HORNETSECURITY

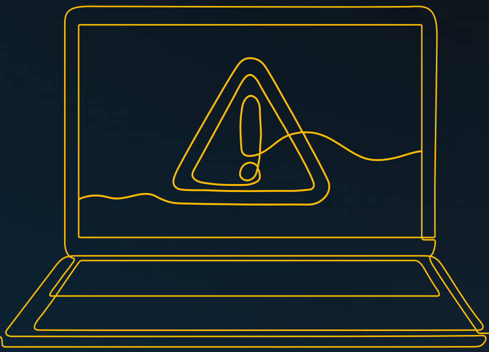
VALUE
PROPOSITION

TEAMS PROTECTION

While email remains the most common attack vector, cyber threats have other points of entry which should not be underestimated. With more and more employees preferring instant messaging to email, Microsoft Teams can only continue to grow as an attack vector, with cyber criminals utilizing malicious links and malware sent by either externally open Teams or compromised internal accounts.
For CISOs, it means added worries, as even the most meticulous and experienced ones are powerless if they don't have clear visibility over every possible attack vector.

PAIN POINTS:

- Lack of visibility over malicious content shared via Teams.
- End users are constantly exposed to potential malicious message.
- Microsoft Teams is evolving beyond an internal communication tool, as users begin more and more external conversations.
- Efficiency suffers as end users and their IT teams have to deal with malicious links and malware.



KEEP YOUR SYSTEMS SECURE AND YOUR EMPLOYEES SAFE WITH TEAMS PROTECTION

Teams Protection protects a tenant from internal compromised accounts by scanning all messages containing URLs, immediately issuing a warning message in the conversation through the AI Cyber Assistant bot. Teams Protection utilizes AI technology used in Hornetsecurity's Secure Links:

- Smart patterns analyze key features of URLs and pages (e.g. re directions, file paths, scripts, etc.) to identify malicious content.
- Supervised and unsupervised machine learning algorithms analyze more than 47 characteristics of URLs and web pages, scanning for malicious behaviors, obfuscation techniques, and URL redirects.
- Deep learning: Computer Vision models analyze images to extract relevant features used in phishing attacks, including brand logos, QR codes, and suspicious textual content embedded within images.

TOP BENEFITS:

- Teams Protection protects a Tenant from malicious messages by using AI and machine learning to scan URLs sent by external users or compromised internal accounts.
- Teams Protection implements a bot that automatically warns users when a malicious link is received.

HIGH-LEVEL FEATURE OVERVIEW:

- Analysis of all direct and channel messages received through Teams by a Microsoft 365 tenant.
  - If a message is identified as malicious, the end user receives a warning from a bot.
- Implementation of dedicated log views with alerts for malicious messages.
- Manual remediation with the Control Panel enables Admins to:
  - Delete an entire Teams conversation containing malicious messages.
  - Prevent the sender of a malicious message from logging into Teams.