Darktrace Cyber AI: Malicious SaaS Administrator

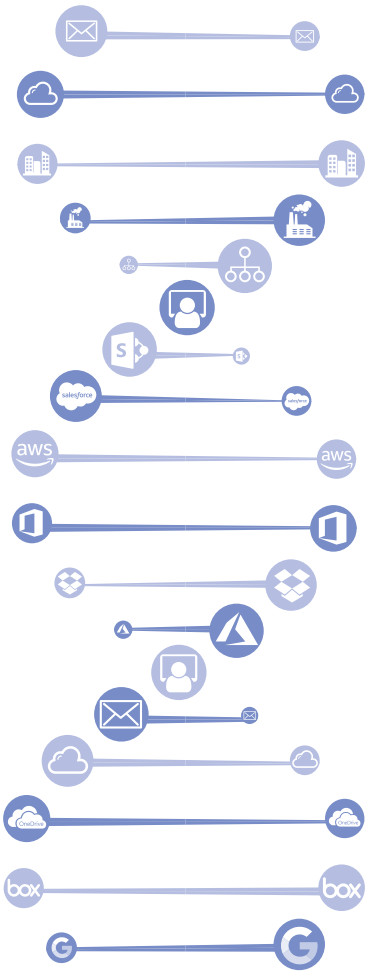
Identifying malicious administrator activity in SaaS platforms is a critical security concern. Whether their motive is fraud, IP gain, or sabotage, administrators who take advantage of their position to damage the company may be one of the most insidious types of insider threats.

Managing SaaS user privileges and activity is already a challenge for security teams, with most defenses relying on simple rules and incompatible controls to monitor these complex environments. This static approach to security is often insufficient – a disquieting fact that is exacerbated when a trusted administrator becomes an insider threat.

Administrators typically have elevated privileges and understand SaaS platforms better than anyone, which means most native and third-party security tools will fail to see subtle malicious behavior. Because these tools have limited visibility, armed only with basic analytics and static policies, they are unable to spot the nuanced behavioral shifts that indicate a malicious administrator. Traditional SaaS security solutions are also siloed from the rest of the network, and therefore cannot connect workforce behaviors across an organization to illuminate the greater narrative of malicious activity when an insider becomes a threat.

This leaves companies vulnerable to serious data loss and damage to operations. Moreover, should customer or employee data be exposed, businesses likely face severe privacy and compliance violations, accompanied by reputational damage, legal liabilities, and financial burden. Considering the massive amount of sensitive data that passes through Salesforce accounts, or the business-critical information that may sit in Box environments, it is clear that organizations require a more adaptive and unified approach to threat detection in this area.

> “Darktrace AI adapts while on the job, illuminating our network and cloud infrastructure in real time, and allowing us to defend the cloud with confidence.”
>
> **CISO, Aptean**



Cyber AI: Detecting Stealthy Insider Threats

Darktrace’s Cyber AI Platform ensures that malicious activity from administrators in SaaS environments is no longer a blind spot. Rather than using pre-configured rules, Darktrace Cyber AI analyzes all SaaS traffic with proprietary AI, building a deep understanding of normal workforce behavior for your entire organization. The power of self-learning Cyber AI allows Darktrace to identify even the most subtle deviations from normal that indicate an insider threat.

Instead of assuming trust, Darktrace Cyber AI uses its evolving knowledge of behavior in SaaS platforms to detect when insiders turn malicious, catching even those nefarious users with administrative privileges. Darktrace is also the industry’s only solution that can correlate activity across SaaS environments with the rest of the organization. This enables the technology to coordinate weak indicators of a threat across areas that have traditionally represented security siloes, providing even greater context and shining a light on workforce behaviors that show up in every corner of the digital business.

Case Study: Disgruntled IT Administrator

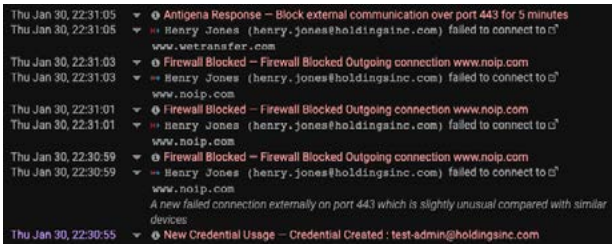
When an organization was forced to make a series of redundancies over the course of a single week, they neglected to take a fired IT administrator's laptop, or to delete their corporate account. The former IT admin logged into one of their SaaS accounts and quickly downloaded many sensitive files – including contact details and credit card numbers from the customer database. They then attempted to secretly transfer the stolen files to a home server via one of the company's regular data transfer services.

Because Darktrace dynamically analyzes logins and file access events across SaaS services, the system could immediately pick up on the unusually large file downloads and the exfiltration. Even though the disgruntled employee was still in the system as a legitimate administrator and used a familiar transfer service, Darktrace Cyber AI understood that the user's behavior within the SaaS platform was highly unusual and an indication of a significant threat.

The Threat Visualizer showing a large spike in data transfers

Subsequent investigation revealed that the malicious admin continually sought to exfiltrate the stolen SaaS files through several other methods, including with an internal server he had used regularly at the company. While the administrator's use of this server may have seemed normal in a different context, Cyber AI was able to connect the dots between the disgruntled employee's actions in the SaaS ecosystem and the corporate network, illuminating the full extent of this user's malicious behavior.

While this activity from a supposedly trusted administrator easily evaded both traditional solutions and native SaaS security controls, Darktrace Cyber AI detected the threatening behavior within seconds. The system instantly alerted the security team and provided detailed and precise information about the nature of the compromise, prompting them to revoke his credentials and quickly retrieve and secure the data. With Darktrace's complete, granular visibility and bespoke knowledge of normal behavior in SaaS platforms, the company was able to avoid any data loss, as well as serious compliance and digital trust consequences.



Darktrace Antigena actioning a targeted autonomous response

Antigena blocks the employee's attempt to transfer files via the cloud