Schutz vor Insider-Bedrohungen

Proofpoint ITM schützt effektiv und proaktiv vor Bedrohungen, die aus dem firmeneigenen Netzwerk stammen.

Proofpoint ITM: die Highlights

- Identifizierung von Benutzerrisiken
- Vorbeugung und rasche Aufklärung von Insider-Vorfällen
- Unterbindung unautorisierten Datenabflusses (Data Loss Prevention)
- Einhaltung des Daten- und Mitarbeitendenschutzes
- Rasche Inbetriebnahme dank mehr als 400 mitgelieferten Regelwerken
- Kein Security-Spezialwissen für die Anwendung notwendig
- On-Prem-Installation

Gemäss dem Verizon Verizon Data Breach Investigation Report 2020 sind 30 Prozent der Datenschutzverletzungen auf Insider zurückzuführen – sei es durch bösartige Motive, Unwissen oder schlicht unachtsames Verhalten. Eigene Mitarbeitende und Auftragnehmer sind also signifikant mitverantwortlich für das Gesamt-Bedrohungsszenario. Dazu kommt, dass Insider-Bedrohungen in der Regel lange nicht erkannt werden und betroffene Unternehmen erst reagieren, wenn der Schaden schon angerichtet ist. Herkömmliche Cybersecurity-Lösungen genügen zur Abwehr von Insider-Bedrohungen und deren Folgen nicht. Die innovative Insider-Threat-Management-Lösung von Proofpoint geht einen anderen Weg: Proofpoint ITM erkennt Risiken von internen Sicherheitsvorfällen durch kontextbezogene Informationen und sammelt dazu Daten über User-Rollen, User-Aktivitäten, Alarme und Events von Drittsystemen wie SIEM-Lösungen sowie über Veränderungen und Verschiebungen von Daten. Auf Basis von mitgelieferten Regelwerken erkennt Proofpoint ITM jedes auffällige Verhalten und kann das Sicherheitsteam und die verantwortlichen User rechtzeitig informieren, noch bevor ein Schaden entsteht. Ist der Vorfall bereits geschehen, liefert die Lösung fallbezogene Informationen für eine rasche Aufklärung.

Proofpoint ITM schützt Unternehmen zuverlässig, proaktiv und DSGVO-konform vor Datenverlusten, schädlichen Aktionen von Mitarbeitenden und Markenschädigung sowie vor den anfallenden Behebungskosten, die durch böswillig, fahrlässig oder unbewusst falsch handelnde Insider entstehen.

proofpoint.

Herstellerflyer
proofpoint / ITM

Insider Threat Management mit Proofpoint ITM

Die Insider-Threat-Management-Plattform (ITM) von Proofpoint korreliert User-Aktivitäten und Informationen zur Bewegung von Daten und ermöglicht dem IT-Security-Team, User-Risiken zu erkennen, Datenverluste zu verhindern und schneller auf insiderbedingte Sicherheitsvorfälle zu reagieren.

Identifikation von User-Risiken

Proofpoint ITM nutzt raffinierte Analytik und greift auf bekannte Bedrohungsmuster zurück, um potenzielle Insider-Bedrohungen frühzeitig zu erkennen und abzuwehren. Eigene Mitarbeitende und Auftragsnehmer, die Zugriffe auf das firmeneigene Netzwerk besitzen, werden dabei kontrolliert. Dabei bleibt die Privatsphäre stets gewahrt: Die Lösung befolgt alle DSGVO-Vorgaben.

Zeitgerechte Reaktion auf Sicherheitsvorfälle

Mit Proofpoint ITM bleibt der gesamte Kontext rund um Insider-Sicherheitsvorfälle im Blick. Eine effektive Reaktion auf solche Incidents ist innert Minuten oder Stunden statt erst in Tagen oder Wochen möglich. Betroffene User und das Security-Team werden unmittelbar informiert. Beweismittel zur Entscheidungsfindung und zum Einleiten rechtlicher Schritte lassen sich rasch zusammenstellen, ohne dass dabei vertieftes IT-Wissen notwendig ist.

Umfassende Datenbasis

Die Daten für das User-Monitoring stammen aus unterschiedlichen Quellen, unter anderem von schlanken Agents, die auf den Endgeräten und Servern installiert sind, sowie von SIEM-Plattformen wie Splunk, QRadar, McAfee oder LogRhythm. Zur Analyse der Zugänge von externen Auftragnehmern dient ein dedizierter Server. Dank des mitgelieferten Regelwerks mit über 400 vorkonfigurierten Policies lässt sich Proofpoint ITM rasch und ohne Security-Spezialwissen in Betrieb nehmen und nutzbringend einsetzen.

Schutz vor Datenverlust

Komplette Visibilität auf Datenbewegungen bis hin zum Endpunkt – inklusive USB, Copy/Paste, Drucken, Eingaben via Befehlszeile, E-Mail, Webapps und Cloud-Speicher – ermöglicht es, unbefugten Datenabfluss unmittelbar zu erkennen, auf Basis von User-Aktivitäten in Echtzeit und applikationsspezifisch zu verhindern sowie Mitarbeitende entsprechend zu sensibilisieren. Eine übersichtliche Konsole sorgt für schnellen Überblick.

BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL
IT Security Distribution