proofpoint

PROOFPOINT THREAT PROTECTION FÜR MICROSOFT OFFICE 365

WICHTIGE VORTEILE

- Hervorragende Blockierung von Malware und anderen Bedrohungen
- Sofortige Übersichten und Erkenntnisse
- Schnellere Reaktion auf Bedrohungen
- Sicherheitskompetenz des Threat Operations Center
- Gewährleistung der E-Mail-Verfügbarkeit

Wenn Ihr Unternehmen nach einer Möglichkeit zur Migration zu Microsoft Office 365 sucht, fragen Sie sich wahrscheinlich, ob Sie zusätzlichen Schutz benötigen.

Da Microsoft weiterhin die Sicherheit der eigenen Infrastruktur ausbaut, nutzen Bedrohungsakteure zur Überwindung der Cybersicherheitsmaßnahmen heute vor allem den Faktor Mensch aus.

E-Mails sind die zuverlässigste Methode, um jede Person in allen Unternehmen auf der ganzen Welt zu erreichen. Daher setzen mehr als 90 Prozent der gezielten Angriffe auf E-Mails, um Ihr Netzwerk zu kompromittieren sowie Anmeldeinformationen und Assets zu stehlen.

Proofpoint Threat Protection für Office 365 schützt Benutzer vor hochentwickelten Bedrohungen und gezielten Angriffen. Diese Lösung stellt Bedrohungsdaten bereit, mit denen Sie diese Angriffe identifizieren können. Zudem erhält Ihr Sicherheitsteam Unterstützung bei der Koordinierung der schnellen Reaktion und Eindämmung. Die Funktion für kontinuierliche E-Mail-Verfügbarkeit gewährleistet, dass Sie Ihre E-Mails jederzeit nutzen können. Unser preisgekrönter Kunden-Support spiegelt unser Engagement für Ihren Erfolg wieder.

HERVORRAGENDE SICHERHEIT

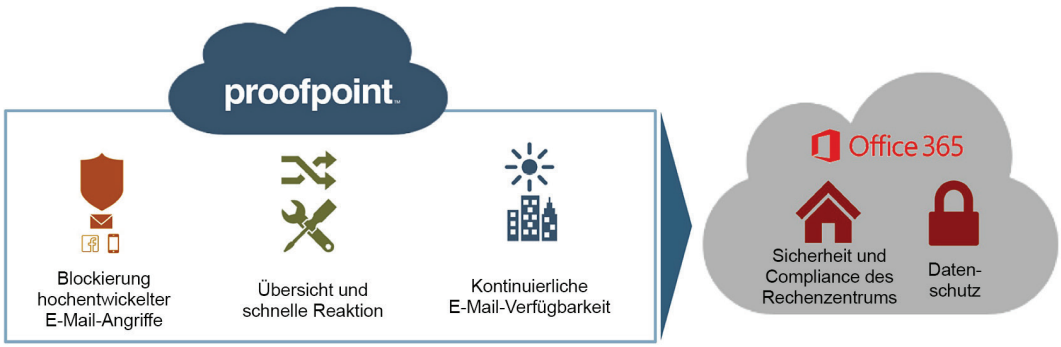
Die Proofpoint-Bedrohungsdaten decken E-Mails, Netzwerke, Mobilgeräte-Apps und Social Media ab. Mit diesem Ansatz der nächsten Generation können Sie branchenführende E-Mail-Hygiene gewährleisten und Spam-E-Mails effektiv abwehren. Außerdem werden neue, nie zuvor gesehene Angriff in Office 365-E-Mail-Umgebungen erkannt.

Ältere Techniken, die sich auf die Reputation von Host, URL und Anhängen verlassen, bieten heute keinen ausreichenden Schutz mehr. Stattdessen benötigen Sie eine moderne Lösung, die Ransomware, BEC (Business Email Compromise), Anmeldedaten-Phishing sowie weitere Bedrohungen abwehrt.

Proofpoint analysiert Bedrohungen in mehreren Stufen mit verschiedenen Ansätzen, um das Verhalten, den Quellcode sowie das Protokoll zu überprüfen. Die prädiktive Analyse identifiziert verdächtige URLs sowie Anhänge und prüft sie in Sandboxes, bevor Benutzer darauf klicken können.

MEHR ÜBERSICHTEN UND ERKENNTNISSE

Übersichten sind von zentraler Bedeutung, wenn Sie Bedrohungen aufdecken, die allgemeine Cybersicherheit verbessern und die Geschäftsziele unterstützen möchten. Da Sicherheit mittlerweile auch in der Unternehmensführung diskutiert wird, ist es jetzt noch wichtiger, die Fragen nach dem „Wer, was, wann, wo und wie“ für Zwischenfälle beantworten zu können. Wenn Sie wissen, ob ein Angriff gegen Ihr Unternehmen Bestandteil einer breiter angelegten Kampagne ist, für Ihre



Proofpoint Threat Protection für Microsoft Office 365

Branche zugeschnitten wurde oder ausschließlich gegen Ihr Unternehmen gerichtet ist, können Sie Ihre Maßnahmen besser priorisieren.

Wenn Sicherheitsverantwortliche in Echtzeit auf wichtige Forensikergebnisse zugreifen können (z. B. welcher Benutzer auf welchem Gerät auf welchen Link geklickt hat, DNS-Suchen, Änderungen von Registrierungsschlüsseln), können sie schnell auf hochentwickelte Bedrohungen reagieren. Statt sich darauf zu konzentrieren, was passiert ist, müssen Sie den Schwerpunkt auf die geeignete Reaktion verlegen.

SCHNELLERE REAKTION AUF BEDROHUNGEN

Automatischer Abruf spart Bereinigungskosten
Sparen Sie wertvolle Stunden, die Sie bisher mit der Extrahierung von E-Mail-Bedrohungen aus Office 365- und Exchange-Postfächern verbracht haben. Diese leistungsstarke Schutzebene gegen aufkommende Bedrohungen verarbeitet Echtzeit-Bedrohungswarnungen vor schädlichen URLs sowie Anhängen und verschiebt identifizierte E-Mails in einen Quarantänebereich, auf den die Endbenutzer nicht zugreifen können. Zu jeder Aktion wird eine Task-Historie zur ergriffenen Schutzmaßnahme erstellt. Sie definieren die Regeln: Sollen E-Mails automatisch oder auf Anforderung extrahiert werden? Möchten Sie die E-Mail zur Überprüfung aufbewahren oder für einen kurzen Zeitraum speichern und anschließend automatisch löschen?

Schnelle Auswertung und Bestätigung von Kompromittierungen
Wenn ein Zielsystem eine schädliche E-Mail erhalten hat, wie können Sie herausfinden, ob dieses System bereits kompromittiert wurde? Dank automatisierter Forensiksammlung und Kompromittierungsprüfungen für Endgeräte erfahren Sie schnell, welche Reaktionen Priorität erhalten sollten. Unternehmen müssen nur einen Teil der betroffenen Systeme beheben und erhalten dadurch eine skalierbare Möglichkeit zur Risikominderung sowie zum Schutz ihrer Marke.

INTEGRATIONSMÖGLICHKEITEN:

Zusätzliche Erkenntnisse zu Bedrohungen
- Palo Alto Networks
- Splunk

URL-Erzwingung
- Blue Coat
- Open DNS

Netzwerkerzwingung
- Cisco
- Check Point
- Fortinet
- Juniper
- Palo Alto Networks

Erzwingung des Benutzerzugriffs
- Active Directory
- Cyberark
- Imperva

Intelligentere Sicherheitsinvestitionen
Nur mit einem integrierten Ansatz können Sie ein nachhaltiges Sicherheitsprogramm aufbauen und dafür sorgen, dass Ihre Sicherheitsinvestitionen intelligenter sowie schneller funktionieren und Ihre ROI steigern. Dank Proofpoint können in Office 365-E-Mails gefundene Ereignisse in Echtzeit in Ihr vorhandenes Sicherheits-SIEM integriert und E-Mail-Daten mit anderen Datenpunkten in Ihrem Netzwerk korreliert werden. Mit automatisierten oder koordinierten Reaktionen über bestehende URL-, Netzwerk- oder Benutzer-basierte Erzwingungspunkte kann ausgehende Kommunikation mit Steuerungsnetzwerken schnell unterbunden, kompromittierte Benutzer in Gruppen ohne Berechtigungen verschoben oder andere Maßnahmen definiert werden.

Volles Engagement für Ihren Erfolg: Unsere Bedrohungsexperten
Ihr Erfolg steht an erster Stelle, und dediziertes Sicherheits-Know-how ist schwer zu finden. Zusätzlich zu unserer preisgekrönten weltweiten Produkt-Support-Abteilung bietet das Threat Operations Center einen ganz besonderen Vorteil für unsere Kunden. Dieses Team besteht aus herausragenden Bedrohungsforschern und ist rund um die Uhr tätig. Es fungiert als Erweiterung Ihres Sicherheitsteams und nutzt hochentwickelte Bedrohungsanalysen, um Ihnen die Kontextinformationen und Erkenntnisse zur Verfügung zu stellen, die Sie zum Verständnis der Akteure bzw. Kampagnenaktivitäten in Ihrer Umgebung sowie zur Priorisierung der Bedrohungen benötigten.

GEWÄHRLEISTUNG DER E-MAIL-VERFÜGBARKEIT

Wenn es in irgendeiner Form zu einem Ausfall kommt – sei es auf Seiten von Microsoft oder durch Authentifizierungsprobleme auf Ihrer Seite – können Sie problemlos über ein Webportal nativ auf Outlook zugreifen. Während Ihr IT-Team die Kontrolle wiedererlangt, ist der Zugriff weiterhin über einen ständig aktiven sekundären E-Mail-Dienst möglich, der die Posteingangsdaten der letzten 30 Tage liefert. Dadurch ist die Verfügbarkeit nicht mehr von nur einem Anbieter abhängig.

WEITERE INFORMATIONEN

Entscheiden Sie sich für Funktionen zur Verbesserung der Sicherheit und Übersicht, zur schnelleren Reaktion sowie zur Gewährleistung der Verfügbarkeit, damit Ihre Office 365-Implementierung ein voller Erfolg wird. Zusammen mit unserem preisgekrönten weltweiten Support-Team hat Proofpoint bereits vielen Unternehmen dabei geholfen, vor, während und nach dem Wechsel zu Office 365 einheitliche und zuverlässige Sicherheit zu erreichen. Weitere Details sowie Informationen dazu, wie Sie sich für eine Bedrohungsbewertung anmelden können, finden Sie unter www.proofpoint.com/office365.

INFORMATIONEN ZU PROOFPOINT
Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.