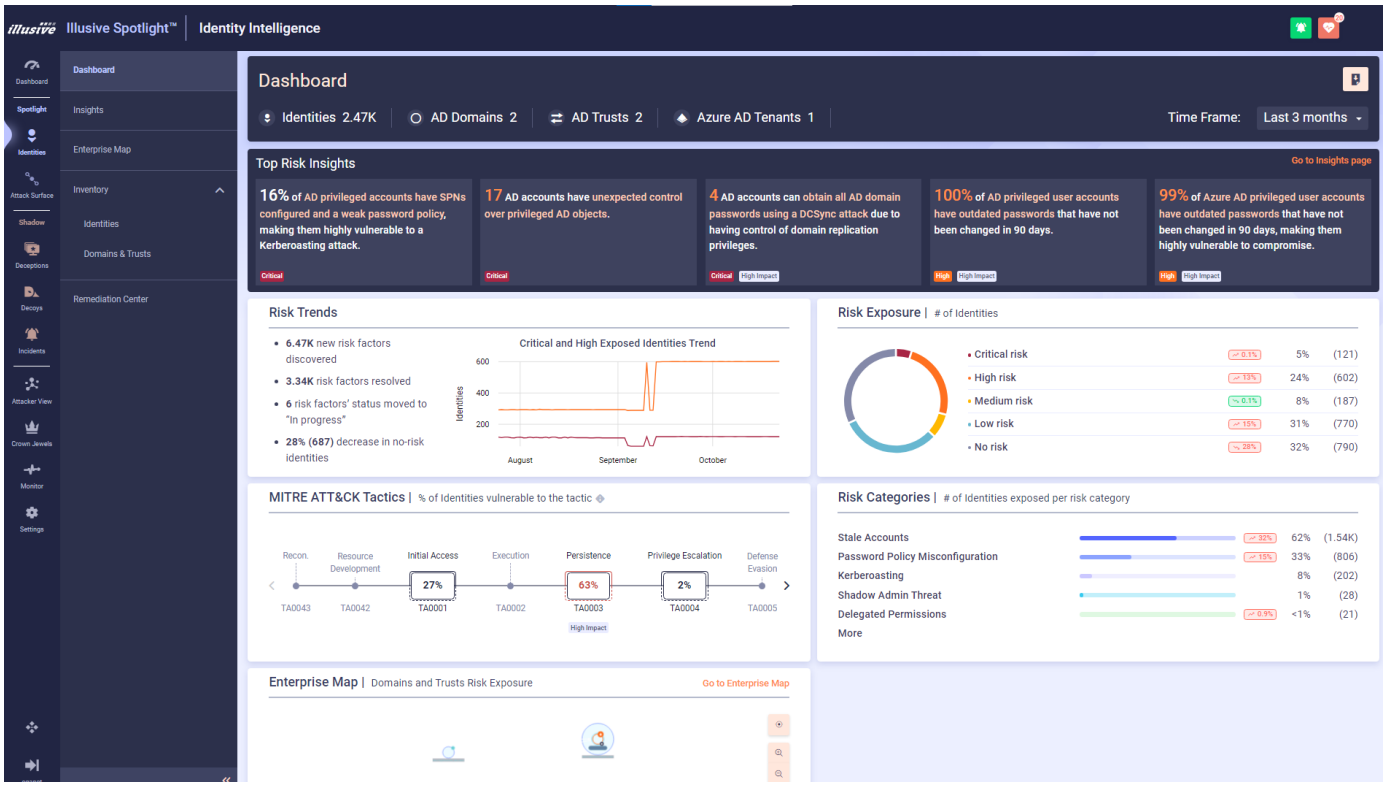

Abb. 2: Das Dashboard zu Identitätsrisiken in Proofpoint Spotlight.

Gefährdete Identitäten aufdecken, priorisieren und beheben

Proofpoint Spotlight deckt die Schwächen in Ihren Identitätssicherheitsrichtlinien und tatsächlichen Umgebungen auf. Um einen vollständigen Überblick und die Priorisierung aktueller Identitätsschwachstellen bereitzustellen, prüft die Lösung folgende Systeme:

- **Verzeichnisstrukturen:** Active Directory und Entra ID (ehemals Azure AD)
- **PAM-Lösungen:** CyberArk und Delinea Centrify
- **Endpunkte:** Clients und Server:
- **Aufgaben**

Proofpoint Spotlight behebt Identitätsschwachstellen, die Angreifer für die Ausweitung ihrer Kompromittierungen benötigen, und verhindert auf diese Weise Angriffe.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.