CHECK POINT

CloudGuard™ SaaS

SUPERIOR THREAT PREVENTION FOR SaaS APPLICATIONS

Office 365 · G Suite · box · salesforce

Dropbox · servicenow · slack · EGNYTE

THE SaaS SECURITY CHALLENGE – NOT WHAT YOU'D EXPECT

Organizations seeking to optimize business operations and reduce costs increasingly move to cloud applications and software-as-a-service (SaaS) products. In fact, Gartner maintains that over 70% of the organizations already use cloud applications.

However, while SaaS applications improve business agility, they also expose businesses to risks. Enterprise SaaS applications are highly exposed, as they only require an internet connection and can be accessed by anyone, anywhere. Furthermore, SaaS applications are provided with insufficient default security that allows unrestricted file sharing and malware delivery.

90%
OF SaaS BREACHES CAUSED BY HACKING

Surprisingly, the biggest risk in enterprise SaaS usage does not come from mindless data sharing, but from external threats. These mainly come in the form of unauthorized access to corporate SaaS accounts. Indeed, Check Point's Incident Response team found that an alarming 90% of the SaaS breaches are caused by hacking. Specifically, 50% of these breaches are caused by a takeover of employee SaaS account.*

*Check Point Incident Response statistics, 2017

Check Point CloudGuard SaaS
SUPERIOR THREAT PREVENTION FOR SaaS APPLICATIONS

BENEFITS

- Block malware delivery and zero-day threats
- Prevent SaaS account takeovers
- Protect file sharing and sensitive data
- Manage from a unified console
- Ensure comprehensive security coverage
- Gain full visibility into shadow IT

FEATURES

- Zero-Day Threat Prevention
- Identity Protection
- Comprehensive Threat Intelligence
- Simplified Management
- Data Leakage Prevention
- Shadow IT Discovery

KEY STRENGTHS

- Award-winning zero-day threat prevention
- Unique technology prevents SaaS account takeovers
- Powered by Check Point Infinity architecture

ELIMINATE REAL SaaS THREATS

Office 365 · G Suite · box · salesforce
Dropbox · servicenow · slack · EGNYTE

Check Point CloudGuard SaaS prevents attacks on enterprise-used SaaS applications.

While most solutions in the SaaS security space focus purely on application control and data leakage, CloudGuard SaaS provides complete protections against hijacking of employee SaaS accounts, sophisticated malware and zero-day threats, and sensitive data sharing.

CloudGuard SaaS is the only security solution tailored for real SaaS threats.

USE CASES

- Block Malware and Zero-Day Threats
- Stop Phishing Emails for Office 365 and G Suite
- Block Unauthorized Access to Saas on Mobile and PCs
- Block Sharing of Sensitive Data
- Detect and Control Shadow IT
- Manage Security from a Single Pane of Glass

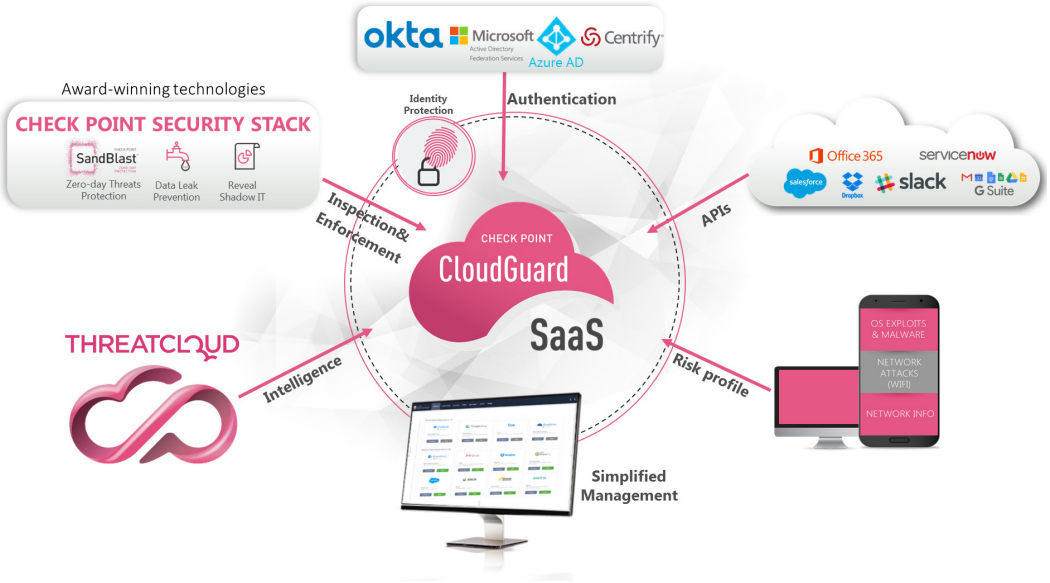
HOW DOES IT WORK?

Check Point CloudGuard SaaS is offered as a cloud service that protects enterprise SaaS applications, within minutes' deployment. Installed in the cloud, it integrates with various SaaS providers using APIs.

When a user shares an email / file through SaaS application, CloudGuard SaaS is notified through API. Its security engine then scans the data for threats and malicious content, and determines if it needs to be quarantined, cleaned, removed, etc.

Scanning the data for threats, CloudGuard SaaS uses a full-blown Check Point security stack. This includes: the award-winning SandBlast technology for zero-day threats protection and malware prevention; a data leak prevention engine; and the ability to reveal shadow IT scenarios. Designed to protect from real SaaS threats, CloudGuard SaaS also provides Identity Protection, with ID-GuardTM, a patent-pending technology that prevents SaaS account takeovers.

Activity is logged and can be monitored in a web-based management console, as well as through Check Point's renowned SmartConsole. Powered by Check Point Infinity architecture, CloudGuard SaaS provides consolidated activity logging and policy management for cloud and on premise, as well as rich threat intelligence for a comprehensive security coverage all across the board.



PREVENT EMPLOYEE ACCOUNT TAKEOVER WITH ID-GUARD™ TECHNOLOGY

An **Account Takeover** is a form of identity theft in which the legitimate credentials of an employee are stolen and used illegitimately by a cybercriminal. By impersonating the user, the criminal is then able to carry out activities and transactions in the victim's name.

CloudGuard SaaS uses ID-GuardTM patent pending technology to prevent unauthorized users and compromised devices from accessing your SaaS apps, thus stopping them from taking over SaaS user accounts. It intercepts them using machine learning algorithms that analyze user behavior and feed off of sources like: mobile and PC on-device detection of OS exploits, malware and network attacks, SaaS native APIs, and Check Point's Threat Cloud.

Identity Protection with ID-GuardTM technology: CloudGuard SaaS Identity Protection uses ID-GuardTM technology to ensure legitimate access to SaaS applications and prevent takeover of employee SaaS accounts. CloudGuard SaaS integrates with various identity providers, like: Okta, Microsoft Active Directory, Azure Active Directory, etc., and adds

a layer of security to their authentication process. Whenever a user attempts to access a SaaS account, whether through mobile or a PC, CloudGuard SaaS matches their identity using techniques like: device finger printing, logins checkup, locations validation for login and emails, and so on. By incorporating CloudGuard SaaS inputs into identity provider's authentication process, suspicious logins (e.g.: seen in two different locations, bad IP reputation) are immediately denied and blocked. CloudGuard SaaS Identity Protection is transparent to users and does not require their involvement.

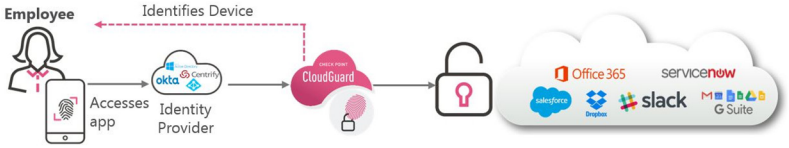
CloudGuard SaaS Identity Protection Works in Two Modes

1. Agent Mode

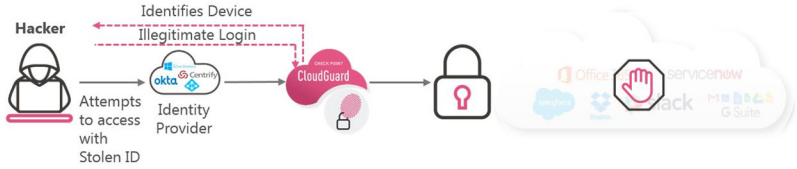
ID-GuardTM in agent mode provides leading identity protection for all SaaS applications including Office365, G Suite, Salesforce, Microsoft Azure and Amazon AWS management consoles. It offers an end-point agent that is installed on organizational and personal end-points like desktops, laptops, and mobile devices, and secures SaaS logins deterministically.

How? When an employee attempts to access a SaaS account, their access is authenticated by an identity provider. CloudGuard SaaS then matches their identity: it sends a query to the employee's device to check if an ID-GuardTM agent is installed. Once ID-GuardTM is found, the user and device will be authorized to log into the SaaS application.

CloudGuard SaaS Identity Protection with ID-GuardTM technology is transparent to users and does not require their involvement.



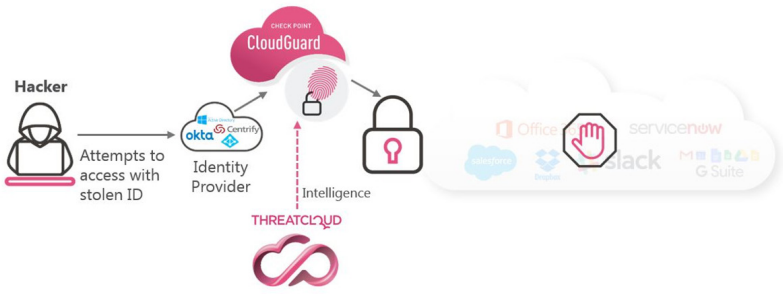
In case a hacker tries to access the SaaS application with a stolen identity, CloudGuard SaaS matches their identity against logins from an agent-installed device. When ID-GuardTM agent is absent from a device the user will not be authorized to access the app, even if they have the credentials.



2. Agentless Mode

An agentless mode allows ID-GuardTM to instantly work all across your organization, without the need to deploy on-devices agents. Besides allowing two-factor authentication through SMS; network, location, or device type can be used as basic but efficient controls.

This mode leverages Check Point's rich threat intelligence coming from its wide install-base and on premise security gateways to make smart decisions about user logins to SaaS applications. Thus, "bad" scenarios like: suspicious locations login attempts, anomalies in user actions, and bad reputation source IP, are identified and the hacker is blocked from accessing the SaaS account.



PREVENT ZERO-DAY THREATS WITH AWARD-WINNING TECHNOLOGY

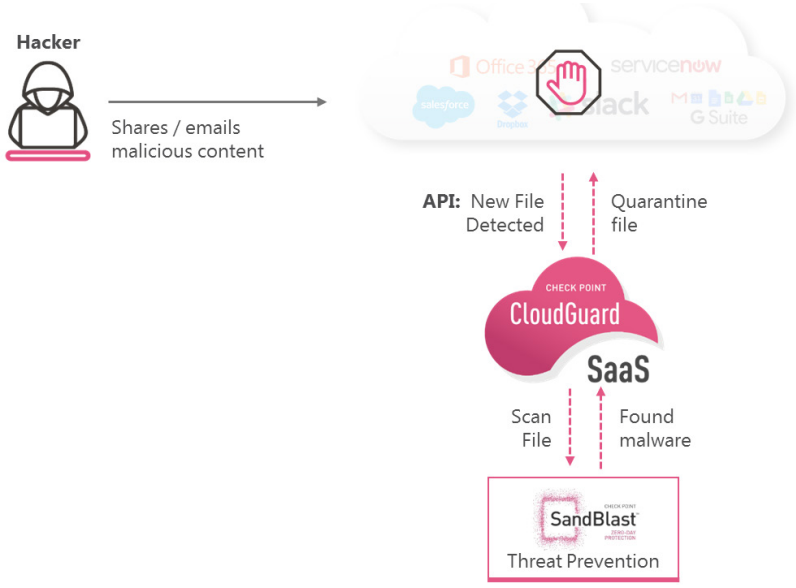
Check Point CloudGuard SaaS prevents malware and zero-day threats from getting into SaaS apps. With a simple add-on deployment, CloudGuard SaaS Threat Prevention prevents phishing and zero-day malware attacks, protects in-app file sharing, quarantines malicious emails and files, and provides a multi-layered protection.

Its comprehensive email security suite for Office365 and Gmail includes anti-phishing and malware prevention technologies, which unlike traditional MTAs or SMTP gateways use APIs to integrate with email providers. This means:

1. Network changes are not required
2. Internal correspondences are scanned to prevent lateral movement of threats

CloudGuard SaaS uses Check Point's award-winning SandBlast technology, which includes:

- Evasion-resistant CPU-level threat emulation blocks first-time seen malware and keeps you protected from the most advanced cyber threats
- Proactive threat extraction sanitizes files and eliminates potential threats to promptly deliver a safe file version to users
- Anti-virus protection blocks known malware
- Anti-phishing for SaaS email provides advanced protection of user emails through URL filtering and content analysis



CloudGuard SaaS prevents malware delivery even on unmanaged devices and anywhere your SaaS applications are accessed from.

PROTECT DATA WITH CLOUDGUARD SaaS DATA LEAKAGE PROTECTION

CloudGuard SaaS detects sensitive data sharing via SaaS and immediately limits data exposure. It enables you to force a data encryption policy based on your company needs.

How? When an employee shares data through SaaS application, CloudGuard SaaS is notified through an API. The file is then scanned and in an event of sensitive data sharing; like credit card details, or competitive information, file sharing is blocked, or "unshared" (e.g. Box, Dropbox) to prevent data leaks.

Prevent Shadow IT

CloudGuard SaaS extends Check Point's capabilities in shadow IT detection and control. It detects shadow IT of SaaS applications, adding to Check Point's security gateways that provide wide and granular shadow IT control for cloud applications, as well as application control and risk scoring for new and traditional apps.

CloudGuard SaaS processes email notifications (e.g., "You have a new slack message") and uses them as additional validators to detect shadow IT cases. CloudGuard SaaS shadow IT detection is available on CloudGuard web user interface and will soon integrate with Check Point SmartEvent.

With that, Check Point allows enterprises to both detect and prevent risky applications usage and control shadow IT usage with a granular policy down to action level.

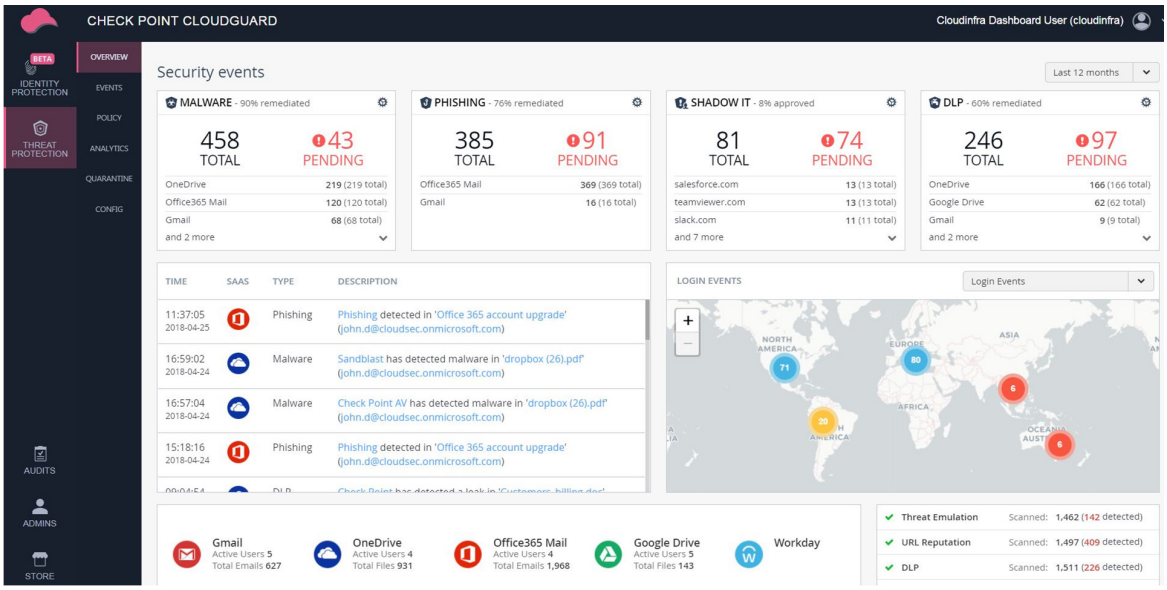
Refer here: https://appwiki.checkpoint.com for the full list of supported apps.

END-TO-END SaaS SECURITY COVERAGE AND UNIFIED MANAGEMENT

CloudGuard SaaS provides a comprehensive security coverage across the enterprise. It uses Check Point Infinity architecture and enables consistent policies and shared threat intelligence across network, cloud, and mobile devices. Deployed within minutes, it also provides a simplified management platform that instantly scans for previous and current threats

CloudGuard SaaS offers both an autonomous web user interface and a consolidated management option using Check Point SmartConsole.

Check Point SmartConsole simplifies security management with centralized monitoring for CloudGuard SaaS:



- Traffic is logged and can be easily viewed within the same dashboard as Check Point security gateways
- Security reports can be generated to track security compliance across the entire network