Darktrace Cyber AI: Compromised SaaS Credentials

Given the sheer amount of data that passes through SaaS environments and the speed of digital business afforded by these spaces, compromised credentials can allow threat actors to surreptitiously launch attacks that spread fast and far.

Today's digital workforce leverages a wide variety of SaaS platforms to handle critical operations and sensitive information, from customer data and financial records to valuable intellectual property. A lack of visibility in SaaS accounts can expose the organization to operational disruption, data loss, and hefty compliance and remediation expenditures.

Criminals can gain access to corporate SaaS accounts in several ways, from social engineering and spear phishing attacks, to automated brute-force attempts, which can be extremely effective if employees have weak passwords or lack multi-factor authentication. Passwords can even be leaked inadvertently – for instance, if a user accidentally leaves login details in an open-source code repository. Yet whatever the method, threat actors are often just one successful attempt away from stealing the crown jewels of an organization.

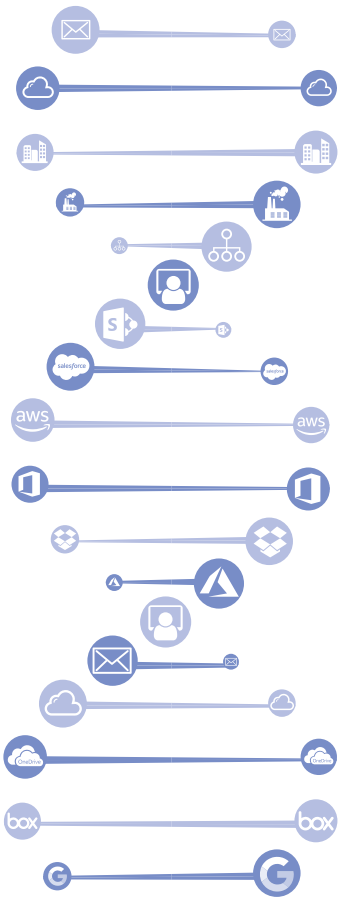
Both native and third-party security tools lack the ability to spot subtle patterns of malicious behavior within SaaS platforms, instead relying on static rules and pre-defined policies. This approach leaves organizations with limited visibility and control over their SaaS infrastructure. Moreover, siloed security tools are unable to correlate workforce behaviors in SaaS with activity in the rest of the organization, and thus fail to see the full extent of an attack that involves compromised SaaS credentials.

Cyber AI: Identifying the Subtle Signs of Credential Compromise

It takes the immune system approach of Darktrace's Cyber AI Platform to detect threat actors with compromised SaaS credentials. Just like the human body, Darktrace uses a bespoke understanding of 'self' for an organization and its workforce to identify subtle deviations from normal that indicate an emerging threat. Instead of relying on simple and static rules, Cyber AI builds a multi-dimensional understanding of normal workforce behavior in SaaS environments to detect the weak indicators of account compromise.

Even when an attacker hides behind legitimate SaaS credentials, Darktrace's self-learning AI will still detect the subtle signs that the user behind the login is not who they appear to be, ensuring that the impact of attacks can be mitigated. By learning the normal 'pattern of life' of every user in the business, Darktrace is also the only solution that can correlate fragmented workforce behaviors in SaaS services with activity in the rest of the organization. With enterprise-wide context, organizations can avoid security siloes, using self-learning AI to see the larger incident and detect every step of an attack involving compromised SaaS credentials.

> "Less than 1/3 of businesses are monitoring abnormal user behavior across their cloud footprint. This is alarming considering the significant increase in usage of cloud apps and collaboration platforms."
>
> **Cybersecurity Insiders**



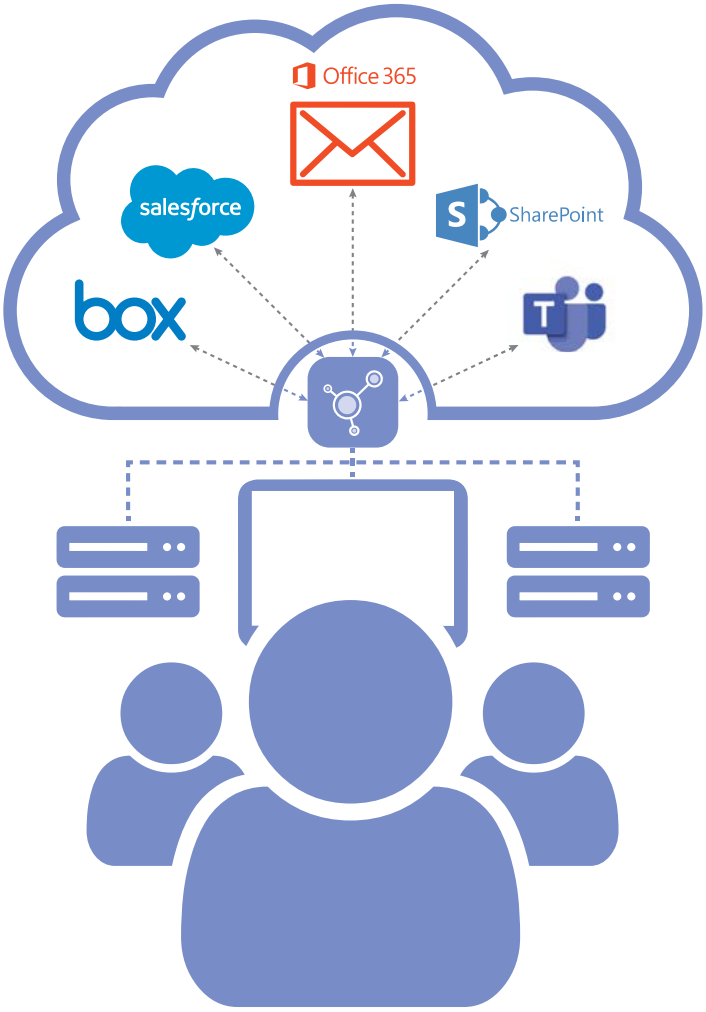
Case Study: Microsoft 365 Compromise and SharePoint Infiltration

At a US-based insurance company, Darktrace Cyber AI's bespoke knowledge of workforce behavior and visibility across SaaS platforms was crucial for stopping an attack that started with a compromised Microsoft 365 account.

When a threat actor successfully logged in to one of the client's Microsoft 365 accounts from an IP address located in the United Arab Emirates, Cyber AI identified the behavior as anomalous, as no other Microsoft 365 accounts had ever been observed logging in from this IP address. Four days later, another rare IP located in the UAE was seen accessing the same compromised account. This time, the threat actor set up a new email rule, and further used their illegitimate access to read and write to files on the user's personal SharePoint account.

Darktrace Cyber AI had not previously seen any other user accounts communicating with UAE-based IPs from the particular network identified in these incidents, indicating that the observed behavior was highly unusual for the customer and the result of compromise.

While the customer's legacy tools only allowed them to see the threat when changes were made to the compromised account that broke the pre-configured rules, Darktrace Cyber AI picked up on the anomalous behavior as soon as it occurred and clearly illuminated the attacker's movement between SaaS services. Darktrace was able to alert the security team immediately of the earliest stages of the attack, shining a light on every detail and assuring the threat was neutralized before serious damage could occur.



Darktrace Cyber AI is designed to protect the dynamic employees in your organization – no matter where they work, or the nature of their applications.