DARKTRACE

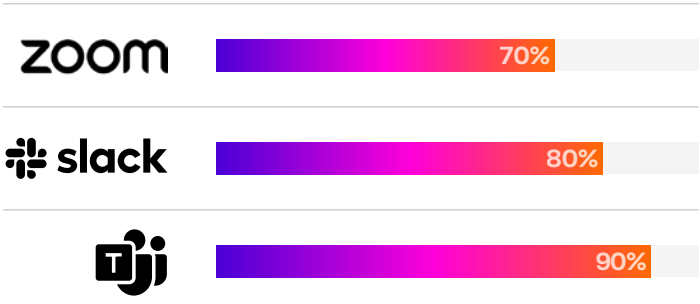
/ EMAIL ADD-ON MODULES

Secure every interaction, wherever it happens

Industry-first cross channel full-message analysis for email, Slack, Teams, and Zoom

Reveal novel threats and cross channel attack paths with a unified engine analyzing full message content **across your key communication channels.**

Messaging and collaboration tools are becoming an essential for daily business communications – the majority of the Fortune 100 companies use:



Attackers have noted this shift, crafting blended campaigns that move fluidly across email, messaging, and collaboration tools. However, most cross-channel security tools still build their email, messaging and collaboration solutions as separate architectures, offering shallow, channel specific controls that provide fragmented visibility into how modern attacks move across the workspace.

Collaboration tool security measures are often primarily focused on identifying malicious payloads by correlating threat intelligence (delivered via URLs or attachments), which fail to account for the rise in novel payloads and payload-less attacks, such as plain text social engineering, or pretexting, where an attacker communicates via various different avenues to boost implicit trust.

Additionally, these platforms are increasingly enabled as external collaboration tools to allow users to work seamlessly with third parties. Exposing employees to external users opens up a world of security risks, exacerbated by their perception as internal tools which means that users let their guard down – making them a prime target to launch a phishing, social engineering or sophisticated payload attack without being detected or blocked.

Unified email and messaging security for **every channel**

Darktrace's messaging security extends its leading behavioral analysis across Teams, Zoom, and Slack, analyzing full message content and correlating it with inbox activity. One AI engine analyzes intent, tone, relationships, and conversation flow across all major communication platforms, stopping blended, multistep attacks that siloed tools miss.

Extends Darktrace's proven Self-Learning AI approach

Just like email, every message is analyzed against the user's normal behavior, including language patterns, relationship history of sender and recipient, tone and payloads – to understand if a message poses a threat. Using this understanding, it can detect malicious payloads and payload-less attacks, even if a harmful link or attachment is never delivered.

Eliminate cross-channel blind spots

Darktrace detects phishing, malware, account takeover attempts, and conversational manipulation across Slack, Teams, Zoom, and email, so attackers can't use collaboration apps as a new entry point, escalation path, or pretext building space – giving analysts a single, coherent view instead of fragmented, channel specific gaps.

Secure both insider threat and external attacks

Even if a suspicious message comes from a trusted user – whether they are internal or a trusted third-party vendor – Darktrace analyzes it against the behavioral profile of that user, protecting organizations from internal and supply chain risk.

Correlate messaging and collaboration activity with email and account environments

Suspicious messaging activity raises alarm bells for that user's other communication platforms, and vice versa, for a quick understanding of compromise. Signals from messaging and collaboration activity also help to augment Darktrace's understanding of a user, improving detection across the entire organization.

Simplify investigations with a single workflow for your communication ecosystem

Security teams get a full picture of attacks in real time, with a unified console showing inbound, outbound, lateral mail, messaging and collaboration alerts within a single workflow.

The Darktrace differentiator: **Messages > payloads**

Most messaging security solutions focus on payloads, i.e. malicious links and attachments delivered in chat, groups, and channels. These solutions can't detect payloadless attacks. Equally, they can only identify payloads they've seen before. Novel payloads, such as zero-day links, will slip through without detection.

Darktrace protects in all cases that other solutions can't, by analyzing the content and context of the messages themselves, in order to determine if they are unusual or malicious, not just those with payloads. It's the only solution that secures against the full spectrum of attacks – malicious payloads, pre-texting, social engineering, novel payloads and zero-days. And as new threat types continue to evolve, from novel AI-driven techniques to everyday workflow abuse, Darktrace's unified behavioral models continuously adapt. driven techniques to everyday workflow abuse, Darktrace's unified behavioral models continuously adapt.

Darktrace analyzes every message for payloads for hundreds of metrics encompassing payloads, account signals, and subtler contextual indicators of social engineering based on content and context

NEED TO KNOW:

Customers must have Darktrace / EMAIL installed to benefit from any of the following Add-ons: Darktrace / EMAIL – TEAMS, Darktrace / EMAIL – ZOOM, Darktrace / EMAIL – SLACK.

Customers need one of the following licenses to deploy the Teams module: Office 365 E5/A5/G5

Microsoft's current API infrastructure doesn't allow third-parties to take actions within Teams via autonomous response **– customers are alerted and notified for Teams threats in the console.**

SEE HOW DARKTRACE HANDLES MESSAGING THREATS IN ACTION.

Video demo ↗

Get a demo ↗