Proofpoint Insider Threat Management

Personenzentrierte Abwehr von Insider-Bedrohungen für moderne Unternehmen

WICHTIGE VORTEILE

- Erkennung riskanter Insider-Aktivitäten und Verhinderung von Datenverlust auf Endpunkten
- Einfachere Reaktion auf Insider- und Datenverlust-Zwischenfälle
- Schnellere Rendite dank stark skalierbarer SaaS-Bereitstellung mit modernem Cloud-nativen Backend
- Gewährleistung der Anwender-produktivität durch ressourcen-schonenden Endpunkt-Agenten

WICHTIGE ANWENDUNGSFÄLLE FÜR PROOFPOINT ITM

- Identifizierung von Anwenderrisiken
- Schutz vor Datenverlust über Endpunkte
- Schnellere Reaktion auf Zwischenfälle durch Anwender
- Aufbau eines Programms zur Abwehr von Insider-Bedrohungen

Proofpoint Insider Threat Management (ITM) setzt auf einen personenzentrierten Ansatz zum Schutz vor Datenverlust, schädlichen Aktionen und Markenschädigung durch Insider. Wir schützen Sie vor nicht autorisierten sowie böswillig, fahrlässig oder unbewusst falsch handelnden Anwendern und korrelieren Anwenderaktivitäten und Datenbewegungen, um Datenschutzverletzungen durch Insider zu verhindern. Wir erkennen zudem riskantes Verhalten in Echtzeit und bieten leicht verständliche Nachweise zu Fehlverhalten.

Erkennung und Verhinderung von riskantem Verhalten in Echtzeit

Mit Proofpoint ITM lässt sich riskantes Verhalten auf Desktops, Servern sowie in virtuellen Umgebungen, Anwendungen und Dateien live korrelieren – während die betreffenden Anwender aktiv sind und nicht erst nach einem Zwischenfall. Wir stellen Echtzeit-Transparenz bereit, die effektive neue Möglichkeiten zur Korrelierung, Erkennung und Behebung von Insider-Zwischenfällen bietet.

Über Crowdsourcing zusammengestellte reale Bedrohungsszenarien

Erkennen Sie in Echtzeit riskantes Verhalten, zum Beispiel:

- Datenexfiltration
- Riskante laterale Datenbewegungen
- Missbrauch von Berechtigungen
- Missbrauch von Anwendungen
- Nicht autorisierter Zugriff
- Riskante versehentliche Aktionen

Mit unserem Regel-Baukasten, der auf boolescher Logik basiert, lassen sich problemlos Regeln und Auslöser erstellen, die für Ihre Umgebung maßgeschneidert sind.
Sie können die mitgelieferten Bedrohungsszenarien nutzen, bestehende ändern oder Szenarien völlig neu erstellen. Unsere umfangreichen Regeln zur Erkennung von Insider-Bedrohungen greifen auf das kollektive Wissen der CERT Division der Carnegie Mellon University, der NITTF, des NIST und unserer Kunden zurück.

Bedrohungssuche per Point-and-Click

Bei der Bedrohungssuche geht es nicht nur um externe Bedrohungen. Mit Proofpoint ITM können Sie Risiken durch böswilliges oder versehentliches Fehlverhalten durch Insider erkennen. Unsere Point-and-Click-Oberfläche erleichtert es Ihnen, ungewöhnlichem Verhalten proaktiv nachzugehen und danach zu suchen.

Die vereinfachte Point-and-Click-Suche bietet folgende Funktionen:

- Überprüfung riskanter Verhaltensweisen und Aktivitäten, angepasst an die Umgebung
- Nutzung intelligenter Gruppen, sodass tausende irrelevante Aktivitäten herausgefiltert werden können und Sie sich auf die relevanten konzentrieren können
- Einordnung anormaler Verhaltensweisen dank Kontext mit Zeitleiste und Screenshot-Nachweisen

Unterstützung bei Datenklassifizierung

Proofpoint Endpoint DLP integriert sich mit Microsoft Information Protection (MIP). Die Vertraulichkeitsbezeichnungen werden von unseren ITM-Agenten während der Interaktion des Anwenders mit der Datei in Echtzeit gelesen. Sie können Regeln für Erkennung und Verhinderung basierend auf der MIP-Vertraulichkeitsbezeichnung, Dateiherkunft, dem Dateitypen und Dateiziel festlegen.

Schutz vor Datenverlust

Proofpoint ITM kann die Exfiltration vertraulicher Daten über häufig genutzte Endpunkt-Kanäle verhindern. Dazu gehören über USB verbundene Geräte wie lokale Synchronisationsordner, NAS-Geräte (Network-Attached Storage), USB-Laufwerke, Multimedia-Geräte und Telefone. Der Schutz funktioniert auch, wenn der User offline ist.

Mit den folgenden Maßnahmen können Sie USB-Aktivitäten je nach Nutzer, Gruppe und Host verwalten:

- Blockierung von Schreibvorgängen auf USB-Geräte
- Erfassung bestimmter USB-Geräte in einer Liste vertrauenswürdiger Geräte
- Blockierung von Dateien, die mit Dateinamenmustern übereinstimmen
- Blockierung von Dateitypen
- Blockierung von Dateiquellen
- Durchsetzung globaler Verhinderungsregeln

Der Schutz der Proofpoint Enterprise DLP-Suite kann auf E-Mail- und Cloud-Anwendungen ausgeweitet werden.

Schnellere Reaktion auf Zwischenfälle

Viele Unternehmen leiten nach einem Sicherheitsereignis Initiativen gegen Insider-Bedrohungen ein und stellen dabei fest, dass die gewöhnlichen Workflows der vorhandenen Sicherheitstools nicht für Insider-Bedrohungen ausgelegt sind. Insider-Daten sind vertraulich und erfordern ein höheres Maß an Zusammenarbeit mit Teams, die nicht in Cybersicherheit involviert sind.

Sofortige Kontextinformationen und unwiderlegbare Beweise

Unsere Workflows sind für anwenderbezogene Zwischenfälle optimiert. Sicherheitsereignisse lassen sich über alle gesammelten Metadaten und Screenshots anhand von Schlüsselwörtern durchsuchen und filtern – Sie müssen also nicht extra eine neue Abfragesprache lernen. Die Filter können Sie für die proaktive Bedrohungssuche oder zur späteren Verwendung in einer Untersuchung speichern.

Bei der Ermittlung wichtiger Ereignisse und Warnmeldungen zu Untersuchungen können Sie diese kennzeichnen und kategorisieren. Bei der Weitergabe von Beweisen lassen sich die relevanten Ereignisse anhand dieser Kennzeichnungen wiederfinden und in übliche Dateiformate (z. B. PDF) exportieren. Die Berichte enthalten Beweise in Form von Screenshots und Kontextinformationen zum Wer, Was, Wo und Wann. Das vereinfacht die Verwaltung für das Cybersicherheitsteam und bietet verständliche Informationen für Personal-, Rechts- und Compliance-Abteilungen sowie Ermittler.

Vorteile der Proofpoint ITM-Architektur

Unsere Cloud-basierte Architektur ist auf Skalierung, Anwenderfreundlichkeit, Sicherheit und Erweiterbarkeit ausgelegt. Mit unserem branchenführenden ressourcenschonenden Endpunkt-Agenten werden Datenaktivitäten erfasst. Dadurch erhalten Sie einen umfassenden, anwendungsunabhängigen Überblick über die Aktionen von Anwendern auf ihren Systemen, ohne deren Arbeit zu behindern.

Reine SaaS-Bereitstellung

Proofpoint Endpoint DLP ist eine moderne SaaS-Plattform und für Skalierung, Analysen, Sicherheit, Datenschutz und Erweiterbarkeit ausgelegt. Einrichtungszeit und Kosten im Backend werden dadurch reduziert – gleichzeitig wird auch die laufende Verwaltung für Sicherheitsadministratoren im gesamten Unternehmen erleichtert. Damit ergibt sich die sofortige Transparenz über Datenaktivitäten.

Eine ressourcenschonende Lösung für zwei Probleme

Proofpoint Endpoint DLP und Proofpoint Insider Threat Management nutzen einen gemeinsamen ressourcenschonenden Agenten und eine moderne SaaS-Architektur. Werden beide Lösungen zusammen genutzt, bietet Proofpoint Endpoint DLP Schutz vor Datenverlustrisiken bei alltäglichen Aktivitäten, während Proofpoint ITM vor riskantem Verhalten böswilliger Anwender und Mitarbeitern mit höherem Risiko schützt.

WEITERE INFORMATIONEN

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