Control.

Defending Against SaaS Supply Chain Attacks

An overview of SaaS supply chain risks with pragmatic recommendations and guidance to mitigate attacks

Table of Contents

Introduction

A software supply chain attack targets the software development process, with the intent of introducing malicious code into "trusted" software packages. This attack typically involves compromising one or more of the components that make up the software supply chain. Upon successfully infiltrating the supply chain, attackers can then insert malicious code or backdoors into the software package. This allows for the ability to steal sensitive data, launch further attacks on the target organization or its customers, or take control of the affected systems and/or applications.

This document provides an overview of software supply chain risks, and offers pragmatic recommendations and guidance to mitigate this type of increasingly common attack that targets Software as a Service (SaaS) applications.

The Lifecycle of a Supply Chain Attack

Supply chain-based attacks have long been a security challenge, however in more recent years cyber security practitioners are encountering a greater number of more targeted and sophisticated attacks. These attacks are a type of cardinality of one-to-many; when the compromising of one victim organization (the supplier) gains entry point into some or all of its customers (the consumers of the service provider). The cascading effects from a single attack may have a widely propagated impact. For this reason, attackers have shifted their focus towards targeting suppliers. Supply chain attacks have significant negative impacts in terms of the downtime of systems, financial implications, reputational damages, and many other negative outcomes. [1]

A software supply chain attack typically follows a series of stages, which can be broadly categorized into the following five phases:

1. **Infiltration**: In this phase, the attacker gains access to the software supply chain by exploiting vulnerabilities in the target system or application. This can be achieved through a variety of means, such as phishing attacks, spear-phishing, social engineering, credential compromise, or exploiting software vulnerabilities.

2. **Implantation**: Once the attacker has infiltrated the software supply chain, the next step typically involves implanting malicious code into the software or system. This can be achieved by modifying the source code, injecting malicious code into libraries or dependencies, or leveraging a backdoor to gain unauthorized access to the system or application.

3. **Propagation**: In this phase, the attacker spreads the malicious code to other systems or applications through the use of various propagation techniques. The goal is to maximize the impact of the attack and infect as many systems or applications as possible.

4. **Activation**: Once the malicious code has been successfully deployed and propagated, the attacker can trigger the attack by activating the code or payload. This can be achieved through a variety of means, such as a timer, an external trigger, or a specific event.

5. **Exploitation**: In the final phase, the attacker takes advantage of the vulnerabilities in the system or application to achieve their objectives, which can range from exfiltrating sensitive data to causing a disruption in service or system functionality.

The lifecycle of a software supply chain attack can vary depending on the specific attack vector and the target system. Understanding the general phases of a supply chain attack is a criticality that cannot be overlooked in order to take the appropriate measures to identify, protect, detect, respond, and recover from supply chain-based attacks. [2] This includes implementing strong security measures, conducting regular security assessments, and monitoring the supply chain for indicators of compromise.

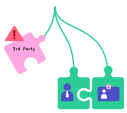
--

[1] The European Union Agency for Cybersecurity (ENISA): Threat Landscape for Supply Chain Attacks (July 2021), https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[2] NIST: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Supply Chain Attack Techniques

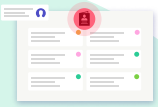
Software supply chain attacks can be difficult to detect and mitigate, which is partly due to the techniques that are often leveraged in a standard attack. There are several techniques, both basic and sophisticated, that provide the desired outcomes of business disruption or data exfiltration; and in many cases more than one technique is used in any given attack. The categories of attack techniques highlighted below are commonly used in supply chain-based attacks.



3rd Party Software Attacks: These attacks are executed by exploiting vulnerabilities present in the software that is part of the supply chain. Attackers often gain access to the 3rd party software and implant malicious code that can be triggered when the software is used by the intended target.

Credential Theft: Both human user and machine identity credentials (i.e. passwords, tokens, or secrets) for a supplier or vendor become compromised, providing unauthorized access to an organization's systems, networks, applications, and data.

Malware Injection: Malware injection attacks involve the insertion of malicious code or malware into software packages or updates distributed through the software supply chain. The malware may be designed to steal data, launch distributed denial of service (DDoS) attacks, or provide remote access to the attacker.



Fraudulent Certificates: Attackers can use fraudulent digital certificates to sign and distribute malicious software that appears to be legitimate. Fake digital certificates such as SSL/TLS or Code Signing certificates can be found and purchased on the Dark Web.

Social Engineering: Social engineering attacks involve manipulating users into divulging sensitive information or installing malware. Attackers can use phishing emails, impersonation attacks, or other social engineering techniques to target employees and compromise their access to the software supply chain.

Tampering and Alteration: In these attacks, attackers modify the software or firmware to insert malicious code that allows them to gain control over the system. The modified software may be distributed to end-users via the supply chain, compromising the integrity and security of the entire system.

Insider Threats: Insider threats involve individuals with legitimate access to the software supply chain who abuse their privileges to carry out attacks. Malicious insiders include employees of software vendors, system integrators, or other third-party vendors involved in the supply chain.

SaaS Application Supply Chain Risk

A main threat vector within SaaS involves machine identity access and the associated credentials with "Shadow Applications." These applications are a form of Shadow IT that are not authorized (i.e. unsanctioned) by an organization's IT department. Shadow Applications have the potential to contain vulnerabilities or backdoors that can be exploited, providing unauthorized access to sensitive information and data. One proven technique is to compromise the credentials and privileges involved in application-to-application interconnectivity.

Many common, 3rd party applications require elevated system privileges to operate effectively. Even when the application can effectively operate with reduced privileges, they will oftentimes default to asking for greater privileges during installation to ensure the application's maximum effectiveness within the organization's IT estate. Unfortunately, organizations will woefully accept 3rd party software defaults without investigating further, allowing for additional accessibility vectors to be introduced into the environment. [3]

Open Authorization (OAuth) is an open standard that issues tokens to users for access to systems. An OAuth access token enables a 3rd party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials. Attackers who steal OAuth tokens can gain access to sensitive data and perform actions with the permissions of these compromised targets, which can lead to privilege escalation and further compromise the environment. [4]

SaaS Application Supply Chain Risk

Shadow Applications have a high propensity to create data silos. The use of unsanctioned applications may result in the inability to integrate with other applications used by the organization, which leads to data silos as well as inefficient workflows. In addition, the risk of data loss will also increase due to the fact that Shadow Applications may not have proper backup or recovery mechanisms in place.

Beyond the risks imposed from a cybersecurity perspective, there are also regulatory compliance considerations (i.e. Payment Card Industry Data Security Standard (PCI DSS, General Data Protection Regulation (GDPR). Many industries have regulatory frameworks and compliance requirements that organizations must adhere to. The use of Shadow Applications will land organizations in non-compliance, resulting in potential fines or legal action from the governing body.

IT departments are responsible for supporting and maintaining authorized applications. If unsanctioned applications are not supported by IT, they will likely lead to issues with compatibility, updates, and security patches. To mitigate the risks associated with unsanctioned applications, organizations should establish clear policies for the use of technology and enforce those policies consistently. Engaging with business users and performing application reviews whereby users provide a business justification for the application is one way to achieve this. It is also important to educate employees on the risks associated with unsanctioned applications and provide them with approved alternatives.

Organizations should regularly monitor their IT estate for unauthorized applications and take prompt action to remove them. Business-critical SaaS applications should undergo rigorous assessments as they should be considered a Tier0 asset; given the sensitive data that is accessed, shared and manipulated within this environment. Both human and machine identities require strong security controls and policies to effectively protect sensitive data, and prevent lateral movement from one business-critical application to another. [6]

OAuth applications are often overprivileged with risky permission scopes, they may not be verified via a Marketplace, as well as may not be approved internally through IT/Security teams. The major collaboration applications companies rely on often support numerous 3rd party application integrations. Unfortunately, it's not uncommon for some of these third-party apps to be overprivileged: [5]

Medium Companies

- Microsoft has an average of **224 third-party application integrations**
  - **11 applications** on average are overprivileged
- Google has an average of **50 third-party application integrations**
  - **17 applications** on average have data access permissions
  - **9 applications** on average are overprivileged

Large Companies

- Microsoft has an average of **743 third-party application integrations**
  - **11 applications** on average are overprivileged
- Google has an average of **81 third-party application integrations**
  - **27 applications** on average have data access permissions
  - **9 applications** on average are overprivileged

Download the full 2023 SaaS Security Threat Landscape Report

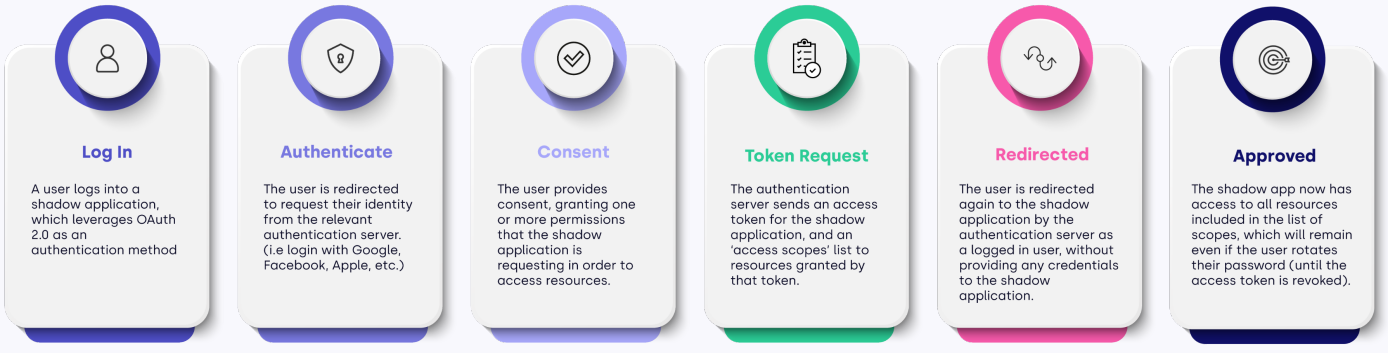


Figure 1. The standard OAuth authentication flow for a shadow application gaining unauthorized access to scopes and corresponding resources from the target application.

[3] CISA: Defending Against Software Supply Chain Attacks, Cybersecurity and Infrastructure Security Agency (April 2021), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

[4] MITRE ATT&CK Framework, T1528, Steal Application Access Token (April 2022), https://attack.mitre.org/techniques/T1528/

[5] DoControl 2023 SaaS Security Threat Landscape Report (March 2023), http://www.docontrol.io/2023-data-report

[6] NIST Special Publication 800-218: Secure Software Development Framework (SSDF) Version 1.1, (February 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

Notable Credential-based Supply Chain Attacks

SAMSUNG, MARCH 2022

The Lapsus$ hacking group obtained and leaked 190GB of Samsung's confidential source. After scanning it, GitGuardian uncovered 6,695 secrets in the leaked source code. GitGuardian's results also indicated that approximately 600 authentication tokens had also been exposed in the source code.

GITHUB, APRIL 2022

An attacker had abused stolen OAuth user tokens to download data from dozens of GitHub's customers. The applications maintained by the compromised platform service providers, Heroku and Travis-CI, were used by GitHub users. GitHub's analysis of the threat actor's behaviors suggested that they mined the downloaded private repository (GitHub's own npm) contents. The attacker scanned the code within these private repos to which the stolen OAuth token had access, seeking out secrets that could be used to pivot into other infrastructure.

TOYOTA, OCTOBER 2022

Toyota publicly disclosed a data leak after access keys were exposed, warning their customers of potential personal information exposure. Some of Toyota's source code was inadvertently published on GitHub and contained an access key to the data server that stored customer email addresses and management numbers. A 3rd party development subcontractor made a significant mistake in allowing that public key to be accessible for almost 5 years.

Mitigation Strategies for Supply Chain-based Attacks

Some of these recent supply chain attacks revealed alarming weaknesses in traditional defense strategies, as well as showing the potential of its cascading negative implications. Despite some of the highly sophisticated tactics, techniques and procedures (TTPs) involved in these attacks, organizations can still adopt security strategies to mitigate the risk of supply chain-based attacks.

Organizations should place their focus around building preventative measures due to the difficulty of mitigating consequences after a software supply chain attack occurs. Security practitioners should observe industry best practices before an attack has occurred. [7] Implementing best practices will bolster an organization's ability to prevent, mitigate, and respond to attacks. Here are a few considerations to combat growing software supply chain risks:

1. **Security Assessment:** Conducting a comprehensive security assessment can help organizations identify vulnerabilities and risks in their supply chain, such as weak points, 3rd-party software providers, and data and communication channels.

2. **Strict Vendor Assessment:** Perform a detailed vendor assessment to identify their supply chain processes and policies, evaluate their security practices and processes, and identify potential vulnerabilities in their systems.

3. **Code Review and Auditing:** Conduct a thorough code review and audit process to ensure that all code is secure and up-to-date. This can include performing static and dynamic analysis, and identifying potential security flaws and vulnerabilities.

4. **Verification and Authentication:** Verify and authenticate all software and hardware components of the supply chain, including the identity of the supplier and any 3rd-party providers.

5. **Continuous Monitoring:** Employ a continuous monitoring system that tracks and monitors all critical activities, including real-time threat detection and response capabilities.

6. **Security Automation:** Implement preventative security controls that automatically revoke access, suspend or remove sanctioned applications that violate organizational policy.

7. **Secure Communication Channels:** Ensure that all communication channels are secure and encrypted to prevent unauthorized access or tampering of sensitive data.

8. **Regular Software Updates:** Keep all software and systems up-to-date with the latest security patches, fixes, and updates, to prevent any vulnerabilities from being exploited by attackers.

9. **Cybersecurity Training and Awareness:** Educate employees and vendors on the importance of supply chain security and their role in maintaining a secure supply chain. Engage with end users on an ongoing basis to reaffirm security best practices, and notify on policy violations or high risk activities.

As the threat landscape evolves, organizations will need to prioritize security and be more aggressive about reducing their risks. Regulatory compliance frameworks, as well as most organizational policy require that business-critical data, both supplier and customer data, be protected. Incorporating some of these techniques, as well as establishing an evidence-based cyber risk management program will help navigate through the evolving threat landscape.

DoControl's Approach to Protecting the SaaS Supply Chain

DoControl provides many foundational controls outlined in the aforementioned mitigation strategies section, that aid in the prevention of a supply chain-based attack at the earliest stages of the attack chain. The DoControl SaaS Security Platform will first discover all interconnected SaaS applications within the estate, and expose a full mapping and inventory of 1st, 2nd and 3rd party applications. The solution helps prevent OAuth token compromise by revoking tokens and removing users, both through self-service tooling as well as via automated security workflows.

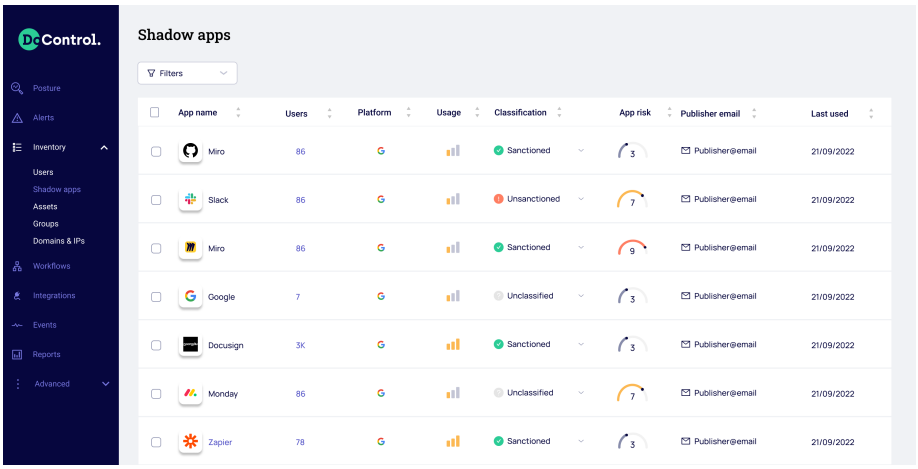
The full context of which platform the application is connected to, how many users have it installed, the risk score (calculated by permissions, scopes, IP addresses, etc.), compliance standards, and more. Security teams can monitor and control application usage and take immediate action on potential policy violations, as well as enforce automated security policies to automatically remediate the potential risk exposed by the application. In order to support the business in a secure way, application reviews with business users can be performed through ongoing interaction and engagement (i.e. via Slack). Automated notifications can be generated when an unsanctioned application becomes introduced to the SaaS estate, and end users can then have them approved through a business justification.

The DoControl solution provides comprehensive Shadow Application governance through discovery, control, and automated remediation. How it works:

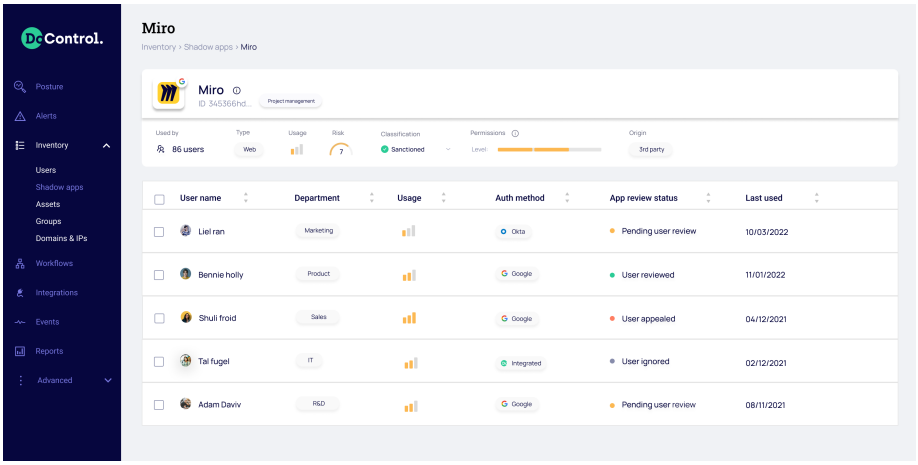
--

[7] CISA: Defending Against Software Supply Chain Attacks, Cybersecurity and Infrastructure Security Agency (April 2021), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdfNIST.SP.800-218.pdf

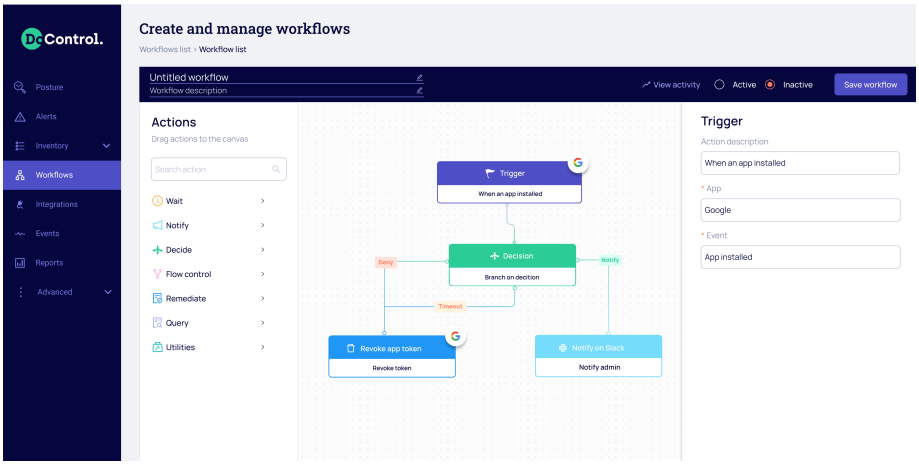
Discovery and Visibility: Discover all connected SaaS applications to the core SaaS stack. Identify issues of noncompliance for the entire SaaS application estate to ensure security policies are effectively enforced. Expose a full SaaS-to-SaaS application mapping and comprehensive inventory of 1st, 2nd and 3rd party applications (i.e. installed users, drive access, drive-wide permissions, and more). IT and Security teams can gain a strong understanding of the riskiest SaaS platforms, applications, and users exposed within the SaaS estate.



Monitor and Control: Perform application reviews with business users through ongoing interaction and engagement (i.e. via Slack). Assign a risk-index to each application to enable the assessment and evaluation of the SaaS estate. Create pre-approval policies and workflows that require end users to provide a business justification to onboard new applications. IT and Security teams can quarantine suspicious applications, reduce overly excessive permissions, and revoke or remove applications or access.



Automated Remediation: Automate security policy enforcement across the SaaS application stack that prevents unsanctioned or high risk application usage, and remediates the potential risk those apps might expose (i.e. invalid tokens, extensive or unused permissions, listed vs. not listed apps, etc.). IT and Security teams can automatically reduce risk exposure related to application-to-application interconnectivity (i.e. automatically suspend or remove potential malicious applications) by implementing Security Workflows.

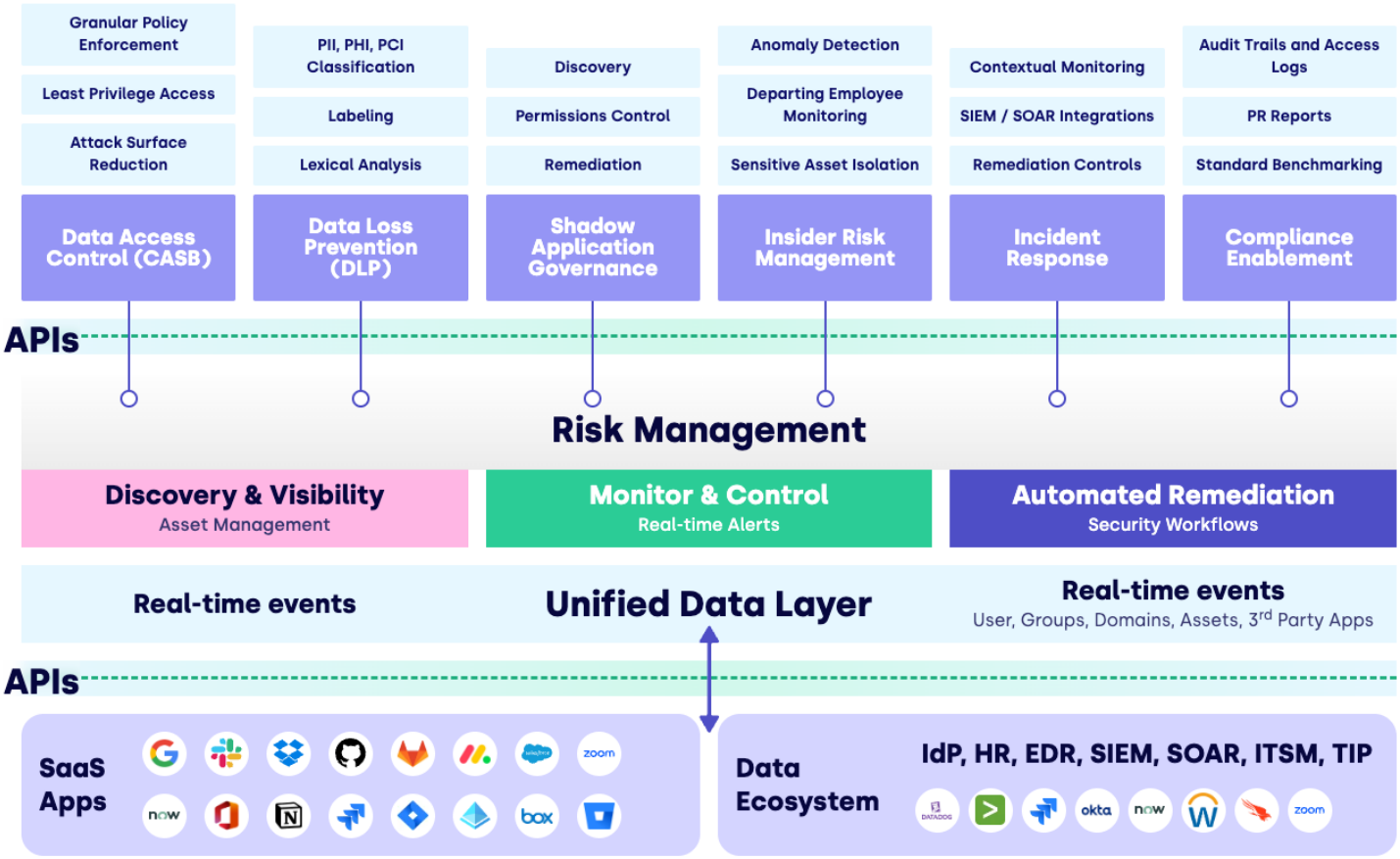


DoControl additionally provides enrichment and contextual data within the SaaS estate. The solution provides application classification through standard identity providers (IdP) Single Sign-on (SSO) prism, as well as human resource information systems (HRIS) for departmental breakdowns. Data enrichment and exposing the full business-context of the SaaS estate will assist Security teams in triaging security events and help streamline incident response efforts. For data access exposure, DoControl connects shadow applications with data access findings and incorporates the risk and overall magnitude to better understand the organization's risk profile. For example, if an application has specific scopes and certain levels of access, it will combine the exposure of files, assets and drives that it's connected to.

The DoControl SaaS Security Platform

DoControl provides a unified, automated and risk-aware SaaS Security Platform that secures business critical data, drives operational efficiencies, and enables business productivity. DoControl's core competency is focused on protecting business-critical SaaS data through automated remediation. This is achieved through preventive data access controls, SaaS service misconfiguration detection, service mesh discovery, and shadow application governance. The DoControl Platform is built upon three foundational tenets which include Discovery and Visibility, Monitor and Control, and Automated Remediation. DoControl provides SaaS data protection that works for the modern business, so they can drive their business forward in a secure way.

Strengthen your SaaS supply chain security posture. Request a demo to get started.



About DoControl

DoControl is an agentless, event-driven SaaS Security Platform that secures business-critical SaaS applications and data. DoControl helps organizations expose their SaaS risk, remediate it quickly, and automatically remediate over time through granular, no-code workflows. DoControl uncovers all SaaS users, third-party collaborators, assets and metadata, OAuth applications, groups, and activity events. DoControl helps reduce risk, prevent data breaches, and mitigate insider risk without slowing down business enablement. To learn more about DoControl, visit www.docontrol.io, read the DoControl blogs, or follow us on Twitter and LinkedIn.