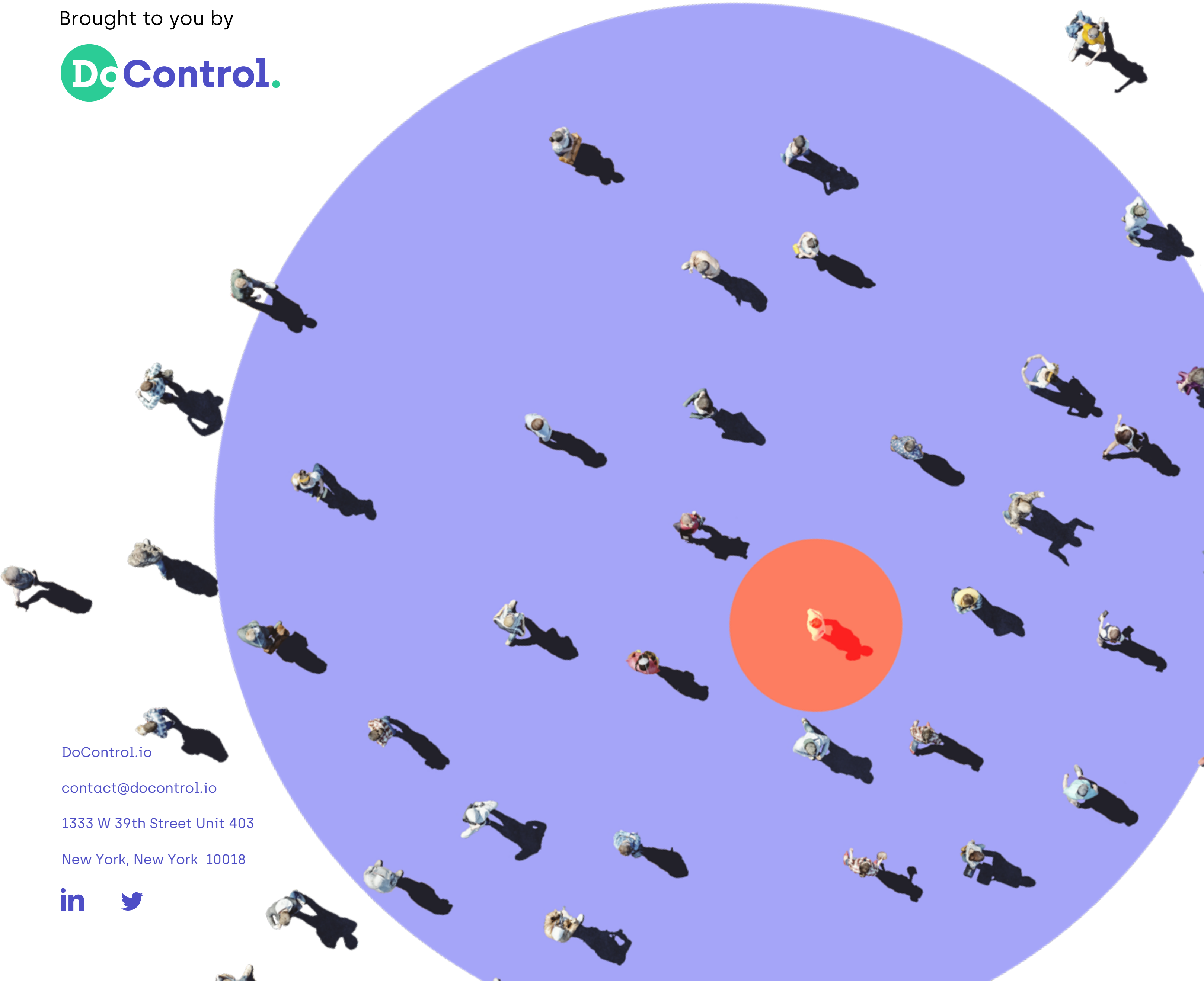
Automated, Intelligent SaaS Data Access Control

Mitigate the Insider Threat to Stop Employees from Exfiltrating Company Data

Brought to you by

DoControl.



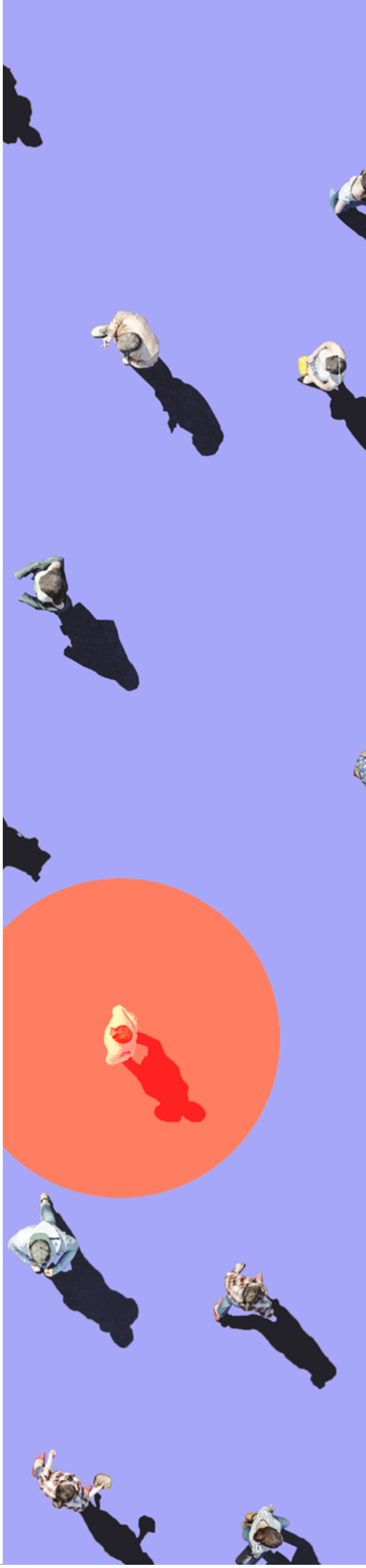
DoControl.io

contact@docontrol.io

1333 W 39th Street Unit 403

New York, New York 10018

Contents



Uncontrolled SaaS Data Access: The Exposure Hiding in Plain Sight

SaaS security is generally focused on keeping unwanted parties out of your applications and data. But the bigger security threat stems from uncontrolled and unmonitored SaaS data access propagated by the people who have legitimate business reasons to be working with your company's SaaS assets: your employees.

SaaS applications are all about easy and efficient collaboration, which is great for business development. Employees can create and share SaaS assets with colleagues, contractors, partners, customers and prospects quickly and easily, launching new ideas and moving intellectual property with a few clicks of a button.

But What Happens When An Employee Just Doesn't Work Out?

Cybersecurity gets put to the test when an employee decides the time is right to move on from your company. In the time leading up to separation and immediately following it, companies are at extreme risk for data exfiltration via an employee-separation insider threat.

There are many manifestations of the insider threat, but for the purpose of this paper we are focusing our examination on the critical time period that begins when an employee makes the decision to leave the company, carries through the day of separation, and includes an indeterminate duration after the employee and the company have parted ways.

For the employee privately planning to leave the company, widespread access to SaaS assets can be an enticing invitation to **download company data or share assets to a private email address** for future use, particularly if being hired by a competitor.

For the employee terminated from the company, the hours and days after layoff or dismissal can often present the now-former employee with an opportunity for **revenge or sabotage**. Either scenario – an employee taking data to a competitor or an employee intentionally inflicting harm on the company on their way out the door – happens far more than it should.

For IT and security teams working to keep company data protected, the employee-separation insider threat must be among their top concerns. The magnitude of the problem makes this an urgent security risk to address immediately and a complex problem that requires automated intelligence to both remediate existing vulnerabilities and to future-proof the security posture of the company.

> **Taking data to a competitor is but one form of insider threat that can inflict serious harm on a company.**

Employee-Separation Insider Threat Lifecycle

Medium-sized businesses and large enterprises alike have intricate organizational structures comprising numerous business units to support the specialized work of different teams carrying out the company's overall business objectives. In most cases, these teams are heavily reliant on SaaS applications to enable their daily work and foster collaboration within and across business units. Mid-sized companies in particular are challenged by their volume of SaaS applications and a lack of specialized IT and security staff to effectively manage threats and protect the business.

500K - 10M

ASSETS STORED IN SAAS APPLICATIONS

According to **our own research** stemming from work with numerous customers and prospects, a company of **1,000** employees can have anywhere between **500,000** and **10 million** assets stored in SaaS applications.

80,000

AVERAGE NUMBER OF DAILY SAAS ACTIVITIES

Across the companies we've analyzed, the average number of SaaS activities (creating files, downloading, duplicating, sharing internally and externally, etc.) undertaken each day exceeds **80,000**.

Amid all those transactions, it can be almost impossible for IT and security teams operating without purpose-built tools to identify activities that could indicate a current employee (or even a former employee) is exfiltrating data to serve personal interests rather than company objectives. Furthermore, even if IT is able to identify the activities and shared assets, cutting off that access could take days or weeks to accomplish when undertaken as a manual process.

Three Prominent Scenarios That Leave A Company Vulnerable To Employee-Separation Insider Threats

A review of three scenarios reveals the peak periods of vulnerability for the company — right before a resignation or termination notice is logged in HR systems and right after the separation has occurred. We refer to these times as the employee-separation insider threat lifecycle.

It is during these times that those who know most about the assets stored in SaaS applications and have access to them are more likely to exfiltrate data by saving assets to external or cloud drives, sharing them with external entities, or granting themselves access to files via their personal email addresses.

To understand the magnitude of the insider threat that companies face due to employee separation, it's important to examine the Insider Threat lifecycle. Let's take a closer look at each scenario and how certain actions at each phase, as well as some inaction, can change the level of risk companies face from insider threats.

1 **Resignation** (employee initiated)

2 **Dismissal** (employer initiated)

3 **Layoff** (employer initiated)

SaaS Insider Threat Lifecycle

Three Possible Paths to Separation from the Company

<table>
<tr><th></th><th>Resignation</th><th>Dismissal</th><th>Layoff</th></tr>
<tr><td>1 Triggering event</td><td>Lack of promotion, personal conflict among coworkers, changes in personal circumstances, etc.</td><td>Poor performance review, introduction of a performance improvement plan, verbal and/or written warnings, etc.</td><td></td></tr>
<tr><td>2 Suspicious activity</td><td colspan="2">Increases in sharing assets externally to personal email or external entities, downloads, files deleted, etc. A time of peak vulnerability for the company.</td><td></td></tr>
<tr><td>3 Verbal notice</td><td>Issued by employee: Possible lag between verbal notice and logging status change in HR systems.</td><td colspan="2">Issued by employer: Should result in immediate change of status in HR systems. Possible lag between verbal notice given to employee and status change logged in HR systems.</td></tr>
<tr><td>4 Notification logged in HR system</td><td colspan="3">Employee status changed from "Employed" to "Garden Leave" in systems like Workday, BambooHR, ADP, and others; employee reclassified as high risk to the organization; likely NOT automatically updated across systems that organizations use daily, such as file sharing, communication, CRM, and other platforms.</td></tr>
<tr><td>5 Last hours/days with the company</td><td colspan="2">Employee is more aware of security processes around offboarding; now employee is on everyone's "radar;" suspicious activity may wane.</td><td>Employee becomes aware of security processes around offboarding.</td></tr>
<tr><td>6 Offboarding</td><td colspan="3">Security/IT teams use identity provider solutions to delete the employee's SaaS user from all relevant SaaS apps.</td></tr>
<tr><td>7 Unmanageable SaaS data access</td><td colspan="3">While the employee no longer has access through their former corporate account, all assets they have ever shared internally, externally, and publicly remain as is and available to customers, vendors, personal accounts, anonymous users, etc.</td></tr>
</table>

Why Do We Have Periods of Peak Vulnerability?

The employee-separation insider threat lifecycle can look different depending on whether the employee's separation from the company is employee-initiated (resignation) or employer-initiated (layoff or dismissal). However, some of the phases can be similar regardless of whether the employee or the company starts the separation process.

Take, for example, the Suspicious Activity phase which covers the days, weeks, or sometimes even months between the employee deciding to leave and the day the separation is announced. When an employee has decided that their tenure with the company is going to end, they may use that time to take company data in the form of SaaS assets. This can be true in the event of an employee-initiated resignation or an employer-initiated dismissal, because each scenario can start with some kind of triggering event. (This is less often relevant for a layoff scenario, however, because employees are usually caught unaware that the layoff is coming, meaning that the triggering event and the day of notification coincide.)

In all cases, however, there are vital steps HR, security and IT teams must take in a timely fashion to minimize the insider threat. And when these things don't happen automatically or quickly, company assets remain at risk.

Resigning Employees

Workplace conflicts or perceived sleights can act as triggering events for employees. Or sometimes external factors having nothing to do with the company or the employee's job may prompt an employee to make a plan to leave, setting the stage for one of the peak times of suspicious activity.

An employee giving notice of intent to leave the company should set several important processes into motion right away. The foremost is a change of employee status in the company's HR systems from "Employed" to "Garden Leave." But there is often a delay between the employee offering verbal notice to their direct manager and that employee officially tendering documentation of their intent to resign. The direct manager may choose to wait for documentation before taking any official action. Then, depending on where this issue falls on the list of priorities the direct manager is juggling, the manager may or may not immediately notify their HR partner. Likewise, the HR partner may not immediately log the employee's change in status.

As with the period prior to the employee giving notice, this time of inefficient operations when the employee has declared their intention but no status change has been formally recorded anywhere within the company, the employee's diminished loyalty to the company may embolden them to steal company data. If security and IT aren't aware of the imminent departure, they won't be in a position of strength when it comes to making sure the involved employee hasn't started acting out of personal interest rather than company interest.

> **Any delay in receiving notification of an employee's intent to leave the company and logging this notification in HR systems unnecessarily extends the company's period of peak vulnerability to data exfiltration.**

Dismissed Employees

The dismissal process is usually swift once the decision has been made by the company to terminate. Most often, once the employee is notified, their access to internal systems is severed immediately. However, we still see companies suffering through the peak periods of vulnerability more often than should be the case.

On the front end of termination, if a company handles the dismissal process correctly, the affected employee is made aware of the possibility of termination several months ahead of the actual decision to terminate. Companies often institute performance management measures, like a performance improvement plan (PIP), to both help the employee focus on the key performance indicators that they need to reach in order to keep their job and to help the company document insufficient performance by the employee in the event the employee continues to fall short of expectations.

An employee working through a 90-day PIP may, at some point, decide their position with the company isn't salvageable and choose to let the dismissal process run its course or proactively resign. In either case, the PIP or the warning issued by the company can serve as a triggering event for the employee, leading the employee to engage in data scraping and exfiltration activities before any final decision has been made or announced.

On the back end of a dismissal, even though the employee may be immediately ushered out of the workplace, sometimes that employee's access to company assets remains intact for hours or even days after the firing. This was the case with a **New York-based accounting firm** that fired an HR executive yet did not immediately revoke her access to all IT systems. Over the course of several days after her termination, the former employee logged in to an external HR platform and deleted thousands of files. As inexplicable as this scenario seems, it's not uncommon, and it can point to a deficiency in the company's technological capabilities as much as a lack of organization.

Laid Off Employees

Not all layoffs are executed with immediate effect. Some employees are granted time to find another position within the company or elsewhere, or they are asked to remain on staff for a period of time to complete certain initiatives or to facilitate a transition of work and/or personnel to others in the company.

As with resigning employees, employees working with a known expiration date on their term of employment may represent a greater risk. If security and IT are unaware of the situation, they don't know that they should be more vigilant regarding the employee's actions on IT systems. But even if notice of the employee's upcoming separation from the company has reached security and IT, they may not have the tools they need to provide the required vigilance.

> **Timing is critical: On an employee's last day with the company, the employee should be offboarded from all IT systems. This does not always happen, though.**

The Uncomfortable Reality of Technological Shortcomings

Once an employee's status in HR systems has been changed from "Employed" to "Garden Leave," the company should consider the employee a high security risk. This status change should be an opportunity for security and IT teams to raise their awareness of the employee's behavior around the company's digital assets and keep a close watch on the employee's actions through separation from the company and offboarding from IT systems.

That said, such observation is often easier said than done. Even a modest-sized business can have subscriptions to myriad SaaS solutions, and these applications can hold hundreds of thousands or millions of assets, any of which may be shared widely among the internal team and also extensively with external entities. Without the technological capabilities to continuously monitor the employee's activities across the full stack of SaaS applications and recognize when data scraping or exfiltration is occurring, the company may be powerless to intervene before significant damage is done.

Again, though, the problem often starts when the employee decides that the time is right to leave the company but that it's not yet time to announce the decision. In this situation, the employee may be engaging in suspicious activity by operating in stealth mode, a period in which the employee's personal interests have begun to diverge from the company's interests. If there's a triggering event that helps the employee to decide to steal company secrets, it's often far easier to steal or scrape data before announcing intent to separate from the company than after notice is given.

Regardless of whether notice has or has not been given, companies need to understand where their SaaS assets are, who owns them and with whom they've been shared. And they need to have a baseline of SaaS activity and automated monitoring capabilities in place to be able to understand normal activity and recognize when anomalous activities begin. In that way, even though companies can't know when an employee is going to resign, they still can, with the right toolset, identify problematic activity and intercede to prevent damage to the company.

Further, while it may seem unfathomable that a company could go through any kind of separation with an employee – friendly or unfriendly – and still allow the now-former employee to continue to access SaaS data and applications, it happens much **more frequently** than many people realize. Former employees whose loyalties now lie with a competitor or who bear a grudge against their former employer can do damage or wreak havoc when they still have access to SaaS applications and other IT systems.

Offboarding and the Uncontrolled SaaS Data Access Severed Employees Leave Behind

On the leaving employee's last day, security and IT teams should use identity provider solutions to delete the employee's SaaS user instance from all relevant SaaS applications. This is a fundamental step in the offboarding process. The real problem, though, is that even when the user is deleted, the SaaS assets the user created necessarily remain, and all of the data access granted through the SaaS applications in which these assets reside persists.

While the employee no longer has access through their former corporate account, everything they have ever shared internally, externally, and publicly remains as is and continues to be available to personal accounts, customers, vendors, anonymous users, etc. Ownership of assets created by the former employee will be transferred to another internal user (further entangling data access control), but the access previously granted remains. This can leave many a back door open to the former employee interested in retaining access to SaaS assets and the data they contain.

> **While the former employee no longer has access through their former corporate account, the SaaS data access they have granted to internal colleagues, private email addresses, external entities and the public remains as is.**

Shifting Security Left with a Data Access Platform for Early Intervention

Even with keen awareness of the risk and timely execution of offboarding activities, you're not in a position to reign in control of SaaS data access if you are relying on native SaaS security features and trying to manage SaaS data access manually. Companies today need a SaaS data access platform that operates across all SaaS applications, providing companies with the automated intelligence they need to maintain a complete inventory of SaaS assets, monitor daily SaaS activity to recognize security-compromising actions, and institute and execute centralized, granular security policies and remediation to stop data exfiltration.

The Right SaaS Security Platform Features Three Key Capabilities:

SaaS Asset Management

Gain full awareness of every entity – individual or organization, internal or external – that has access to your corporate data so you know what needs to be protected. SaaS Asset Management captures a moment in time so that you have a complete inventory of SaaS assets and the internal users, external collaborators and domains that have access to those assets.

Continuous Monitoring

Bolster your SaaS Asset Management with intelligent monitoring that establishes a baseline of SaaS data access across the entire stack of SaaS applications to understand typical SaaS activity and identify anomalous data access. Continuous monitoring provides a centralized view across the array of SaaS applications and flags suspicious activity before it becomes a problem.

Automated Security Workflows and Remediation

Establish and institute dynamic policies that allow for consistent security policy enforcement across all SaaS applications to balance corporate security with business enablement. Look backward to automatically remediate any data access that no longer has a legitimate business purpose. Look ahead by creating security policies that allow or deny SaaS data access by specific users, applications, business units, or domains to keep data protected while allowing the collaboration that SaaS applications were designed for.

DoControl: A New Approach to SaaS Security to Guard Against the Insider Threat

The DoControl SaaS Security Platform allows companies to shift their SaaS security left, allowing for earlier detection of attempted data exfiltration through malevolent SaaS data activity and timely intervention to shut down exfiltration efforts before they become a problem. With DoControl on patrol, security and IT teams do not have to be consumed with looking for nefarious activity and manually managing SaaS data access.

The DoControl Platform helps enterprises mitigate the Insider Threat. By starting with robust SaaS asset management, DoControl provides companies with a complete inventory of SaaS assets and a full mapping of asset ownership and the associated data access enabled for each. This provides security and IT teams with a complete picture of the company's SaaS landscape and allows them to establish a baseline for "typical" SaaS activity.

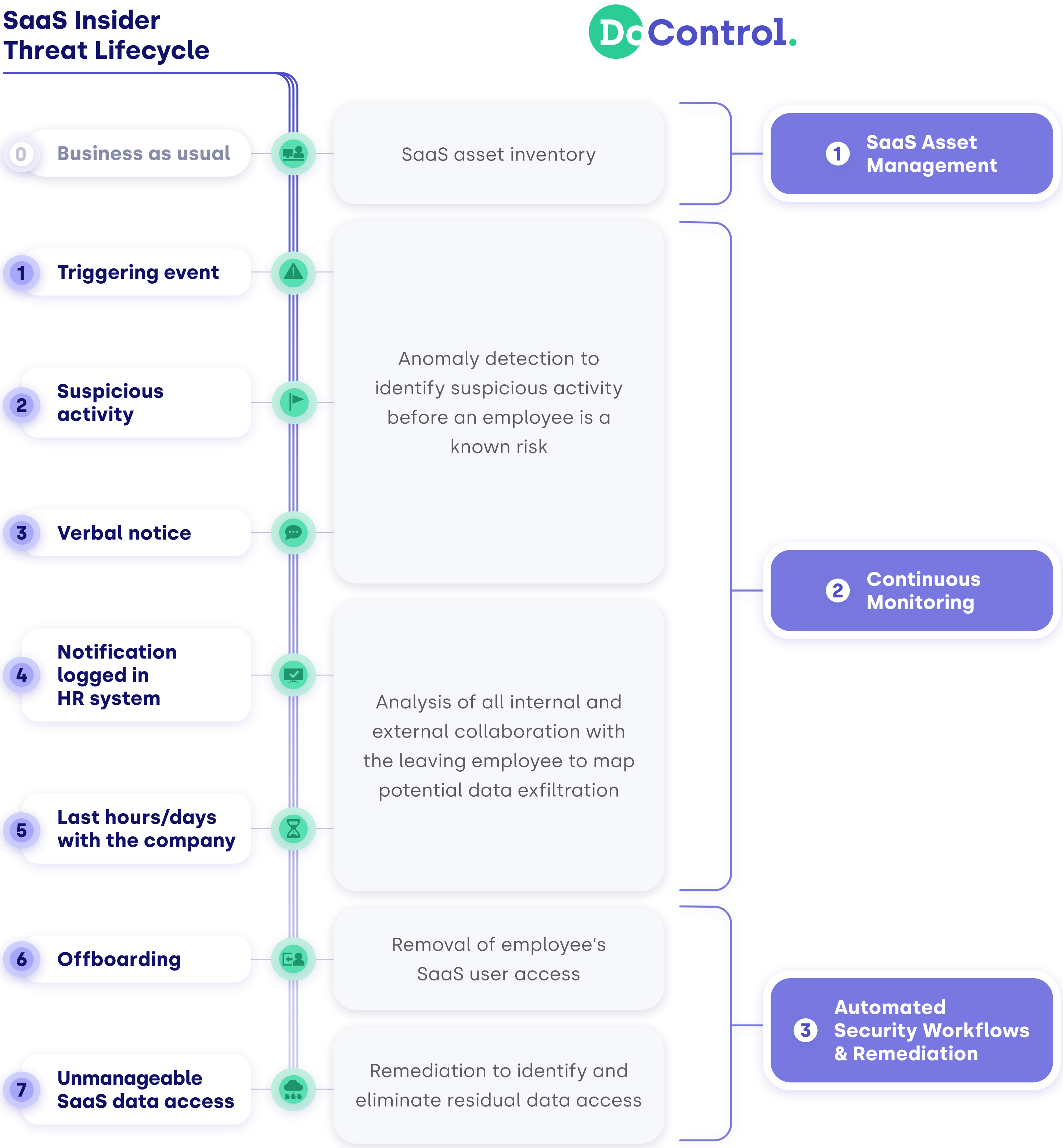
With that baseline in place, DoControl's continuous monitoring capabilities utilize intelligent automation to gauge new activity against the baseline, flag any atypical activity and shut it down until anomalies can be investigated. This protects the company against any suspicious activity that an employee might engage in prior to parting with the company.

DoControl's automated security workflows and remediation then provide protection during the offboarding process by automating the shut-off of data access across all SaaS applications at the moment of the leaving employee's separation from the company. Further, DoControl allows security and IT teams to identify and remediate any lingering access the former-employee may otherwise retain and eliminate access points, protecting the company from data exfiltration.

> **Companies today need a SaaS security platform that operates across all SaaS applications, providing them with automated intelligence to maintain a complete inventory of SaaS assets, monitor daily SaaS activity to recognize security-compromising actions, and institute and execute centralized, granular security policies and remediation to stop data exfiltration.**

DoControl SaaS Security Platform

How DoControl Mitigates the Insider Threat



SaaS Insider Threat Lifecycle

0 Business as usual

1 Triggering event

2 Suspicious activity

3 Verbal notice

4 Notification logged in HR system

5 Last hours/days with the company

6 Offboarding

7 Unmanageable SaaS data access

DoControl.

SaaS asset inventory

Anomaly detection to identify suspicious activity before an employee is a known risk

Analysis of all internal and external collaboration with the leaving employee to map potential data exfiltration

Removal of employee's SaaS user access

Remediation to identify and eliminate residual data access

1 SaaS Asset Management

2 Continuous Monitoring

3 Automated Security Workflows & Remediation

Put DoControl's SaaS Security Platform to Work for Your Company

DoControl's Saas asset management, continuous monitoring and automated security workflows and remediation capabilities provide numerous benefits to companies:

- ✓ Improve business productivity by enabling collaboration through SaaS applications while lowering the risk of data exfiltration or leakage.
- ✓ Implement granular data access controls – by individual, role, application, or domain – to minimize the risk of data breaches.
- ✓ Automate application of dynamic security policies through workflows designed to improve operational efficiencies of security and IT teams.
- ✓ Demonstrate and report on compliance requirements of relevant regulations while lowering corporate liability risk.

To learn more about the DoControl SaaS Security Platform please visit the DoControl website at **https://www.docontrol.io/** ►

To schedule a DoControl SaaS Security Audit and Proof of Vision, **request a demo** ►

To schedule a free SaaS Security consultation, **contact us** ►

About DoControl

DoControl helps organizations prevent data breaches in the most popular SaaS applications, and balance between security and business enablement. Founded by former Google Cloud Cybersecurity members, DoControl provides security teams the automated, self-service tools they need for data access monitoring, orchestration, and remediation within SaaS applications.

DoControl is backed by investors RTP Global, StageOne Ventures, Cardumen Capital and global cybersecurity leader CrowdStrike's early-stage investment fund, the CrowdStrike Falcon Fund. The company's leadership team combines product, engineering and sales experience across cybersecurity, enterprise and SaaS innovators.
For more information, please visit us **here**.

DoControl.

DoControl.io contact@docontrol.io 333 W 39th Street Unit 403, New York, NY 10018