



## TEAMS PROTECTION

E-Mails sind nach wie vor der häufigste Angriffsvektor, aber es gibt weitere Einfallstore für Cyberbedrohungen, die nicht unterschätzt werden sollten. Da immer mehr Mitarbeiter Instant Messaging gegenüber E-Mails bevorzugen, gewinnt Microsoft Teams als Angriffsvektor zunehmend an Bedeutung. Dabei nutzen Cyberkriminelle bösartige Links und Malware, die sie per Chatnachricht versenden. Für CISOs bedeutet das eine zusätzliche Herausforderung: Ohne vollständigen Überblick über sämtliche potenzielle Angriffsvektoren bleiben gefährliche Sicherheitslücken bestehen.

### PAIN POINTS:

- » Mangelnde Sichtbarkeit schädlicher Inhalte, die über Teams geteilt werden.
- » Endbenutzer sind ständig potenziell schädlichen Nachrichten ausgesetzt.
- » Microsoft Teams entwickelt sich über ein internes Kommunikationstool hinaus, da Benutzer zunehmend externe Konversationen führen.
- » Die Effizienz leidet, da Endbenutzer und ihre IT-Teams sich mit schädlichen Links und Malware auseinandersetzen müssen.



### SCHÜTZEN SIE IHRE SYSTEME UND IHRE MITARBEITER MIT TEAMS PROTECTION.

Teams Protection schützt Endbenutzer vor kompromittierten internen Konten, indem alle Nachrichten mit URLs gescannt werden. Wenn eine Bedrohung erkannt wird, erscheint sofort eine Warnmeldung im Chatverlauf durch den AI Cyber Assistant Bot. Teams Protection verwendet KI-Technologien aus Hornetsecuritys Secure Links:

- » Intelligente Muster analysieren Schlüsselmerkmale von URLs und Webseiten (z. B. Weiterleitungen, Dateipfade, Skripte etc.), um schädliche Inhalte zu identifizieren.
- » Überwachtes und unüberwachtes maschinelles Lernen analysiert mehr als 47 Merkmale von URLs und Webseiten, um bösartiges Verhalten, Verschleierungstechniken und URL-Weiterleitungen zu erkennen.
- » Deep Learning: Computervisionmodelle analysieren Bilder, um relevante Merkmale zu extrahieren, die in Phishing-Angriffen verwendet werden – einschließlich Markenlogos, QR-Codes und verdächtiger Textinhalte, die in Bilder eingebettet sind.



## WICHTIGSTE VORTEILE:

- » Teams Protection schützt einen Tenant vor schädlichen Nachrichten, indem es KI und maschinelles Lernen nutzt, um URLs zu scannen, die von externen Benutzern oder kompromittierten internen Konten gesendet werden.
- » Teams Protection implementiert einen Bot, der Benutzer automatisch warnt, wenn ein schädlicher Link empfangen wird.

## ÜBERBLICK ÜBER ZENTRALE FUNKTIONEN:

- » Analyse aller direkten Nachrichten und Kanalnachrichten, die über Teams an einen Microsoft 365 Tenant gesendet werden.
  - » Wenn eine Nachricht als schädlich identifiziert wird, erhält der Endbenutzer eine Warnung vom Bot.
- » Implementierung spezieller Protokollansichten mit Warnungen zu schädlichen Nachrichten.
- » Manuelle Gegenmaßnahmen über das Kontrollpanel durch den Administrator, der in der Lage ist:
  - » Eine gesamte Teams-Konversation zu löschen, die schädliche Nachrichten enthält.
  - » Den Absender einer schädlichen Nachricht daran zu hindern, sich bei Teams anzumelden.