CloudGuard SaaS Reference Architecture

Scope

The recommendations in this document are designed to inform engineers, architects and enterprise security professionals, who want to deploy SaaS applications to internal users without compromising the existing security posture. Readers should be well versed in SaaS applications and Check Point services, and have an interest in finding a modern approach to secure the use of SaaS applications. This document deals specifically with the use of Check Point CloudGuard SaaS as a core product.

Contents

What drives an organization to adopt SaaS apps? ................................................................. 2
Security considerations of SaaS applications ........................................................................ 3
The legacy approach ....................................................................................................................... 4
Legacy technology ......................................................................................................................... 4
Obstacles encountered when using the network-centric approach ............................................. 5
A New Approach – API-driven SaaS security .............................................................................. 5
Overview ..................................................................................................................................... 5
The benefits of the APIs to SaaS application security ................................................................. 6
Check Point CloudGuard SaaS security platform ....................................................................... 7
CloudGuard SaaS architecture ..................................................................................................... 7
Putting identity at the core of SaaS application security ............................................................. 8
Check Point security for SaaS applications ................................................................................. 8
CloudGuard management platform .............................................................................................. 8
CloudGuard SaaS and a zero-trust approach .............................................................................. 9
Designing a CloudGuard SaaS solution ...................................................................................... 9
Designing Identity Protection using Agent-mode ......................................................................... 10
Designing Identity Protection using Agentless-mode .................................................................... 12
Designing Threat Prevention security using CloudGuard SaaS .................................................. 13
CloudGuard SaaS Use Cases ..................................................................................................... 15
Use case – Quick deployment required for new SaaS application ............................................. 15
Use case – OneDrive for all corporate users ............................................................................ 15
Use case – Migrating to Salesforce .............................................................................................. 15
Use case – Dropbox; document sharing and DLP ........................................................................ 16
Use case – Migrating to zero-trust architecture ......................................................................... 16
Integration & Logging .................................................................................................................. 17
Conclusion .................................................................................................................................... 20

Introduction
Software-as-a-Service (SaaS) has evolved from simple email platforms designed for the everyday user, to targeting organizations of all sizes, who have realized the benefits that these applications offer, and have adopted them for corporate use.

According to Forbes, 70% of enterprises have adopted cloud applications, making SaaS a norm for modern businesses. SaaS adoption allows organizations to incorporate everything from cloud-based finance apps to full office suites, into their daily operations.

It is now even possible to run an entire business via SaaS apps.

**Forbes 2017: 70% of enterprises adopted cloud applications**

This is a paradigm shift from the days of hosting services in data-centers, dealing with support, licensing and uptime, to organizations now having a better experience though subscription based SaaS apps.

The change should also be reflected in the way security is approached, i.e. moving away from a network-centric approach to API-driven security, as will be discussed below.

As is often the case with the adoption of new solutions, some very serious security questions will become apparent when the time comes to consider how the organization will use SaaS applications. For example: where does data reside when stored in SaaS apps and how secure is the SaaS app platform from abuse?

**What drives an organization to adopt SaaS apps?**

As with all architectural practices, it should be made clear why an organization would be motivated to use SaaS apps. Understanding the context in which decisions are being made will help to secure the design, make it aligned with the business’s requirements and means, and justify each solution that is deployed.

Adopting new technology and incorporating it into an established system, through the use of SaaS products, may prove to have the following benefits:

- **Cost** – SaaS applications are often more cost-effective than in-house deployments. The applications offer the chance to move more operational costs from CAPEX to OPEX, and cut back on the license, support and infrastructure costs.

---

1. *2017 State of Cloud Adoption and Security*
• **Mobility** – SaaS applications are by nature accessible from any location, which is an imperative point for organizations that have a contingent of employees working remotely. Allowing users to, for example, access platforms such as Salesforce while on the road, is crucial for modern enterprises.

• **Availability** – SaaS applications are conveniently cloud native, meaning that users can take advantage of the cloud’s inherent high-availability, no matter where in the world they may be.

• **Agility** – SaaS platforms allow organizations to work in a more agile manner as they are easily adaptable to suit any business type i.e. the integration of Salesforce into O365.

• **Security** – Organizations often perceive SaaS applications as inherently secure i.e. that the SaaS provider is responsible. This can be seen as reducing the workload on already over-burdened security teams and shift responsibility to the SaaS application providers.

• **Support**– Modern SaaS apps are often only available online, where they receive constant technical updates from their development teams. Organizations adopting SaaS apps can divest themselves from the need to support and maintain similar in-house platforms.

• **Zero-Trust** – Moving security into the application i.e. away from in-line traffic inspection, and using identity as part of the security enforcement, aligns with a Zero-Trust architectural methodology.

**Security considerations of SaaS applications**

The use of SaaS applications fundamentally moves the security ‘goalposts’, in terms of how organizations approach SaaS app security, making it important to correctly identify the associated threats, vectors and risks that these changes introduce to organizations.

“A lot of people think that nation states are running their operations on zero days, but it’s not that common. For big corporate networks, persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive.”

Rob Joyce, NSA’s Tailored Access Operations

Some of the most common challenges are the following:

• **Attack Surface** –SaaS apps are available for everyone to use, authorized or otherwise, which allows them to extend the attack surface into the cloud. Business data stored in SaaS applications should be considered as part of the attack surface.

• **Control** - Organizations need to acknowledge that they may not have full control over how an SaaS provider uses their data. While this may not be a consideration for private users, maintaining control over corporate intellectual property is a concern for business enterprises.

• **Threat Actors** – Bad actors want to compromise SaaS apps as they are considered “low hanging fruit” and targets for phishing attacks. Compromised SaaS apps are high-value targets and useful entry points into trusted networks.

• **Threat Vectors** – Corporate SaaS users will often trust the provenance of files or documents they receive, making the weponization of anything that can be disseminated to a trusting audience is a very attractive attack vector.

• **Security** – SaaS applications are built for general users as well as for corporate use, in some instances they may allow weak passwords or not support multi-factor-authentication (MFA). If this occurs, the app's security will not be aligned with the corporate security policy.

---

2 Credential Stealing as an Attack Vector
• **Data Leakage** – Organizations must be protected from the use of shadow SaaS applications, such as those that are used to share and store documents, as employees often use Dropbox and OneDrive to share information and send documents beyond their workplace’s secure network.

• **Account Takeover** – Bad actors can look to endanger SaaS accounts, by weaponizing documents and sharing them from a legitimate, but compromised, user. The takeover of a corporate 0365 account should be considered a high-value prize to a malicious actor.

• **Identity Protection** - The dual (corporate and personal) use of SaaS adds another layer of complexity to security. Phishing, man-in-the-middle and brute force techniques are all used by threat actors to gain access to corporate SaaS applications.

The above must be considered by organizations wanting to incorporate SaaS apps into their current workflows and some of the security concerns that this move would raise.

![Check Point statistics showing the danger of Account Takeover](image)

**The legacy approach**

As a global leader in cyber security, Check Point is intent on bringing its clients the most up to date and advanced technology. Today, the legacy approach is no longer a relevant mode for securing SaaS apps and should not be relied upon as an option for architects and engineers.

Network security interest began when access to SaaS apps was not a corporate concern and when security engineers thought that GWs running application-control and URL-filtering could enforce a SaaS security policy.

Approaching SaaS security using traditional modes of security, such as firewalls, is therefore, at best, problematic and out-dated. In-line packet inspection also can’t be used as a tool for enforcing SaaS application security i.e. when using a network-centric security methodology, where packets are inspected in transit and decisions are made as to their legitimacy.

The following section will discuss how the legacy, or network-centric, approach is failing as a modern method for SaaS application security.

**Legacy technology**

Traditionally security architects and engineers used services such as application-control and URL-filtering to enforce security policy, utilizing in-line security gateways or proxies. As organizations started to on-board public SaaS, security teams needed to write new network security rules to give users access to such applications.
These rules are, at best, able to inspect network traffic, identify apps and apply heuristics to allow or deny the connections. In reality, in order to make a granular security decision at a network level SSL inspection is required. This is an effective mean of enabling deep packet inspect but will often miss crucial security factors required to properly secure SaaS, for example deep-packet-inspection can prevent account takeover.

The following graphic shows the typical access path to SaaS apps through the traditional network security infrastructure:

---

The legacy approach to SaaS security using traditional architecture

1) Users are defined by network segments and routed to the Internet gateway. Remote workers use a hub-and-spoke architecture and connect to theinternet though the same gateway.

2) The internet gateway is able to perform network security functions such as DLP and zero-day malware protection. In some cases, the GW will perform SSL decryption and use an identity-based policy.

3) Sharing threat intelligence with a cloud-based platform allows IoCs to be disseminated to the wider security ecosystem.

Obstacles encountered when using the network-centric approach

A network-centric approach to SaaS security is problematic for the following reasons:

- **Encryption** – Most SaaS applications use SSL encryption. In order to allow security decisions to be made using full packet inspection forces, organizations need to adopt SSL off-load or decryption. Although this is a security benefit it is often complicated to implement, and also requires organizations to generate, share and trust internal certificates.

- **Threats** – A network-centric security approach is not able to protect against account takeover regardless of its capability. Please refer to the introduction section for a more detailed explanation.

- **Remote Users** – Current trends suggest that users often work remotely or outside of the existing work perimeter. Remote users should be able to access applications over the Internet without their traffic passing through a corporate GW, which a network-centric approach does not permit them to do.

- **Flexibility** – Using network security tools does not allow for flexibility in what and how SaaS apps are accessed. For example new SaaS applications may not have signatures that can be used to identify traffic over the network.

---

A New Approach – API-driven SaaS security

**Overview**
APIs drive most modern IT systems, and cyber security is no exception. Modern security services rely on APIs to interact with SaaS applications and 'inject' security decisions into these platforms. The exposing of low-level controls via API has meant that feature rich cloud-based security platforms are able to interact with the app.

Check Point’s SaaS security platform is driven by APIs and built to meet the security requirements for modern business methodologies.

The benefits of the APIs to SaaS application security

Security professionals will be familiar with the term “CASB”. The CASB label is often used to describe SaaS security platforms: a ‘cloud access security broker’ is primarily concerned with enforcing an access policy, with Check Point’s SaaS being a “CASB 2.0”. CASB 2.0 performs not only CASB services but also implements an advanced threat prevention policy.

CloudGuard SaaS uses public APIs to interact with 3rd Party SaaS solutions and does not intercept any communication between users and SaaS services. Once configured, CG SaaS constantly monitors 3rd party SaaS applications for security events and, based on a defined policy, will either prevent or block various actions and interactions.

Leveraging APIs to interact with SaaS apps and enforce security measures, means that organizations don’t have to concern themselves with legacy network security solutions for SaaS apps. The API approach allows businesses to become more agile, have greater control and move away from network-centric security practices, such as SSL decryption, which no longer have to be applied.
Check Point CloudGuard SaaS security platform

The business drivers for SaaS applications and the security drivers for making their use secure, have now been established. In the previous section the technical and security benefits of moving SaaS security into the application layer using APIs, were explored.

Check Point’s CloudGuard SaaS solution; its components and its security services, will now be examined.

CloudGuard SaaS architecture

CloudGuard SaaS is a cloud-only, API-driven, Threat Prevention and Identity Protection platform that leverages a number of components to perform SaaS application security. This section breaks down the architecture so that the correct configuration is achieved.

The following graphic outlines the key components and their relationships:

1) Agent or Agentless connections options.

   a. Agent-mode – A light-weight agent is installed on all Windows machines allowing user-identity and connection-context to be shared with the CloudGuard SaaS platform. The CloudGuard SaaS is called Guard-ID and is mandatory if identity protection is required.

   b. Agentless-mode – One-time passwords are sent to either the Check Point Sandblast mobile application, or by SMS, and are used to identify users. Agentless-mode also makes use of the connection context, such as source IP, time of connection etc. to relay information to the platform (please see the following section for more details).

2) Identity Providers - CloudGuard SaaS integrates with ADFS using a Check Point agent installed on the ADFS server. CGS can also use cloud based identity providers such as AzureAD (an explanation of the authentication process can be found in the following sections).

3) Service Provider - CloudGuard SaaS essentially acts as the mediator between the Identity Provider and the Service Provider. The user requires this service.
4) **CloudGuard Security Services** – These Check Point services are available to the administrator once the SaaS application has authorized CGS access.

5) **Check Point Security Services including Threat Cloud** – CloudGuard SaaS is deployed into Check Point data centers (currently in the EMEA and USA), maintaining a number of relationships with other Check Point security services, such as Anti-Phishing Indicators, URL Reputation Engines, Check Point Sandblast Cloud, Threat Cloud and more.

6) **CloudGuard SaaS Portal** – All admin is done using a web portal, including setting up the policy, logging etc, and also downloading the required agents.

**Putting identity at the core of SaaS application security**

A key component of a modern security approach is the incorporation of user-identity into the security policy, security platform and the security posture. Label-based or identity-based security is more effective where mobility and agility are business requirements. 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.

The following section will explore the various components and security services that can be leveraged with CloudGuard SaaS.

**Check Point security for SaaS applications**

The security services offered by Check Point SaaS can be split into two categories: Threat Prevention and Identity Protection. Upon configuration, all of these services are available from the Check Point Portal.

**Key controls included:**

<table>
<thead>
<tr>
<th><strong>Check Point Zero-Day Threat Prevention</strong></th>
<th>Uses Check Point SandBlast technology to identify and quarantine files. SandBlast Threat Emulation blocks zero-day attacks using CPU-level sandboxing and SandBlast Threat Extraction, to deliver safe files through file sanitization.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phishing Protection</strong></td>
<td>Stops sophisticated phishing attacks, spear phishing and email spoofing, using AI engines for a higher catch-rate.</td>
</tr>
<tr>
<td><strong>Visibility and Control</strong></td>
<td>Uses Check Point DLP engine to block sensitive data sharing and can enforce encryption, based on policy.</td>
</tr>
<tr>
<td><strong>Identity Protection</strong></td>
<td>Protects corporate accounts from account takeover – an attack vector that Check Point considers the primary threat to organizations adopting SaaS solutions. Some parts of this service require the use of an agent.</td>
</tr>
</tbody>
</table>

**CloudGuard management platform**

The management interface of the platform allows administrators to build the required security policy, download the various CG SaaS agents and configure identity protection policies. Once configured the SaaS portal can display logs and heat-maps to help identify the use of shadow IT. Currently, the management interface is cloud-only.

The screenshot below shows the CG SaaS management portal; please refer to the user manual for more details.
The Check Point CloudGuard SaaS web management portal

CloudGuard SaaS and a zero-trust approach

The CloudGuard SaaS use of identity as a key component of the solution should be considered a part of an organization’s wider adoption of zero-trust architecture. Zero-trust places identity at its core with each user’s identity information being considered before access is granted.

The infographic below illustrates this process:

![Infographic showing the process of zero-trust](image)

Zero-trust people putting identity at the core of access-control

As a security component of a zero-trust architecture Check Point’s SaaS uses an identity-agent to share the user’s ID and connection context with the CloudGuard SaaS. Each request for access is authenticated at the point of the access request, and therefore each session is verified before being established. Connections are not trusted without having first been authenticated.

Using APIs, CloudGuard SaaS shifts security enforcement into the application, which results in less of a need for network layer inspection of SaaS apps.

Designing a CloudGuard SaaS solution

The following steps are aligned with Check Point’s security best practices for configuring CloudGuard SaaS, and focus on management and the agent/agent-less connection options.

Securing SaaS apps using API-driven security

Moving to API-driven security changes the way a security component i.e. CloudGuard SaaS, interacts with both the user and SaaS applications. The infographic below shows the traffic flow for both the agent and agentless connection modes and the Threat Prevention services available.
The SaaS-centric, and advanced view of SaaS security using a cloud architecture methodology

**Agent-Mode**

1) In Agent-mode the Guard-ID agent is installed. The Guard-ID app makes a direct connection to the CloudGuard SaaS platform and shares user-identity and connection-context information. The Guard-ID sends identity and IP information to CloudGuard SaaS via an outbound only SSL connection.

2) CGS is constantly monitoring the SaaS apps, so when the access request is made, the platform will match the request to the Agent.

3) The information shared by the Guard-ID agent allows the platform to restrict the SaaS sign-in and perform an Anomaly detection, such as ‘impossible travel’.

**Agentless-Mode**

4) In Agentless-mode the user makes a direct connection to the SaaS application.

5) Users are sent a one-time-password to either a mobile Guard-ID app, such as a Sandblast mobile, or as an SMS. This password completes the multi-factor authentication.

**Threat Prevention**

6) All CGS services are configured from the portal.

**Designing Identity Protection using Agent-mode**

In order for the CGS platform to collect user-ID and connection context, Guard-ID needs to be installed on the endpoint (please check the latest install guides from the Guard-ID compatibility list).

Guard-ID performs the simple low resource-intensity task of sharing identity information with the Check Point SaaS platform. The agent provides the platform with the user’s context i.e. which AD group they belong to, Geo-location, source IP and device type.

Please note that Guard-ID is required to set-up account takeover protection, and is the Check Point recommended solution, as it gives the widest range of security options.

The Guard-ID agent is a standalone application installed from the download area of the portal.
The Guard-ID agent comes in two deployment options: either as a standalone MSI for deployment on Windows machines, or embedded into the Check Point Mobile Device Security application, that can run on either iOS or Android operating systems.

How the agent works

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

The device sends information about the context (IP, browser, device type, etc) and the CGS compares that to the identity provider. This communication with the device is done in the background and therefore does not affect the user login experience. The method also reduces the risk of second-factor authorization being stolen by a hacker i.e. via malware on the device.
Diagram displaying the ID-Guard application sharing information to the CloudGuard SaaS platform

The above diagram shows the agent scanning a device to determine if it poses any risk (e.g. jailbroken, malware, a man-in-the-middle attack). CGS can therefore block access to an SaaS-based on risk.

Designing Identity Protection using Agentless-mode

Agentless-mode allows organizations to quickly deploy Identity Protection, and not have to initiate on-device agents. Without an Agent, the platform allows two-factor authentication via SMS, network, location, or device-type, to allow basic, but efficient contextual access controls.

It is also possible to allow users who do not have ID-guard installed to access SaaS apps using a one-time password, sent via the ID-Guard app installed on another device or via SMS.

The following scenario is used to explain how the Agentless based install service works:

1) Agentless-mode can be used for some basic but efficient controls which allow the administrator to define rules for specific user groups, networks or IPs, locations and device types i.e. the OS version etc.

2) Agentless-mode provides classic 2FA (one-time passcode sent by SMS) managed centrally for all SaaS.

3) The advanced Agentless-mode can perform anomaly detection on user activity across all SaaS apps. It identifies insecure or suspicious configurations like email forwarding rules, as well as suspicious or conflicting user activity. For example: too many login attempts, unusual login/file-sharing/email sending patterns, etc.

Check Point recommends Agentless-mode as being the quickest mode when onboarding the CloudGuard SaaS service.

Identity security policy configuration
All CloudGuard SaaS services are configured through the cloud portal, including identity services.

Assuming that the CloudGuard SaaS platform has been authorized to interact with the various SaaS applications, the next step will be for the CloudGuard SaaS administrator to create the identity security policy.

To check which applications have been authorized, please refer to the 'Identity Protection – Policy Rules’ page in the CloudGuard SaaS portal.

Based on the corporate SaaS-usage policy the administrator can set the various inspection actions, such as when the organization wants to enforce a policy that would only allow end-users to sign-in from a device that has the ID-Guard agent installed and registered.

**Best practice:** Organizations should adopt a policy that balances its risk appetite with their security requirements.

**Designing Threat Prevention security using CloudGuard SaaS**

This section explores the use of Threat Prevention services within the Check Point SaaS platform.
Each SaaS application that has authorized CloudGuard SaaS to enforce security, will allow the administrator to configure a threat prevention policy per SaaS application, that is under the control of CloudGuard SaaS.

Configuration is done from the “Policy Rules” page:

![Screenshot of the landing page for the threat prevention policy](image)

For each SaaS application, a set of threat prevention options are available from the “Policy Rule” page. It is important to note the various options available and to adjust the policy to an organization’s standards.

![Configuring the threat prevention policy](image)

**Email quarantine**

Check Point recommends that email quarantine is the primary security service that should be enabled for SaaS applications. Quarantining emails reduces the risk of patient-0 infections.

The following screenshot is an example of what this looks like:

![Email quarantine logs showing malicious email’s details](image)
CloudGuard SaaS Use Cases

Use case – Quick deployment required for new SaaS application
An organization has made a decision to migrate their business operations from MS Office to G Suite. Although the administrators have already begun test piloting the changeover, they have not made considerations in regards to securing access to the new platform.

Solution
Check Point recommends the use of Agentless-mode, so that when a user attempts to log into G Suite, the user’s authentication is checked against the corporate ADFS server. Consequently, if the user is legitimate then an OTP is sent to the user’s Sandblast mobile app.

Use case – OneDrive for all corporate users
An organization has decided that sharing documents using FTP or email is neither secure nor scalable with modern file-sizes or when users are off-site. They know that users are currently using their own OneDrive accounts and would like to provide this platform, but using only company accounts.

Solution
The organization asks all users to create a OneDrive account using their corporate email address. Guard-ID is then installed on each machine through the corporate global policy, and authorized through the CloudGuard SaaS portal.

The organization then follows the CloudGuard SaaS Admin Guide and integrates AD into the CloudGuard SaaS platform. Once completed only user devices that have the Guard-ID application installed, are allowed to access their corporate OneDrive accounts and share documents.

Use case – Migrating to Salesforce
An organization is considering to move their sales team onto a Salesforce SaaS platform.

The advantages to the business are:

1) The company doesn’t have to pay for IT professionals and specialists to support an in-house customer management platform.
2) They have chosen Salesforce as it provides them with exactly the platform that they need, because a simpler platform is not available to them in-house.
3) The platform is available to remote workers, which is crucial since most sales people are on the road.

The security administrator raises the following concerns:

1) How do we make sure that only legitimate users access our Salesforce account and what happens if an unauthorized person gains access to all of our sales data?
2) Salesforce itself may be attacked; can we afford to lose our IP data?
3) How do we extend our existing security posture to Salesforce when we don’t have any control over the underlying platform?

Solution
The company investigates how they could use single-sign-on (SSO) with their existing Check Point perimeter GW. However, this will not meet the requirements for advanced security within the actual Salesforce platform. The administrator chooses to deploy Check Point’s SaaS and, within minutes, designs an advanced threat prevention policy.

The following diagram displays the various security services that the administrator can deploy:
Use case – Dropbox; document sharing and DLP

An enterprise needs to share documents internally and would like to allow users to take their work away from the office setting, however, the files are too large and can’t be emailed. This also prevents the employees from collaborating.

Dropbox and OneDrive are a perfect fit for the company but before the security team can allow access to the whole of DropBox and OneDrive through the perimeter firewalls, they have the following concerns:

1) Even if they use application awareness on the egress gateway, they are still opening up access for corporate and private use of these applications.
2) How do they ensure that no malicious files are uploaded and shared with other users?

Solution
Using Guard-ID means that only corporate devices and users would be able to connect to the corporate Dropbox account, as Check Point’s CG SaaS would block other connections. CG SaaS would also monitor the files uploaded; and encrypt any files sent from the Dropbox account.

Use case – Migrating to zero-trust architecture

A company is redesigning its office space and wants all employees to be able to work via laptops, in any part of the building and from home. They are also considering only having raw internet access in the new office space.

The in-house security architect is interested in pursuing a zero-trust architecture for the following reasons:

1) Zero-trust would mean that the company doesn’t have to enforce network security zones in the building. All floors would be able to share a flat network with no internal firewalls.
2) The company wants the new office to be open-planned with no fixed work space, so the user’s ID only, must be able to define what access they are granted.
3) Employees will work from home as well as the office, and require the same level of security.
4) The company wants users to be mobile and use SaaS applications so that they can work from anywhere.

The in-house engineers also make the following security point: if the company wants users to work in an open-plan space, then the security policy needs to be aware of a user’s identity. Using IP addresses in a firewall policy won’t work if people are constantly moving.

Solution
The network security team choose Check Point’s CG SaaS as a CASB 2.0, to be part of their zero-trust architecture for the following reasons:

1) All new users will have laptops on which will be installed a full endpoint suite as well as an agent to share identity with (i.e. the Guard-ID).
2) Users will be able to access the various SaaS applications without any network restrictions, resulting in the same experience as from any company controlled location.
3) Their access to all applications, including SaaS apps, would be consistent with the user’s identity and not their network location.
4) Irrespective of location or app, the corporate security policy will be enforced and the business protected from malicious code and bad-actors inside and out.

Check Point’s CG SaaS allows for some of the network security components between the users and SaaS apps to be removed, users are able to access O365 from any location, and access can be granted based on identity.

Integration & Logging

A key requirement of any security service is to log and add value to the overall security posture. Part of building a security ecosystem is to centralize reporting and events so that they can be correlated with events in other parts of the network. CloudGuard SaaS is able to display records in the events page of the portal and also ship logs to an on-site collector. This section will look at both options.

Portal event page

CloudGuard SaaS is designed to look and feel like any other Check Point management platform, so users of the Check Point Domain Management solution should have no problem navigating this product. The CGS portal presents logs and security events in various templates, much like Check Point’s SmartEvent.
From the “Events” page, the administrator is able to get an initial situation analysis from all authorized accounts, and simply click and drill-down to view more detailed information.

Log cards

Using the same format as Check Point’s SmartLog, security event information is displayed in a log card format. The following graphic displays an example of a connection that has been blocked as the attempt was made from a machine that did not have the Guard-ID agent installed. The reason for the block can clearly be seen alongside information on the location of the threat, and other details.

<table>
<thead>
<tr>
<th>Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Info</td>
</tr>
<tr>
<td>Access Rule Name:</td>
</tr>
<tr>
<td>Time:</td>
</tr>
<tr>
<td>Type:</td>
</tr>
<tr>
<td>Product family:</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Log Server Origin:</td>
</tr>
<tr>
<td>Log Server IP:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application / Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
</tr>
<tr>
<td>User:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action:</td>
</tr>
<tr>
<td>Reason:</td>
</tr>
<tr>
<td>Access Rule Name:</td>
</tr>
</tbody>
</table>

Example of a log card displaying a packet dropped for identity protection violation

CloudGuard SaaS security CheckUP

CloudGuard SaaS allows admins to run a CheckUP report straight from the web portal, which is important for highlighting the security concerns around SaaS security.
SmartEvent integration

Currently, CloudGuard SaaS is able to send logs to an on-premise Check Point Log Manager, which will contribute to an organization's network visibility. CloudGuard SaaS also allows the integration of the SaaS control panel into the on-premise management console (Early-Availability)

The following diagram shows how CG SaaS integrates with the existing Check Point SmartEvent platform to allow threat correlation and increased visibility:

![Diagram of GC SaaS & Data Centre GWs pushing events to a centralized SmartEvent Server](image)

A key benefit of the single-platform architecture is the ability for components to seamlessly integrate, which occurs when deploying ID-Guard alongside a Sandblast agent. Once deployed, these agents will perform a level of posture checking that will protect SaaS from infected endpoints.

Log export

In the event that the logs need to be viewed outside of the platform and the log integration has not been configured, the logs can be exported in a number of formats directly from the portal.
Conclusion

Adopting new technology and ways of operating, such as integrating SaaS platforms into existing systems, is an exciting opportunity for organizations to scale their business and migrate to using modern technology and following security best practices.

We have explored the reasons for why traditional modes of security are inefficient, and how moving security into the SaaS applications is the correct and most advanced approach.

This document also equipped the reader with a rationale as to why an organization should use an API-based security platform, such as Check Point’s CloudGuard SaaS, to properly secure SaaS access and protect their business from threats.

Supporting documentation

The following Check Point documents are provided in support of this guide:

CloudGuard SaaS Getting Started Guide

O365 Access-Control Using Legacy Gateway
https://community.checkpoint.com/t5/Policy-Management/O365-access-filtering-in-R80-10/td-p/13374

CloudGuard SaaS Data-Sheet
https://www.checkpoint.com/products/saas-security/

ID-Guard Agent - Installation and Enrollment
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132233

CloudGuard SaaS Identity Technical Brief Guide

CloudGuard SaaS Threat Prevention Technical Guide

Okta and Office 365: sk134192
http://supportcontent.checkpoint.com/solutions?id=sk134192

Okta and G Suite: sk136993
http://supportcontent.checkpoint.com/solutions?id=sk136993

Microsoft AD FS and Office 365: sk133692 http://supportcontent.checkpoint.com/solutions?id=sk133692

Microsoft AD FS and G Suite: sk132716
http://supportcontent.checkpoint.com/solutions?id=sk132716