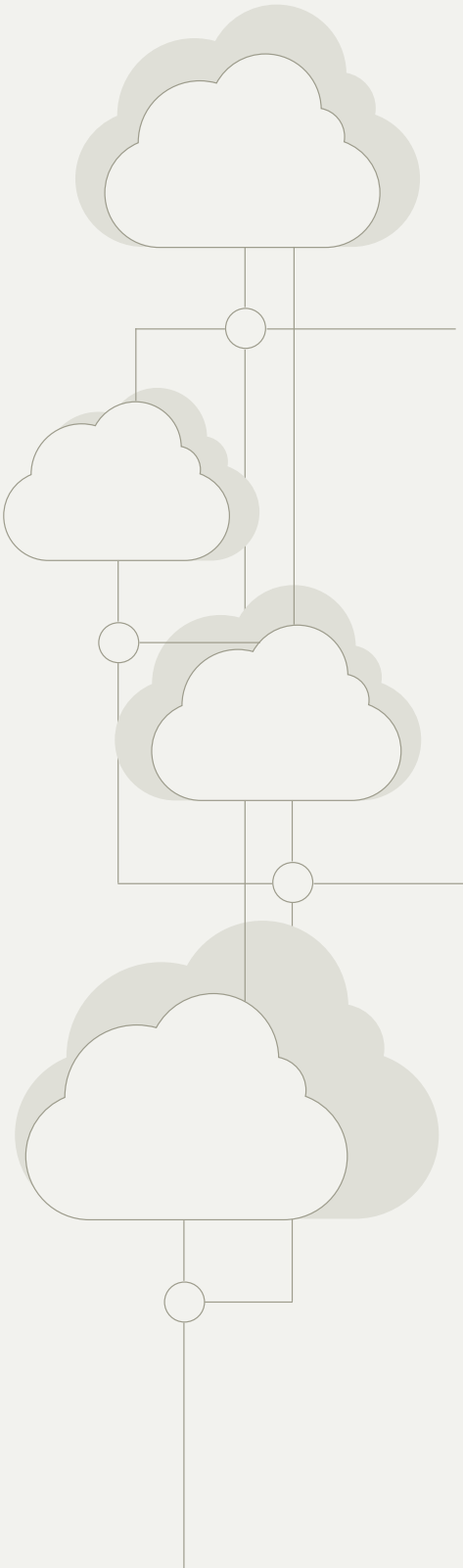
CrowdStrike White Paper

CROWDSTRIKE

HOW TO FIND AND ELIMINATE BLIND SPOTS IN THE CLOUD

Visibility in the cloud is an important but difficult problem to tackle. It differs among cloud providers, and each one has its own positive and negative aspects. This guide covers some of the logging and visibility options that Amazon Web Services (AWS) and Google Cloud Platform (GCP) offer, and highlights their blind spots and how to eliminate them.

KNOW AND UNDERSTAND YOUR VISIBILITY OPTIONS



Cloud providers typically offer some sort of default logging or monitoring at no extra cost, but it is never enough to gain sufficient visibility into what's going on across your organization. They also provide additional paid services that allow you to gain more visibility into your environments for a variety of use cases. Because each cloud provider does things slightly differently, blind spots and the lack of visibility differ across providers.

THE CLOUD CONTROL PLANE

The "control plane" offered by a cloud provider is essentially what handles "cloud operations," or API calls. The control plane must be accessible from anywhere on the internet, and is what allows users to interact with the cloud and the resources in it. For example, API calls made through the AWS Command Line Interface (CLI) are routed through the AWS control plane, allowing you to take actions such as launching a new Amazon Elastic Compute Cloud (EC2) instance. In GCP, the control plane handles things such as calls made through the "gcloud" CLI.

Visibility into which API calls are being made in your environment is incredibly important, which is why many of the free, default logging services are provided. These include CloudTrail Event History in AWS (a 90-day history of API calls made in your account) or something like activity logging in GCP, which provides a broad overview of activity in a project. These default offerings have shortcomings, however — without additional configuration you will miss things.

To monitor the cloud control plane, you need to use built-in services provided by your cloud provider, but those logs should then be exported to an external security information and event management (SIEM) solution, such as Splunk, for further analysis and alerting. These services include things like configuring an AWS CloudTrail trail for every region and for every event type across your organization, or applying GCP audit logs to all supported services at the organization level.

NETWORK AND HOSTS

When it comes to activity within your cloud network or the hosts within that network, there typically is no free default offering to gain visibility. There may be default logging on your hosts, such as bash history, but there is nothing aggregating those logs and providing you access to all of your hosts through a unified interface.

Many built-in and third-party offerings are available to gain visibility into activity in your network and on your hosts. The CrowdStrike Falcon® platform is one option for host-based monitoring and visibility that allows you to detect and prevent threats in real time. Other offerings, such as AWS VPC (Virtual Private Cloud) Traffic Mirroring or GCP Packet Mirroring, can help with full packet capture within your cloud network. VPC flow logs are another useful tool for network visibility, and offerings such as AWS GuardDuty can monitor those flow logs, as well as DNS logs and CloudTrail logs, to detect threats and unusual activity within your environment.

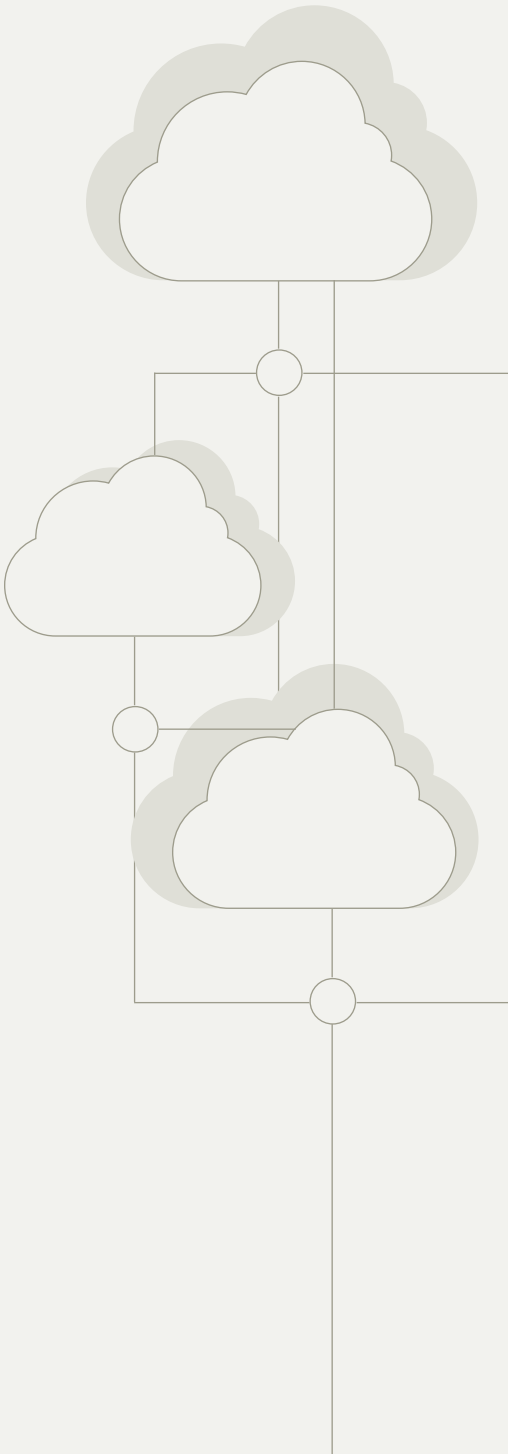
PAIN POINTS AND BLIND SPOTS

No matter which monitoring and visibility options are available, even if you utilize all of your cloud provider's built-in services (and even some third-party services), there are likely pieces missing from the puzzle.

DATA-LEVEL EVENTS

Data-level events differ from control plane or management events because they are actions performed on specific data rather than on a cloud resource. For example, AWS Simple Storage Service (S3) data events log activity for objects in an S3 bucket, providing insight into who's interacting with what objects. Without additional configuration (and therefore additional cost), these event types are not logged. Some services offer data-level event logging, such as S3 bucket access logs, but others, such as AWS EBS Direct APIs, do not.

To ensure you are not losing insight into data-level events, you should enable them where possible. Where it is not possible, we recommend that you deny all users access to those data-level APIs.



UNDOCUMENTED APIS

Every cloud provider publishes documentation for their supported APIs, which allows you to identify what is possible in their specific cloud. The problem is there are often undocumented APIs supported by each cloud provider that may be exposed when they should not be. Often these undocumented APIs are used to enhance the user experience, such as providing a good UX through the web console the provider supplies. Because these are undocumented and generally not for direct access, they are not logged where other documented APIs are logged. This lack of logging could allow an attacker to perform certain actions in your environment with no way for you to know they did.

To prevent undocumented APIs from being used maliciously in your environment, it is important to grant permissions on a granular level. That is, don't grant permissions using wildcards (such as using a "*" in AWS), don't use "managed" permissions sets (as they are often overly permissive), and regularly review the permissions you grant your users to ensure they are properly restricted. By allowing listing permissions on a granular level, you can avoid much of the risk that undocumented APIs expose.

PRE-GA SERVICES

Another potential blind spot in the cloud is pre-GA (general availability) services. This could include alpha, beta, gamma, pre-production or similar services. Such services are often blocked from the public and only permit access to listed users, but many times they are made available for public use while still in pre-GA status.

One example of how to access pre-GA services are the commands available through the "beta" and "alpha" groups of the "gcloud" CLI, which can be accessed with "gcloud beta <service>" and "gcloud alpha <service>," respectively. Just because they are pre-GA doesn't mean they are not logged, but this is where you may encounter services that do not yet support logging and have a potential for abuse. You can prevent access to many of these beta

and alpha services in GCP by denying users access to enabling new APIs in their projects and only providing them access to a list of trusted services.

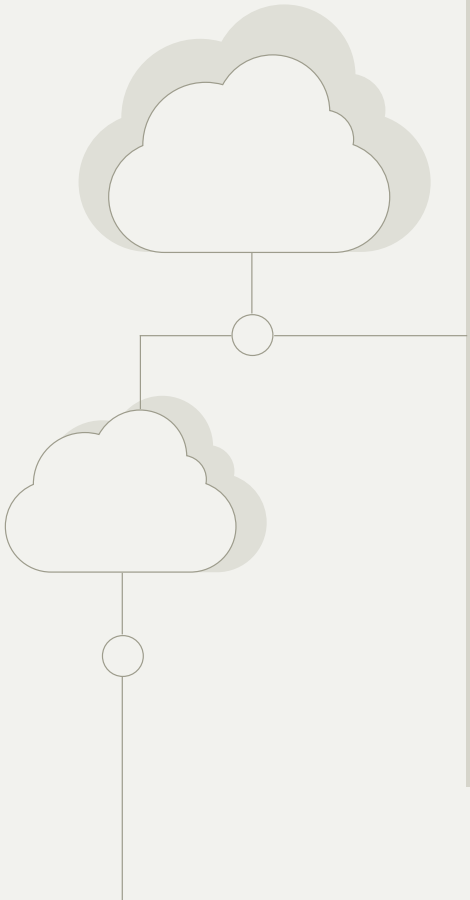
Permissions must be set at a granular level so they only grant access to necessary services and APIs. These risks often arise when wildcards or managed permission sets are applied in an environment, where you can't be 100% sure of every service and action you have granted to your user. When setting the permissions granularly, you can ensure that nothing unexpected can be accessed by your users.

THE PRINCIPLE OF LEAST PRIVILEGE

Without taking advantage of logging and visibility offerings provided by cloud providers, you can quickly lose insight into what's actually going on in your environment. Visibility gaps can still exist even with the proper services enabled, as we discussed with data-level events, undocumented APIs and pre-GA services, so it's necessary to follow the principle of least privilege to avoid granting access to services and APIs that escape your monitoring capabilities.

It may seem like the cloud provider's responsibility to not release undocumented APIs or pre-GA services, but until they do it is your responsibility to delegate permissions and access in such a way that these APIs do not expose your environment to risk.

For more information about how CrowdStrike Cloud Security solutions can help increase visibility and control of cloud resources, prevent misconfigurations, protect workloads and ensure compliance, visit **www.crowdstrike.com**.



ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Request a demo

Learn more at **www.crowdstrike.com**