# Introduction

<table>
<thead>
<tr>
<th>SaaS Security: Risks and Challenges</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility Silos</td>
<td>5</td>
</tr>
<tr>
<td>Configuration Risk</td>
<td>5</td>
</tr>
<tr>
<td>Loss of Control</td>
<td>5</td>
</tr>
<tr>
<td>Lack of Expertise</td>
<td>5</td>
</tr>
</tbody>
</table>

# CASB Limitations

| Comprehensive Visibility Underpins Security | 5 |

# Building Cloud Detection and Response Capabilities

<table>
<thead>
<tr>
<th>Steps to Build CDR Capabilities</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation</td>
<td>7</td>
</tr>
<tr>
<td>Normalization</td>
<td>7</td>
</tr>
<tr>
<td>Contextual Enrichment</td>
<td>7</td>
</tr>
<tr>
<td>Analytics</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practical Challenges</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proprietary Models of Identity and Access Management</td>
<td>8</td>
</tr>
<tr>
<td>Disparate Logs</td>
<td>8</td>
</tr>
<tr>
<td>Non-Standard API Interfaces</td>
<td>8</td>
</tr>
<tr>
<td>Lack of Security Detection Expertise</td>
<td>8</td>
</tr>
</tbody>
</table>

# An Alternative to DIY: Obsidian CDR

<table>
<thead>
<tr>
<th>What Obsidian Offers</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>9</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>9</td>
</tr>
<tr>
<td>Incident Response</td>
<td>9</td>
</tr>
<tr>
<td>Risk Assessment and Reporting</td>
<td>9</td>
</tr>
</tbody>
</table>

# Conclusion

| 11 |
Introduction

SaaS is everywhere. Software-as-a-service is driving agility and allowing businesses to focus on their core mission better than ever before. Over the past few years, companies have moved critical business email, collaboration, sales, payroll systems, and code repositories to SaaS. According to Gartner, the global market for SaaS is expected to reach $151.1 billion by 2022, accounting for over 42% of public cloud services spend¹. Sensitive data now lives in the cloud, including patient records, employee details, business intelligence, and customer records.

![Saas Market Size ($B)](image)

Figure: SaaS Market Growth Projection (Gartner)

"We have seen two years' worth of digital transformation in two months."

Satya Nadella
CEO of Microsoft, Apr 2020

This embrace of SaaS is outpacing the ability of security teams to adapt to new threats. What’s more, security teams must figure out how to safely enable the use of SaaS without slowing down the business. Doing nothing is not an option, and existing gateway-based approaches to cloud security that focus on blocking access to the cloud are inadequate.

Cloud detection and response (CDR) enables security teams to defend cloud applications and infrastructure from account compromise, insider threat, and access misuse without impacting productivity. The CDR approach is based on consolidated visibility, analytics, and threat monitoring to quickly mitigate risk in the cloud.

This whitepaper serves as a guide for establishing CDR capabilities in your organization.

¹Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020:
SaaS Security: Risks and Challenges

Security in the cloud is a shared responsibility between the cloud provider and its customer. Organizations that assume that the cloud provider does everything and fail to recognize their responsibility get into trouble. In the world of SaaS, the application provider secures the underlying physical infrastructure, network, OS, and application, freeing up customers to focus their efforts on identity and access management (IAM) and data protection. The challenge is that businesses often forget that keeping track of who has access, and what that access is used for, is still their responsibility.

Given the incredible power in the hands of the users of SaaS applications, security teams need to ensure on an ongoing basis that user accounts are protected, and that the cloud applications are being used appropriately. This means being able to detect and mitigate internal and external threats in the SaaS applications:

- Are adversaries trying to break into their SaaS apps?
- Are users doing something inappropriate or dangerous and leaking data?
- Are internal users being malicious?
- Are administrators misconfiguring settings, resulting in a weaker posture?

This is easier said than done. SaaS environments are always on and always accessible. Anyone with valid credentials and appropriate entitlements can get into accounts and access data in SaaS applications from anywhere in the world.
Visibility Silos

SaaS applications implement unique models of access, privileges and roles that govern what users can access and do in the applications. Each application maintains authorization and entitlement management inside the platform. Entitlements are buried deep across many applications, creating visibility silos. Beyond being buried, different levels of granularity and different role names add further work to security teams to understand appropriate access.

Loss of Control

SaaS applications are often managed by application administrators with limited (or no) security expertise. The administrative focus is on ensuring availability, usage, and productivity. These application owners are unable to detect security issues such as account compromise and unintentional leakage of sensitive data, and the application itself might be segmented away from security or even IT. It is hard for security to help secure applications they don’t have access to.

Configuration Risk

Widely used SaaS applications like Salesforce, G Suite, Office 365 and Box offer auditing, logging, encryption, and access control. Organizations are still responsible for configuring these applications appropriately according to security best practices, and ensuring that configurations don’t drift over time. Relying on default values for these settings can be dangerous.

Lack of Expertise

Even the best security teams find it difficult to keep up with security threats and controls across their SaaS applications. Furthermore, the data needed to detect and investigate anomalies and weak configurations is scattered across different places in the cloud applications’ consoles and hard to properly extract.

CASB Limitations

Cloud access security brokers (CASBs) emerged as an early solution for SaaS security. CASBs were built to police cloud access and slow down cloud adoption. CASBs sit between cloud service users and cloud service providers and intercept traffic to enforce security policy. The primary use cases driving CASB adoption are data loss prevention (DLP) and uncovering shadow IT.

As mentioned before, business is embracing SaaS because it allows for better agility and speed, which means users need access to these applications without friction. CASB is yesterday’s attempt to expand the notion of the corporate perimeter, but the perimeter is long dead. Beyond the friction and implementation challenges of CASB, security teams have always needed the ability to detect problems and respond to them, something CASBs have failed to deliver on.

Comprehensive Visibility Underpins Security

Security teams need to be able to quickly detect and investigate suspicious behavior, privilege misuse, data breaches and account compromise incidents with contextual analysis. For SaaS, security teams have questions like:
Who has excessive privileges?
Did employees depart and their accounts are still lingering?
Is an account showing signs of compromise?
Is a legitimate user acting in a suspicious or dangerous way?
Is our logging configured properly in case of an incident response situation?
Are files shared too broadly?
Has a user granted excessive permissions to a third-party application?
Are APIs being abused?

Threat discovery, hunting, incident response, compliance monitoring and audit all require an activity timeline that has been enriched with contextual data. When it comes to incident response and recovery, speed of data retrieval and analytics is key. Having quick, consolidated access to data about users, privileges, and activity that IR teams need to analyze the situation makes a big difference in the outcome and impact.

Comprehensive security is predicated on having continuous, consolidated visibility of access, privilege, and activity. As the adage goes, you can’t secure what you can’t see. Security teams must monitor which users have accounts in each application, which accounts have privileges, and what users and service accounts are doing in the SaaS applications.

This knowledge of how SaaS applications are being used is also essential for security hardening and account hygiene. Teams can start implementing security best practices such as enforcing multi-factor authentication (MFA) and cleaning up unused accounts to reduce the attack surface.

Building Cloud Detection and Response Capabilities

The previous section talked about the importance of having a clean, consolidated view of access, privileges, and activity in SaaS applications. Cloud detection and response (CDR) enables security teams to defend cloud applications by delivering consolidated visibility and data-driven analytics to detect, investigate, and mitigate threats in the cloud. It is a new, comprehensive data driven approach to cloud security.

For organizations that want to build CDR capabilities from the ground up, there are several steps involved.
Steps to Build CDR Capabilities

Aggregation

Most widely used SaaS applications provide API-based access related to accounts, privileges, roles and activity. This data needs to be collected and stored centrally for analysis. The mechanism for collecting the data needs to be robust and handle the scale of your organization, and storing months of data is often beneficial to the security team.

Normalization

A key challenge in SaaS is that each application stores information in different formats. Activity data is at different levels of granularity and uses platform-specific labels and nomenclature. Once the data is aggregated, it should be normalized so that a security analyst or incident responder is able to understand and use the data for detections and investigations without worrying about all the nuances and application-specific differences.

Contextual Enrichment

Data from different applications varies in the amount of context available, so enrichment about identities, locations, and threat intelligence is the next step. Tying a user’s accounts and privileges with their activity in cloud applications can be useful for detecting signs of suspicious activity and insider threat.

Analytics

After centralizing and cleaning the data, the security team needs to be able to interact with it in order to obtain insights and value. This is where questions need to be asked around workflows and use cases. What types of threats is the team looking to detect? How can this accelerate incident response? Will this dataset enrich alerts and events from other parts of the security stack?
Regardless of the answers to these questions, it is likely the team will want to detect unusual login events, inspect spikes in activity related to file downloads or uploads, and audit administrator-level activity. Furthermore, teams will want to see activity as a timeline of events for triage and investigation situations. From a technical perspective, design decisions need to be made on how queries and jobs are executed against the dataset, as well as how analysts and investigators interact and pivot through the data.

**Practical Challenges**

When attempting to establish a significant new capability like CDR, there are several challenges an organization must overcome.

**Proprietary Models of Identity and Access Management**

SaaS applications have unique models of access, privileges and roles that govern what users can access and do in the applications. For example, G Suite offers pre-built administrator roles as well as custom roles with one or more administrator privileges. Salesforce has a user role hierarchy that can be used with sharing settings to determine the levels of access that users have to data, as well as profiles that define how users access objects and data, and what they can do within the application. To understand what a user has access to, you need to understand each application's privilege and access model.

**Disparate Logs**

The format and of content of activity logs also varies a lot across SaaS applications. Even the same SaaS application may provide different logs based on the subscription level. In some applications, you need to explicitly enable logging and the API to access it. For example, before you can access data through the Office 365 Management Activity API, you must enable unified audit logging for your Office 365 organization. You also need to understand how often the data is refreshed and made available via API.

**Non-Standard API Interfaces**

The API interfaces exposed by SaaS applications are not standardized across services, and may change frequently. This complicates data collection because you need to understand how the API interfaces of different SaaS applications are architected, and stay on top of any API version deprecations.

**Lack of Security Detection Expertise**

Even with access to data from SaaS applications, security teams may lack knowledge about common security risks and emerging threats in the cloud. Without an understanding of how attackers may try to get past the defenses and ways that users may abuse applications, it is hard to build reliable detections.
An Alternative to DIY: Obsidian CDR

Cloud detection and response offers powerful benefits for securing SaaS applications, but building and maintaining a system for CDR takes time, effort, and expertise. An alternative to the do-it-yourself method for CDR is to use a third-party cloud detection and response solution like Obsidian that enables security teams to focus on mitigating risks and threats and improving the security of their SaaS applications.

Obsidian Cloud Detection and Response provides continuous visibility and powerful analytics to uncover, investigate, and respond to breaches and insider threats in SaaS applications quickly without slowing down business. Because Obsidian is delivered as SaaS and uses API-based integrations to connect with SaaS applications, organizations can get started in minutes.

Obsidian has built rich API-based integrations with SaaS applications that are most widely used by businesses, including Salesforce, G Suite, Office 365, Box, Dropbox, Zoom, Slack, GitHub, and Workday. Beyond traditional cloud connectors offered by other products that superficially extract data from cloud services, Obsidian’s data infrastructure is built with a deep understanding of how the APIs are structured, what data can be retrieved, and with what frequency. Connecting an application to Obsidian takes just a few minutes, and the data starts coming in almost immediately.
What Obsidian Offers

Visibility
First and foremost, Obsidian provides a clean, consolidated view of users, data, and applications in the cloud for the first time: Who is using SaaS apps? Should they have access? Are they doing the right thing?

- Inventory of users and access
- Role mapping
- Activity monitoring
- Third party authorizations

Threat Defense
Using a unique identity-centric approach, Obsidian generates alerts around breaches and insider threats informed by configuration and behavioral analysis and machine learning. The Obsidian platform detects indicators of anomalous logins, SaaS persistence, data exfiltration, lateral movement, malicious insider activity, OAuth token abuse, and other threats. Threat hunting teams can use the powerful search interface to proactively discover threats.

- Compromise detection
- Suspicious insider discovery
- Threat hunting

Incident Response
Obsidian provides quick searching, filtering, and export capabilities to give incident responders the timelines and context they need. Furthermore, understanding what privileges the users in scope have and what related activity is occurring further helps accelerate scoping and investigation into root cause. Finally, should teams want to stop the bleeding, they can remediate directly inside Obsidian to lock accounts, unshare files, remove mail forwarding rules, and more.

- Activity timeline
- Contextual analysis
- Remediation

Risk Assessment and Reporting
Obsidian generates recommendations to harden the security of cloud applications by removing stale accounts and fixing misconfigurations. Obsidian enables security teams to detect configuration changes that weaken the security posture of applications, and observe when users are given additional privileges. Teams can also use the data to audit and report on compliance adherence.

- Account hygiene
- Configuration drift
- Compliance
Conclusion

As the adoption of cloud applications worldwide grows unabated, security teams are challenged to protect their users and data in third party applications and infrastructure that they don’t control. Attackers are exploiting trust by successfully masquerading as users and service accounts, utilizing legitimate access to resources in the cloud services through credential stuffing, social engineering, spear phishing, brute force password guessing, and other techniques. How do you protect your users, data, and applications in environments you don’t control?

A few years ago, an increasingly mobile workforce stretched the secure network perimeter beyond the datacenter and office to thousands of mobile devices and laptops on WiFi networks at coffee shops, airports, and hotels. Security teams could not see what users were accessing and running on their personal devices – the same devices that they also used to access business email and services. Even in organizations that had antivirus and other preventative tech in place, attackers were using innovative techniques to compromise user endpoints without triggering warnings. The solution to this growing problem was Endpoint Detection and Response (EDR). EDR gave security teams core capabilities that they lacked before: contextual visibility, detection and response. These capabilities empowered security teams to investigate and respond to incidents quickly, giving them a leg up in the fight against the new wave of threats.

Cloud Detection and Response (CDR) capabilities give security professionals the comprehensive visibility they need to detect, investigate, and mitigate threats in the cloud by continuously collecting, normalizing and analyzing large volumes of state and activity data from SaaS applications. Just as EDR addresses the need for ongoing visibility of your endpoints, CDR provides single-pane visibility into what’s happening in cloud environments with full relevant context around access and privileges. CDR is the essential set of capabilities that enable organizations to fully embrace SaaS securely.