Check Point CloudGuard SaaS
Identity Protection

Hackers are after your Identity

Account Takeover in SaaS applications is a form of identity theft in which a threat actor steals an individual or employee's valid login details, and then uses them to impersonate the user in order to carry out activities and transactions in their name.
With 90% of SaaS data breaches caused by an employee account takeover, the surge in Identity Protection solutions continues to grow.

Most employee SaaS account takeovers occur in the following ways:

- **Phishing**
- External **malware**;
- **Man-in-the-Middle** attacks (on an Airport or a Café Wi-Fi™, for example)
- **Password Spraying** and other brute force techniques
- Various types of **session hijacking**

CloudGuard SaaS Identity Protection

Check Point CloudGuard SaaS Identity Protection delivers the most secure access and avoids ID theft. CloudGuard SaaS provides leading identity protection for all SaaS applications, including Microsoft Office365, G Suite, OneDrive, Dropbox, and Box.

Check Point has developed a unique Identity Protection engine, which integrates with any Identity Provider and SaaS Provider that supports the SAML 2.0 protocol.

CloudGuard SaaS utilizes intelligence engines within CloudGuard SaaS, as well as leverages Check Point's rich threat intelligence, ThreatCloud™, to make smart decisions about user logins to SaaS applications. Thus, "bad" scenarios, such as suspicious location login attempts, impossible travel login attempts, anomalies in user actions, bad reputation source IP addresses, or prohibited geographic locations, are identified and the user (or hacker) activity is reported and/or blocked from accessing the SaaS account.

CloudGuard SaaS Identity Protection offers three deployment modes:

- One-time passcode via SMS (Agentless Mode)
- One-time passcode via in-app Push Notification (Hybrid Mode)
- Interrogation of device via the Agent to assess device security posture and other contextual meta-data (Agent Mode)

CloudGuard SaaS Identity Protection adds layers of security not offered by other MFA solutions and provides the following benefits:

1. **Security Posture of the device (2FA is not enough!)** – If the device is at risk as determined by the ID-Guard™ Agent (the Agent), then the device is not allowed to access the protected SaaS applications. The use of the Agent is optional, but required to obtain the security posture of the device. By requiring the Agent, an infected device will be prevented from accessing the protected SaaS applications, no matter if the user is authenticated.
2. **Mix Mode (Hybrid Mode) capability** – When configured, the user can access protected SaaS applications from an agentless device by receiving and using a one-time passcode sent via in-app push to the Agent running on at least one device per user. This configuration also enables the authorization process with a fallback mode to offer flexibility in many deployment scenarios to best fit your organization's needs and requirements.
3. **Rich SaaS Intelligence** – Identifies suspicious user activities and SaaS configurations with anomaly detection, compliance definitions, AI, and machine learning. Detects identity theft and account takeover during and after the fact, regardless of the authentication process.
    a. **Contextual Access** – Based on contextual meta-data, such as device location, IP address, etc., the device can be allowed or blocked access to protected SaaS applications based on policy. For example, your policies may allow devices located within your corporate network (IP address range context) to be granted access to selected SaaS applications, but additional inspection is required for devices outside of your corporate network. Additional inspection may prevent users from accessing protected SaaS applications unless these users are inside the corporate network, otherwise the user may be required to use of a one-time passcode.
    b. **Anomaly Detection** - Identifies impossible travel events, such as logging in from the US and within 1 hour logging in from the UK. Identifies new device from new location. Identifies mailbox rules to forward email to an external domain or to delete security warning emails as they come in.
4. **Threat Intelligence** – Identifies malicious sources, networks, and IP addresses. Takes action feeding off a huge intelligence community, validating and sharing risks for collateral benefit.

CloudGuard SaaS Identity Protection allows your organization to choose between modes per policy: Agent Mode, Agentless Mode, or Hybrid Mode. For example, CXO level users may belong to a group that allows them to use Agent and Agentless devices (Hybrid mode), but all other groups must use Agent devices (Agent mode). In another example, the policies may require an Agent device when located outside the corporate network only.

This capability of per policy deployment modes provides the most flexibility to best fit your organization's needs and requirements.

Read on for a detailed description of Identity Protection deployment modes.

Agent Mode

In Agent mode, CloudGuard SaaS secures SaaS logins deterministically via an endpoint agent (ID-Guard Agent) that is installed on organizational and personal endpoints, such as desktops, laptops, and mobile devices.

Agent Mode enables the administrator to guarantee access to SaaS applications only from known and risk-free endpoints.

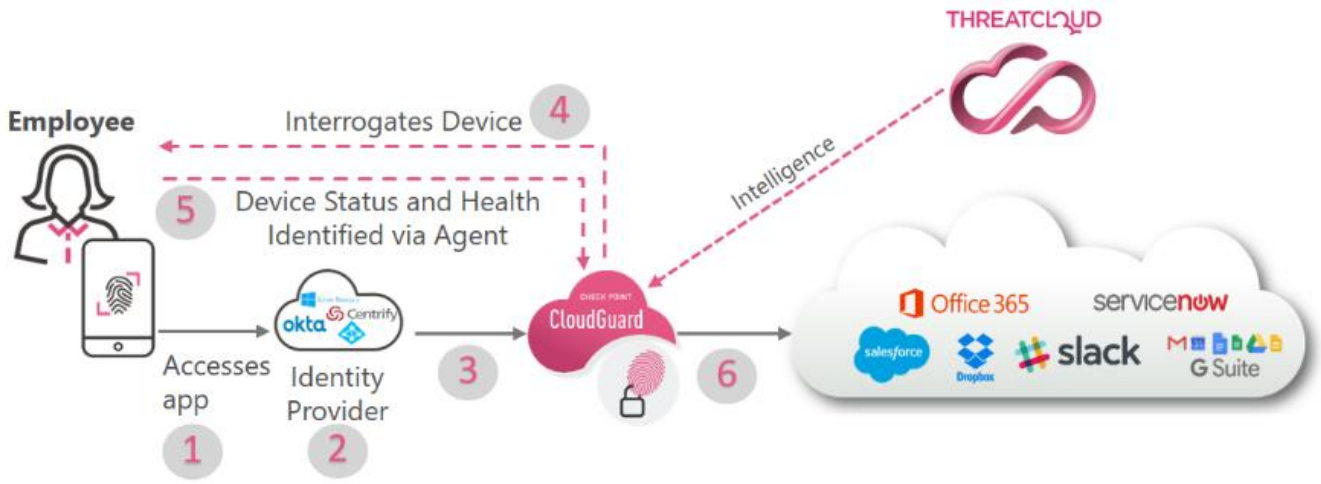
An effective security agent allows the following benefits:

- Applies to ALL use cases: mobile, PC, native apps, etc.
- Provides built-in security for the device, which allows enterprises to detect malicious activity and further secure access to SaaS applications.
- Does not require IT admins to manage any certificates
- Deploys easily with or without device management systems
- Provides secure second factor authentication without additional user involvement, absolutely hassle free
- Create policies that require context-specific authentication methods and security, based on specific authentication attempt scenarios. Context will vary from no risk to high-risk attempts.
- Determine context by device IP addresses and networks, device type and location, users and groups' context, SaaS applications in use, and risk level.
- Decide the appropriate authentication control for any scenario, maximizing security, and minimizing user hassle.

CloudGuard SaaS Identity Protection with the Agent is transparent to users and does not require their involvement when accessing SaaS services from registered endpoints.

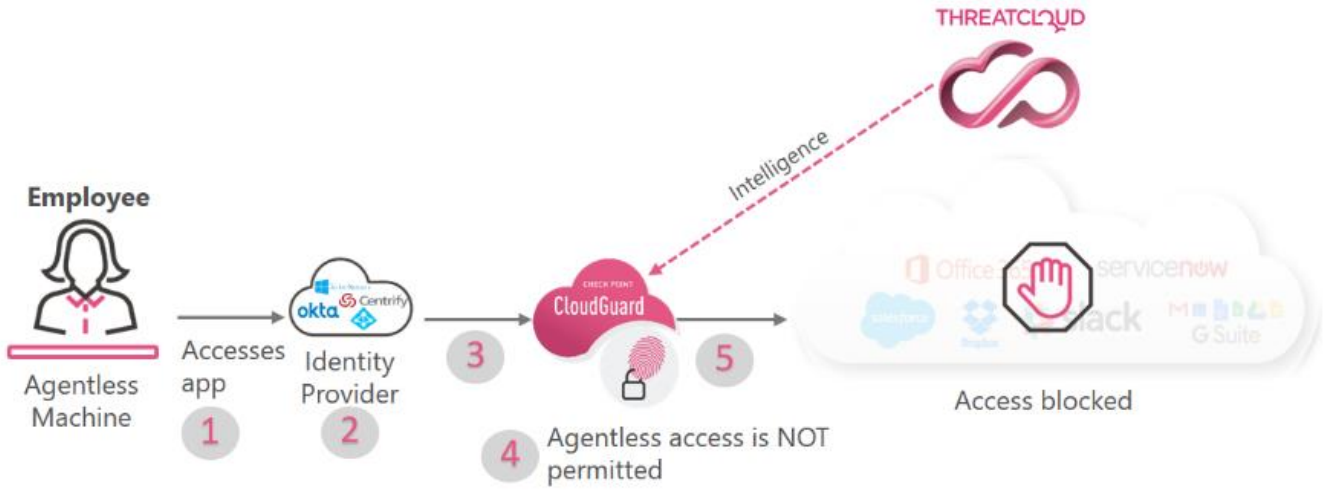
How it works: Legitimate Employee accessing SaaS account from Agent device

When an employee attempts to access a SaaS account (1), their access is authenticated by an identity provider (2), such as Microsoft ADFS, G Suite, okta, etc. CloudGuard SaaS (3) then matches the user's identity and sends a query to the user's device (4) to check if the Agent is installed. Once the Agent is verified (5) and any contextual meta-data is inspected, the user and device will be authorized to log into the SaaS application (6) without user intervention.



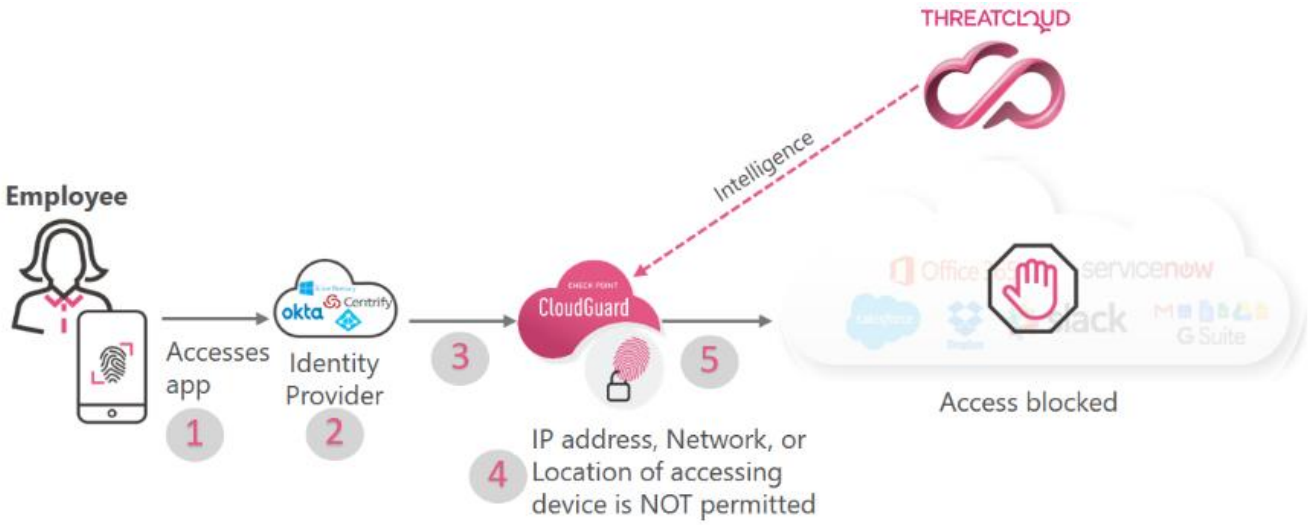
How it works: Legitimate Employee accessing SaaS account from Agentless device (not permitted)

When the employee attempts to access a protected SaaS account (1) from an agentless device, their access is authenticated by the identity provider (2). If the corporate policy has been configured block agentless access (4), then the login session will be blocked (5). For more information regarding Hybrid Mode, please see that section below.



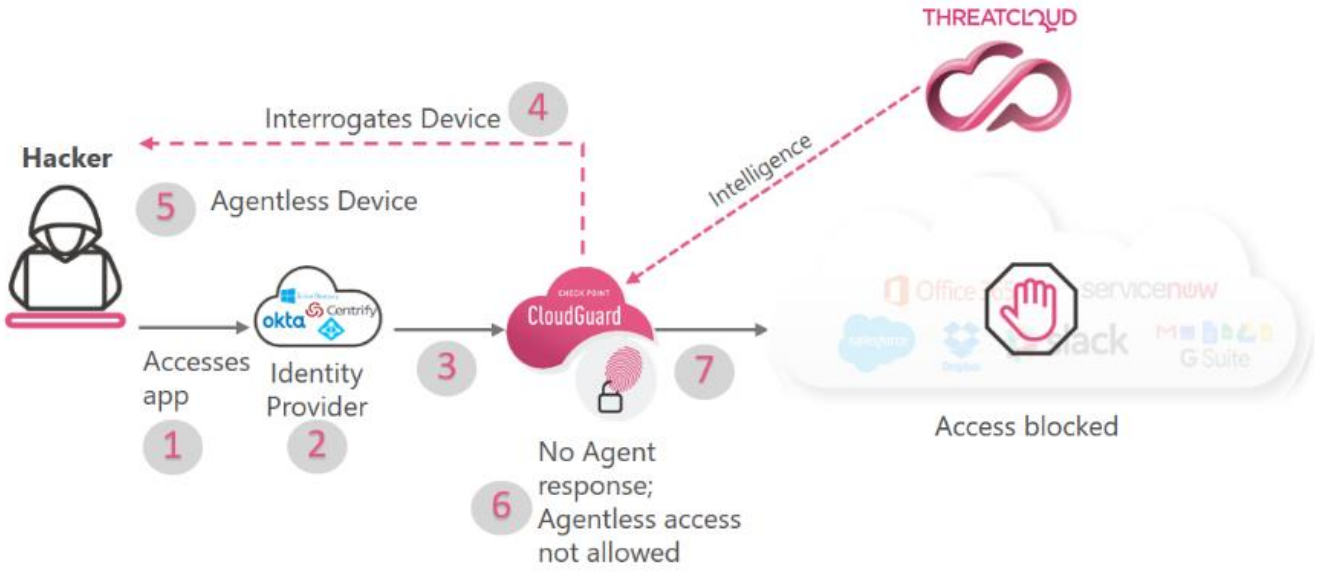
How it works: Legitimate Employee accessing SaaS account from Agent device from non-permitted location

When an employee attempts to access a SaaS account from an Agent device (1), their access is authenticated by the identity provider (2). CloudGuard SaaS (3) matches the user's identity and checks contextual meta-data, such as location or IP address, for the accessing device. If the contextual meta-data is not allowed (4), such as the device is in Moscow, and access for this user is not permitted from Russia, then the access is blocked to the SaaS account (5).



How it works: Hacker accessing SaaS account with stolen identity credentials

In case a hacker tries to access the SaaS application with a stolen identity, CloudGuard SaaS matches their identity against logins from an agent-installed device. When the Agent is absent from a device, the user will not be authorized to access the SaaS application, even if they have the correct credentials.



Agentless Mode

An agentless mode allows CloudGuard SaaS Identity Protection to start protecting SaaS identities all across your organization immediately, without the need to deploy on-device agents. Besides allowing two-factor authentication through SMS; network, location, or device-type can be used as basic, but efficient contextual access controls.

Key functionality of CloudGuard SaaS Identity Protection's contextual access control policies are:

- Create policies that require context-specific authentication methods and security, based on specific authentication attempt scenarios. Context will vary from no risk to high-risk attempts.
- Determine context by device IP addresses and networks, device type and location, users and groups' context, SaaS applications in use, and risk level.
- Decide the appropriate authentication control for any scenario, maximizing security and minimizing user hassle.

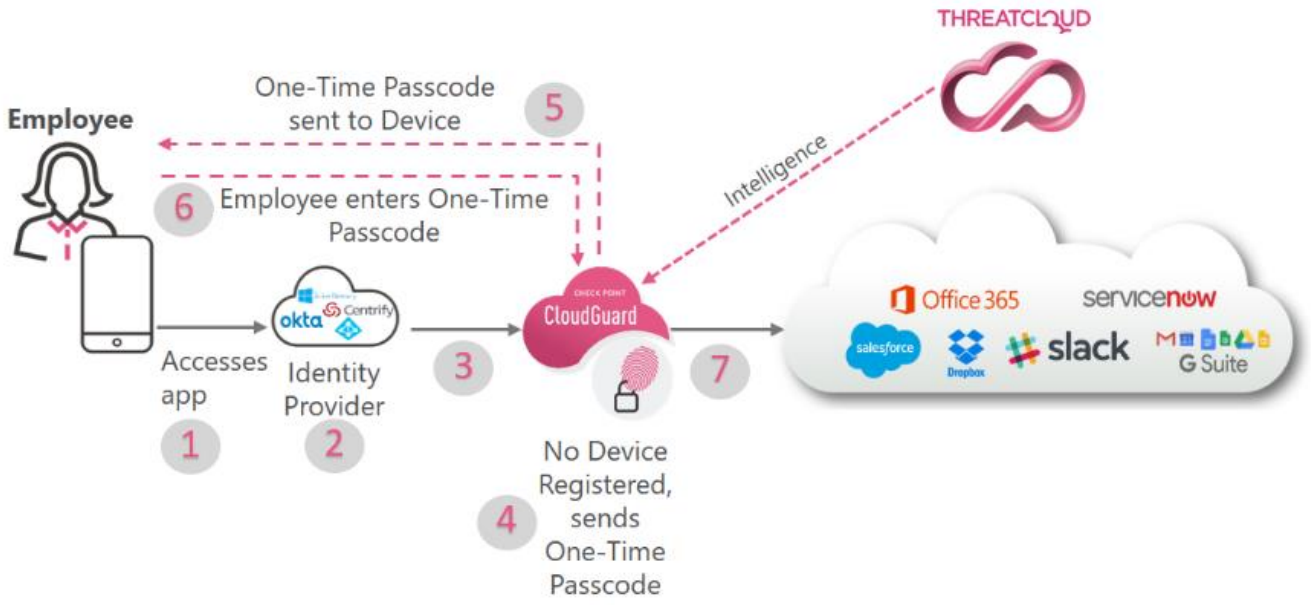
The agentless mode leverages the same threat intelligence as Agent Mode to make smart decisions about user logins to SaaS applications. Thus, "bad" scenarios, such as suspicious location login attempts, impossible travel login attempts, anomalies in user actions, bad reputation source IP addresses, or prohibited geographic locations, are identified and the user (or hacker) activity is reported and/or blocked from accessing the SaaS account.

Agentless Mode provides the following security benefits:

- Policy rules for device type, OS, IP, and location
- Centralized multi-factor authentication
- Machine learning engines validate user logins and identify bad scenarios, such as unusual SaaS app activities, different locations, and different devices
- Status check-ups for rules, permissions, privileges, etc.

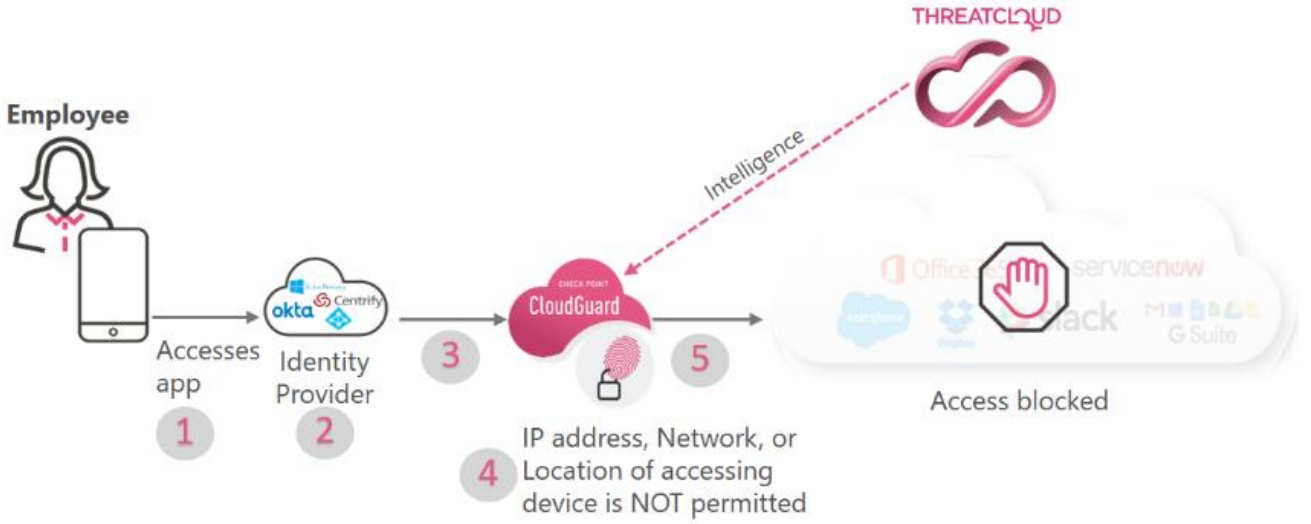
How it works: Legitimate Employee accessing SaaS account from Agentless device

When an employee attempts to access a SaaS account from an agentless device (1), their access is authenticated by the identity provider (2). CloudGuard SaaS (3) then matches the user's identity and sends a query to the user's device to check if the Agent is installed. Noting that the Agent is not installed nor registered on the accessing device (4) and there is no contextual access meta-data preventing further login; the CloudGuard SaaS (5) sends a one-time passcode over SMS to the user's smartphone. The user enters this one-time passcode into the SaaS challenge (6). Once the one-time passcode is verified, the user and device will be authorized to log into the SaaS application (7).



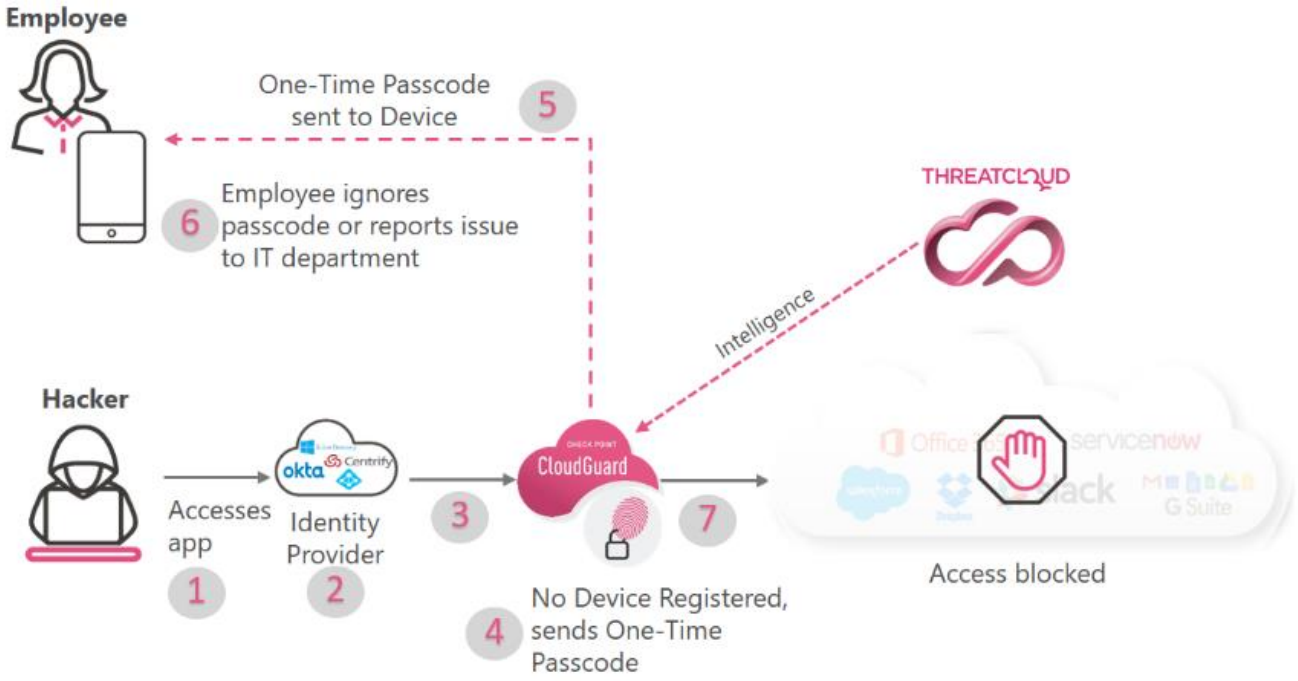
How it works: Legitimate Employee accessing SaaS account from agentless device from non-permitted location

When an employee attempts to access a SaaS account from an agentless device (1), their access is authenticated by the identity provider (2). CloudGuard SaaS (3) matches the user's identity and checks contextual meta-data, such as location or IP address, for the accessing device (4). If the contextual meta-data is not allowed, such as the device is in Moscow, and access for this user is not permitted from Russia, then the access is blocked to the SaaS account (5).



How it works: Hacker accessing SaaS account with stolen identity credentials

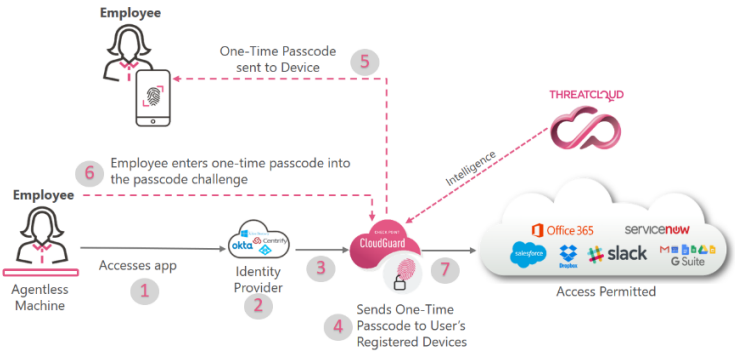
When a hacker attempts to access a SaaS account from an agentless device (1), their access is authenticated by the identity provider (2). CloudGuard SaaS (3) then matches the user's identity and sends a query to the user's device to check if the Agent is installed. Noting that the Agent is not installed nor registered on the accessing device, further contextual access meta-data, such as location or impossible travel, may immediately block access. However, if there is no contextual access meta-data preventing further login, then the CloudGuard SaaS (4) sends a one-time passcode over SMS to the user's smartphone (5). The hacker does not receive this one-time passcode, and therefore, will not have the correct passcode to enter into the SaaS challenge. The hacker's login will be blocked (7) and the attempt will be reported to the administrator via the console.



Hybrid Mode

When configured, the user can access protected SaaS applications from an agentless device by receiving and using a one-time passcode sent via in-app push to the Agent running on at least one device per user. This configuration also enables the authorization process with a fallback mode to offer flexibility in many deployment scenarios to best fit your organization's needs and requirements.

How it works



At least one device per user, often a mobile device such as a smartphone, must have the Agent installed and registered. This registered device will receive an in-app notification containing a one-time passcode the user will enter into the challenge from the SaaS website when accessing protected SaaS applications from agentless devices.This is the same scenario as Agentless Mode, except that the one-time passcode is sent via an in-app push notification (5) to the Agents running on the user devices. In-app push notifications are more secure than sending the one-time passcode via SMS, which can be spoofed or intercepted.