

# Proofpoint CASB Adaptive Access Controls

## Manage Access and Data to Secure Your Cloud Apps

### CHALLENGES

- Cloud account takeover
- Risky access to cloud apps
- Data loss and compliance

### KEY CAPABILITIES

- Prevent unauthorized access with identity and role-based controls
- Reduce compliance risks with device-based access and data controls
- Protect sensitive files with real-time data loss prevention
- Deploy quickly in the cloud

### PRODUCTS

- Proofpoint CASB
- Proofpoint SaaS Isolation

### WHY PROOFPOINT?

- People-centric security controls (Very Attacked People™, privileged users, and users more vulnerable to cyber attacks)
- Granular policy controls based on risk, context and user role
- Actionable threat intelligence (IP reputation, high-risk suspicious logins)
- Agentless and robust solution deployed in a matter of hours

The modern workforce is cloud-based, remotely distributed and, more than ever, a prime target for today’s cyber attacks. Just as the traditional office and 9-to-5 workdays have morphed into more flexible and responsive routines, threats have shifted from the old network perimeter to people and the data, systems and resources they access.

In this evolving environment, securing access to cloud apps, preventing data loss and staying compliant is critical.

When working from home or another remote location, users lack the protection of the corporate network. They often work on unmanaged devices. They may download files with sensitive data to their personal devices. This combination leaves organizations vulnerable to cyber threats such as credential compromise—which in turn leads to account takeover, data loss and all kinds of phishing-based attacks such as business email compromise (BEC).

These risks are real, and they’re significant. Fortunately, Proofpoint CASB can help you mitigate them. Our easy-to-deploy solution quickly secures Microsoft 365 (Office 365), G Suite, Zoom, Box, Salesforce, Workday and more.

CASB’s adaptive access controls enable real-time security measures based on risk, context and role. It automatically blocks access from risky locations and networks and by known threat actors. And it applies risk-based controls to high-risk and high-privilege users, including step-up authentication, managed-device policy rules and VPN enforcement.

Unlike static security and compliance controls that apply to every user in the same way, CASB-enabled access controls are adaptive. They enable you to apply just the right amount of security and compliance controls without unduly burdening lower-risk users.

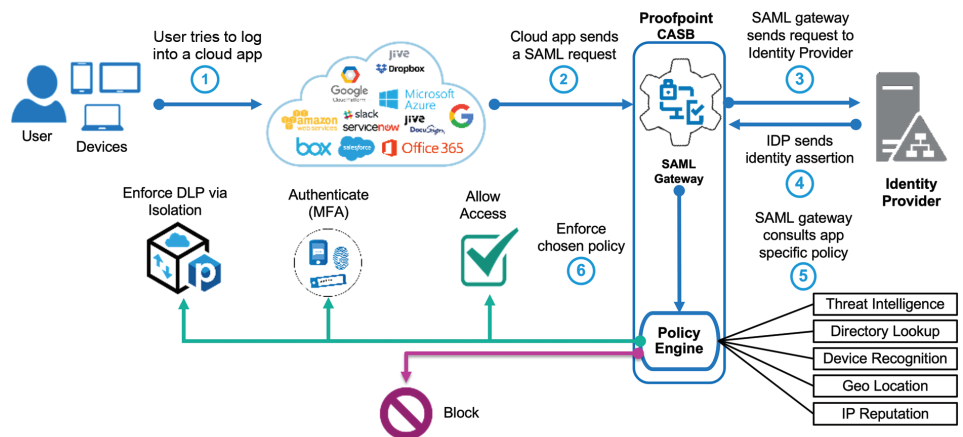


Figure 1: Adaptive access controls architecture.

## CLOUD THREAT PREVENTION

Users' account credentials are the keys to your kingdom. When cyber criminals compromise these credentials from cloud accounts, they can launch attacks inside and outside of your organization.

Adaptive access controls use threat intelligence about known threat actors to block suspicious logins and prevent account takeover. CASB also uses contextual data to further confirm a user's identity and prevent risky access. Contextual data includes:

- User location
- Device
- Network
- Login time

You can use these risk indicators to define access control policies to prevent attackers from gaining access to your corporate applications.

### Common Policies

Here are common CASB policies used to stop cloud-based threats.

#### Block high-risk suspicious logins

When an attacker's signature is already known to Proofpoint, you can prevent such high-risk suspicious logins by using CASB's adaptive access controls. Proofpoint tracks suspicious logins across tens of millions of accounts and has the best understanding of cloud threats. For example, you can block access to your highly attacked user accounts when CASB detects a suspicious login.

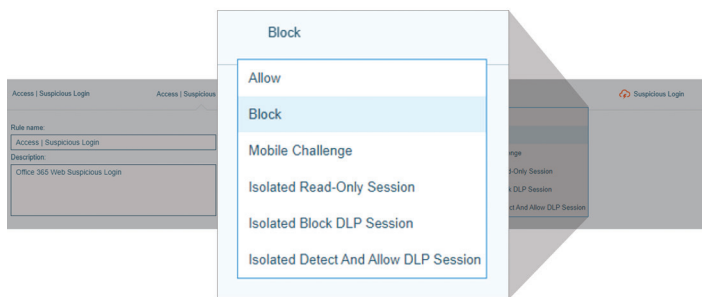


Figure 2: An example of a CASB rule for blocking suspicious logins.

#### Block access from risky countries and networks

You can create a blocklist of countries where your organization does not have a presence but is the source of attacks. Or based on the IP reputation provided by Proofpoint, you can block or require multifactor authentication (MFA) for access from risky networks such as Tors, proxies and virtual private networks (VPNs) used for anonymity by attackers.

## PEOPLE-CENTRIC ACCESS

To meet security and compliance requirements, enterprises must secure access to approved apps and corporate data to all users. These include employees that might be on-site or remote, as well as contractors, partners and suppliers. But just because the cloud enables universal access doesn't mean you should. Organizations need to be able to author policy sets specific to the user's role and privileges and the sensitivity of the app and the data it holds. People are the new perimeter and securing them requires thoughtful user experience. Proofpoint helps you apply adaptive access controls for users/groups who are Very Attacked People™ (VAPs) or have access privileges to high-value data, systems and resources.

### What is a VAP?

Just as people are unique, so is their value to cyber attackers and risk to employers.

They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have unique professional contacts and privileged access to data, systems and resources.

These three factors – vulnerability, attacks and privilege – determine their overall risk.

**V: Vulnerability.** They may use unmanaged devices or untrusted networks without VPNs or ZTNA controls. They might be prone to opening phishing email or clicking unsafe links.

**A: Attack.** They are heavily targeted by cyber attacks. This might mean receiving a high volume of attempted attacks, being targeted in unique and potent ways, or by especially successful attackers.

**P: Privilege.** They have access to valuable data, systems and resources. Sometimes the privilege may not be obvious. An assistant may not have access to valuable company data. But that user has access to executive email, contacts and calendar, useful in BEC-style attacks.

A VAP is someone who poses an elevated risk because of any combination of these factors.

Not everyone is a VIP. But anyone can be a VAP.

### Common Policies

Here are common CASB policies for managing access according to users' individual vulnerability, attack profile and privilege.

#### Enforce MFA for VAPs

You can elevate security for users at risk. For example, if certain users are identified as VAPs by Proofpoint's people-centric threat intelligence, you can block or challenge their access to sensitive apps.

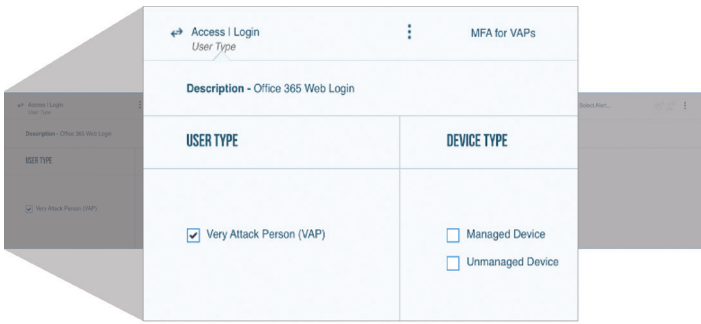


Figure 3: An example of a CASB policy rule to control what devices VAPs can use to access Microsoft 365 on the web.

You can allow users to browse an application inside of a secure isolation browser in read-only mode. Or you can prevent upload and download of files with DLP violations.

Employees in most organizations routinely share high-value content in the cloud. This includes everything from employee and client records to source code and formulas. Detecting and preventing data breaches and compliance violations is critical. First, you need risk-aware data security that can perform data loss prevention (DLP) scans in real time. Then you need to be able to block sensitive content from being uploaded to the cloud or downloaded to personal devices.

### Common Policies

Here are common CASB policies used to help secure devices

#### Read-only access for unmanaged device not on trusted networks

Employees access corporate data in sanctioned applications such as Microsoft 365, Salesforce, Atlassian and more from their personal devices. That activity creates new risks for your corporate data.

When data is downloaded or synced to a personal device, the information travels beyond your protected environment. If a device is stolen, the data is lost.

That's why an organization may want to allow users to access collaboration tools from any device but limit data downloads to managed devices only. With CASB, you can easily create a policy that directs unmanaged devices to a secure isolated browsing session that doesn't allow any file uploads or downloads.

#### Block DLP violations for unmanaged device, even on corporate network or equivalent

More than half of data breaches are caused by malicious or criminal attacks. When the user is on corporate network or VPN, the risk of an outside cyber attack is lower. In this case, you may want to allow non-sensitive file downloads to unmanaged devices while blocking sensitive file transfers.

With CASB, you can create a policy that would direct users into an isolated session that applies enterprise DLP policies on all file transfers. If a DLP violation is detected, the transfer is blocked.

### Enforce access via Virtual Private Network (VPN) for privileged users of sensitive apps

You can block access to sensitive apps by privileged users unless they are using a corporate VPN or zero-trust network access (ZTNA) such as Proofpoint Meta. You can define IP ranges for your corporate network and VPN.

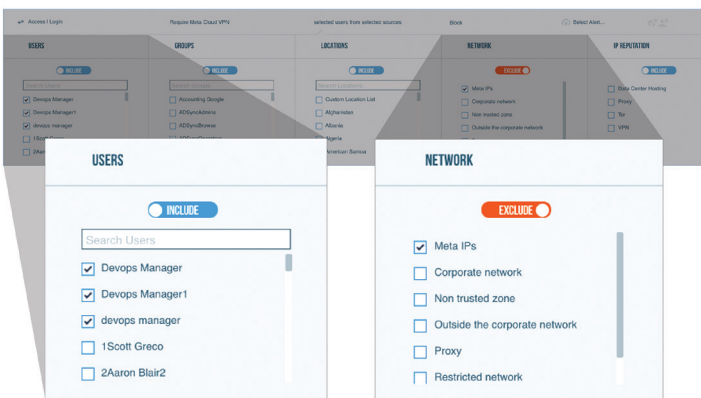


Figure 4: An example of CASB rules for requiring VPN or ZTNA for admins and other privileged users for remote access.

### DEVICE-BASED CONTROLS FOR REAL-TIME DATA LOSS PREVENTION

Poor device security poses one of the biggest risks of unmanaged devices. When an employee accesses company data over an unsecure network on an unmanaged device, the risk of leaks or loss soars. The information can be easily accessed and shared by others outside of the organization unless you have deployed controls on the apps used to access, share and save it.

With CASB-enabled adaptive access controls, you can allow your people to access cloud apps securely from anywhere on any device. CASB:

- Detects device certificates
- Helps you create data security policies for devices
- Enforces real-time controls via integration with Proofpoint SaaS Isolation

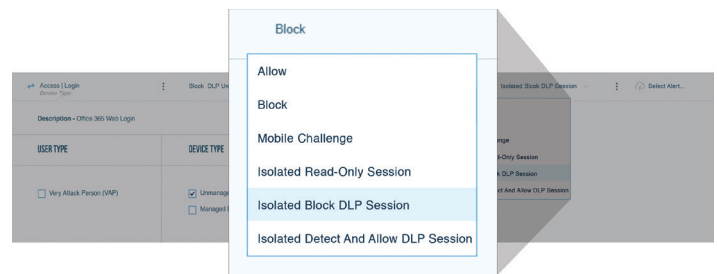


Figure 5: An example of a CASB rule for blocking sensitive content download on unmanaged devices.

## DEPLOY QUICKLY IN THE CLOUD

CASB's adaptive access controls redirect your cloud app logins to our SAML gateway. This gateway brokers the federated authentication between each service provider and the identity provider. It is deployed in-line with the identity provider.

To each application the SAML gateway appears as the identity provider. To the actual authoritative identity provider (which maintains the user directory and manages user lifecycles), the SAML appears as a service provider.

User provisioning and other identity workflow management functions are retained by the identity and access management solution. Based on rule engine evaluation, the SAML gateway supports multiple access control actions. These include MFA, session protection and real-time DLP.

Compared to forward- and reverse-proxy-based approaches, our SAML gateway offers distinct architectural advantages for real-time account controls and DLP. Here are a few:

- **Works with any device.** You can secure app access for any user on and off the corporate network for both corporate-managed and personal devices.
- **Works with any IT-approved app.** The SAML gateway can support any IT-approved cloud app that supports SAML 2.0 and is federated through an identity provider.
- **Doesn't require an endpoint agent:** Because the SAML gateway acts as an identity provider and inspects the login transaction, it does not require an agent on the endpoint to route traffic. Not having to manage the lifecycle of a user's device means better time to value.
- **Policy-driven:** Adaptive access controls offer customizable flows for threat, DLP and app controls. These options let you balance risk against trust.
- **Robust and scalable:** The SAML gateway does not rely on techniques such as URL re-writes or SSL termination to inspect network traffic. Inspecting only the login transaction means low latency. As such, there is no risk of "breaking" the cloud app and no loss of cloud app coverage.
- **Offers user privacy.** Unlike other inline solutions, the SAML gateway neither inspects all data nor does it have visibility to user credentials. If the user is re-directed to browser isolation for data loss prevention, only file transfers are inspected. No data is stored unless there is a policy violation. This preserves the user's and organization's data privacy.

Because Proofpoint CASB is agentless and cloud-based, implementation can happen quickly—with no additional hardware to install. With the help of Proofpoint Professional Services, most organizations can implement cloud access and data controls in a matter of hours.

## PRODUCTS

### Proofpoint Cloud App Security Broker (CASB)

Proofpoint CASB helps you secure cloud applications such as Microsoft 365, Google G Suite, Box and more. We protect you from account compromise, oversharing of data and compliance risks in the cloud. Our solution gives you adaptive controls to secure access to your cloud apps. With CASB, you get:

- People-centric visibility to threats
- Automated response capabilities
- Comprehensive data security with DLP
- Cloud app and third-party apps governance

Our agentless architecture delivers unparalleled time to value and enforces policies in real time. Our powerful analytics help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you.

### Proofpoint SaaS Isolation

SaaS Isolation is an optional add-on to Proofpoint CASB that secures users' access to cloud apps and data by isolating browser sessions in a secure container. This unique solution secures file uploads and downloads for risky users and behaviors. It applies cloud DLP policies to file transfers in real time, preventing theft or loss of sensitive data. It helps you solve the security, productivity and privacy challenges that come with high-risk cloud use. SaaS Isolation supports any IT-approved application through our agentless architecture. It's simple to deploy, manage and support.

#### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at [www.proofpoint.com](http://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](http://Proofpoint.com)