Proofpoint Shadow

Rechteerweiterungen und laterale Bewegungen in Echtzeit stoppen

Wichtige Vorteile

- Frühzeitige Erkennung von Angreifern und umfassende Untersuchung von Bedrohungen
- Weniger False Positives im SOC dank zuverlässiger Warnmeldungen
- Einfache Bereitstellung agentenloser Technologie mit geringem IT-Aufwand
- Kontinuierlicher Schutz durch dynamische Anpassung an Änderungen in der IT-Umgebung
- Bewährte Skalierbarkeit bei Netzwerken mit mehr als einer Million Endpunkten
- Schließung von Lücken, die bei Signatur- und Anomalie-basierter Bedrohungserkennung entstehen

Bei über 90 % der Cyberangriffe werden riskante Identitäten ausgenutzt. Die Angreifer haben ihre Strategie angepasst: Sie nehmen nun privilegierte Identitäten ins Visier und versuchen nicht mehr, Systeme direkt zu kompromittieren. Dies hat zu einem sprunghaften Anstieg erfolgreicher Ransomware-Angriffe und Datenkompromittierungen geführt. Durch die Fokussierung auf gefährdete Identitäten können Angreifer die Zeitspanne für ihre Attacken von Monaten auf einige Tage oder sogar Stunden verkürzen.

Proofpoint kann Ihnen helfen. Unsere leistungsstarke Lösung Proofpoint Shadow verwandelt Ihre Endpunkte in ein Netzwerk aus Täuschungen, sodass es für Angreifer beinahe unmöglich wird, sich unbemerkt lateral in Ihrem System zu bewegen. Als Teil der Proofpoint Identity Threat Defense-Plattform erkennt Proofpoint Shadow Bedrohungsakteure deterministisch an ihren Interaktionen mit scheinbar legitimen Pfaden auf Ihren Endpunkten, die jedoch in Wahrheit von uns platzierte Täuschungen sind.

Im Gegensatz zu anderen Tools ist Proofpoint Shadow nicht auf Signatur- oder Verhaltensanalysen angewiesen. Zudem verwendet die Lösung keine Agenten oder Honeypots, die missbraucht werden könnten. Stattdessen ermöglicht die agentenlose Architektur Täuschungen, die für Angreifer unauffällig operieren. Proofpoint Shadow hat sich bei mehr als 160 Red-Team-Übungen in weltweit führenden Sicherheitsorganisationen wie Microsoft, Mandiant, dem US-Verteidigungsministerium sowie Cisco bewährt.

Abb. 1: Angreifer nehmen im Verlauf der Angriffskette jetzt vor allem gefährdete Identitäten ins Visier.

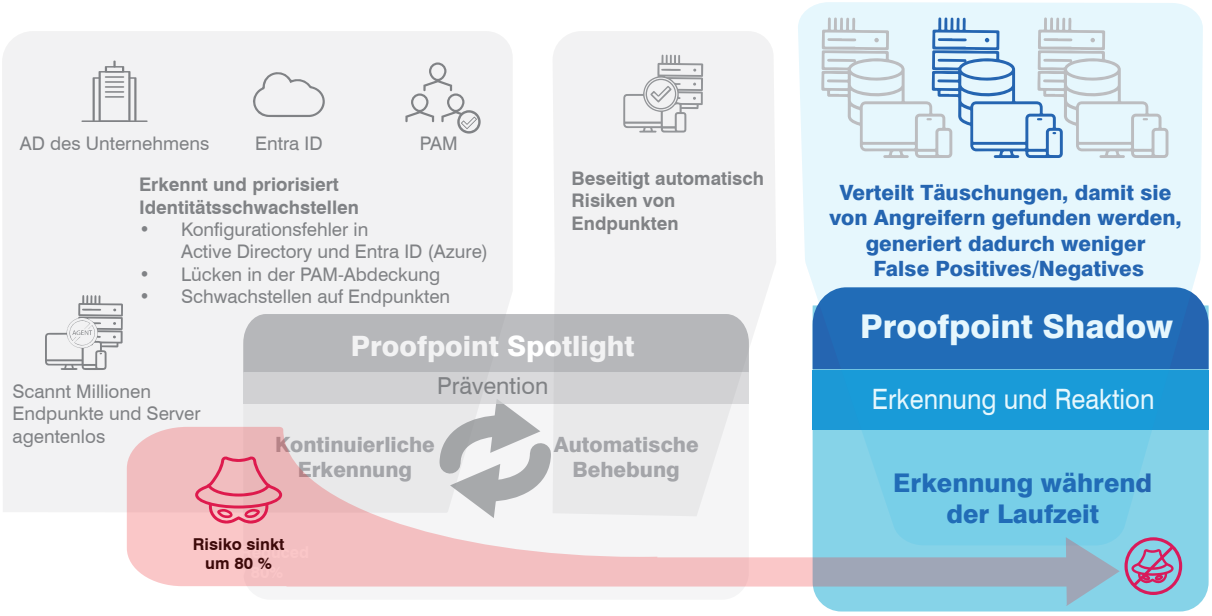

Abb. 2: Als Teil der Proofpoint Identity Threat Defense-Plattform erstellt Proofpoint Shadow ein Netzwerk aus Täuschungen, die laterale Bewegungen im Netzwerk erkennen und davor warnen.

Von probabilistischer zu deterministischer Erkennung

Bedrohungen lassen sich mit verschiedenen Methoden erkennen und abwehren. So kann beispielsweise nach ganz konkreten Mustern bzw. Signaturen gesucht oder das Verhalten eines potenziellen Bedrohungsakteurs analysiert werden. Konventionelle Tools scheitern häufig daran, schwerwiegende Angriffe mit Rechteerweiterungen oder unbemerkten lateralen Bewegungen im Netzwerk zu erkennen. Diese unzureichende Erkennung ermöglicht es Bedrohungsakteuren, Konten zu übernehmen, Ransomware zu übertragen oder Daten zu stehlen. Sicherheitsteams benötigen also einen moderneren und zuverlässigeren Ansatz, um diesen Angriffen einen Schritt voraus zu sein.

Proofpoint Shadow bietet einen deterministischen Ansatz. Die Lösung nutzt ein weit verteiltes Netzwerk von Täuschungen, um Akteure über die gesamte Angriffskette hinweg aktiv zu beschäftigen und ihre Aktivitäten zu verfolgen. Die Täuschungen sind tief in den Endpunkten des Unternehmens verborgen. Sie wirken wie echte Dateien, RDP-Sitzungen, Datenbankverbindungen, E-Mails, Skripte und andere Objekte, nach denen Angreifer suchen. Wenn diese sich mit einer Täuschung beschäftigen, schickt Proofpoint Shadow eine Echtzeit-Warnmeldung inklusive Forensikdaten an das Sicherheitsteam. Anschließend kann das Team anhand dieser Informationen gezielte Entscheidungen treffen, um den Angriff zu stoppen und das Unternehmen vor Schäden zu bewahren.

Agentenlose Technologie für Erkennung und Schutz

Der einzigartige agentenlose Ansatz von Proofpoint Shadow, der mehr Entscheidungsfreiheit bietet, hilft sowohl IT-Administratoren als auch Sicherheitsteams. Intelligente Automatisierung und ein geringer operativer Aufwand erleichtern IT-Teams die Arbeit. Und im Gegensatz zu anderen Sicherheitstools, die Software-Agenten einsetzen, können Angreifer Proofpoint Shadow nicht ausschalten oder umgehen.

Über 75 Täuschungstechniken

Proofpoint Shadow setzt mehr als 75 aktive Täuschungstechniken ein. Die Lösung erstellt falsche Dateien und Dateifreigaben, Datenbankverbindungen, FTP- und RDP/SSH-Verbindungen, Browser-Verläufe und URLs, Windows-Anmeldedaten, Netzwerksitzungen, E-Mails, Skripte und sogar Verläufe von Teams-Chats, die als unsichtbare Stolperdrähte fungieren und für Angreifer besonders attraktive Ziele sind. Durch die Kombination dieser Techniken können Sie Angreifer auf frischer Tat ertappen – unabhängig davon, ob die Kompromittierung innerhalb oder außerhalb Ihrer Umgebung beginnt.

Mit Proofpoint Shadow kann das Sicherheitsteam hunderte individuelle gefälschte Word- und Excel-Dateien erstellen lassen, die den echten in nichts nachstehen und sogar das Unternehmenslogo und den Briefkopf tragen können. Wenn die Angreifer versuchen, sich mit den falschen Daten aus den Dokumenten weiteren Zugriff zu verschaffen, erhalten die Sicherheitsadministratoren entsprechende Warnmeldungen.

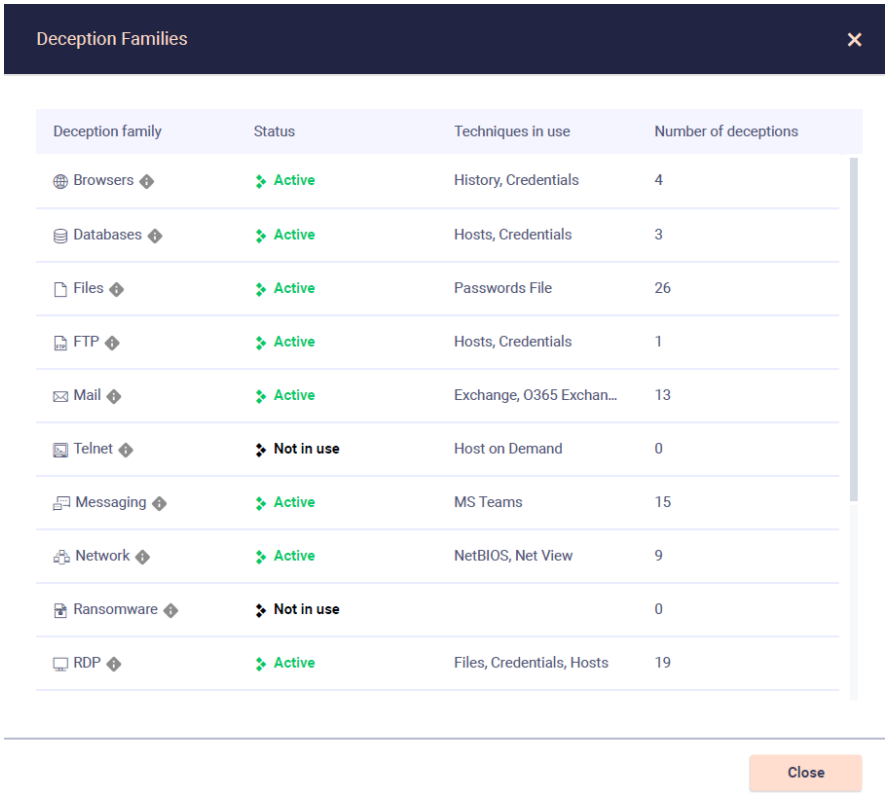

Abb. 3: Die Benutzeroberfläche von Proofpoint Shadow.

Automatisierte Täuschungen, die für jeden Endpunkt angepasst werden können

Das intelligente Automatisierungssystem von Proofpoint Shadow erstellt realistische und glaubwürdige Täuschungen für Angreifer. Die Lösung kann sich problemlos anpassen und lässt sich ohne Aufwand für das Sicherheitsteam skalieren. Proofpoint Shadow analysiert die Endpunkt-Landschaft und entwirft für jedes Gerät individuelle Täuschungen, die sich mit nur einem Klick bereitstellen lassen. Zudem übernimmt die Lösung die kontinuierliche Anpassung und Verwaltung der Täuschungen.

Die Perspektive der Angreifer

Die Verwaltungskonsole von Proofpoint Shadow bietet eine Fülle an Forensikdaten über Angriffsaktivitäten. Sie stellt dem Sicherheitsteam wichtige Informationen darüber bereit, wie nah Angreifer bereits an kritischen Assets sind. Zudem bietet sie eine vollständige Zeitleiste der Aktivitäten, die erfolgt sind, nachdem die Angreifer auf Täuschungen hereingefallen sind. Darüber hinaus kann sie Sicherheitsanalysten zeigen, wie die Täuschungen aus Sicht der Angreifer aussehen.

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**.

proofpoint.