WHITE PAPER

Operational Security Overview

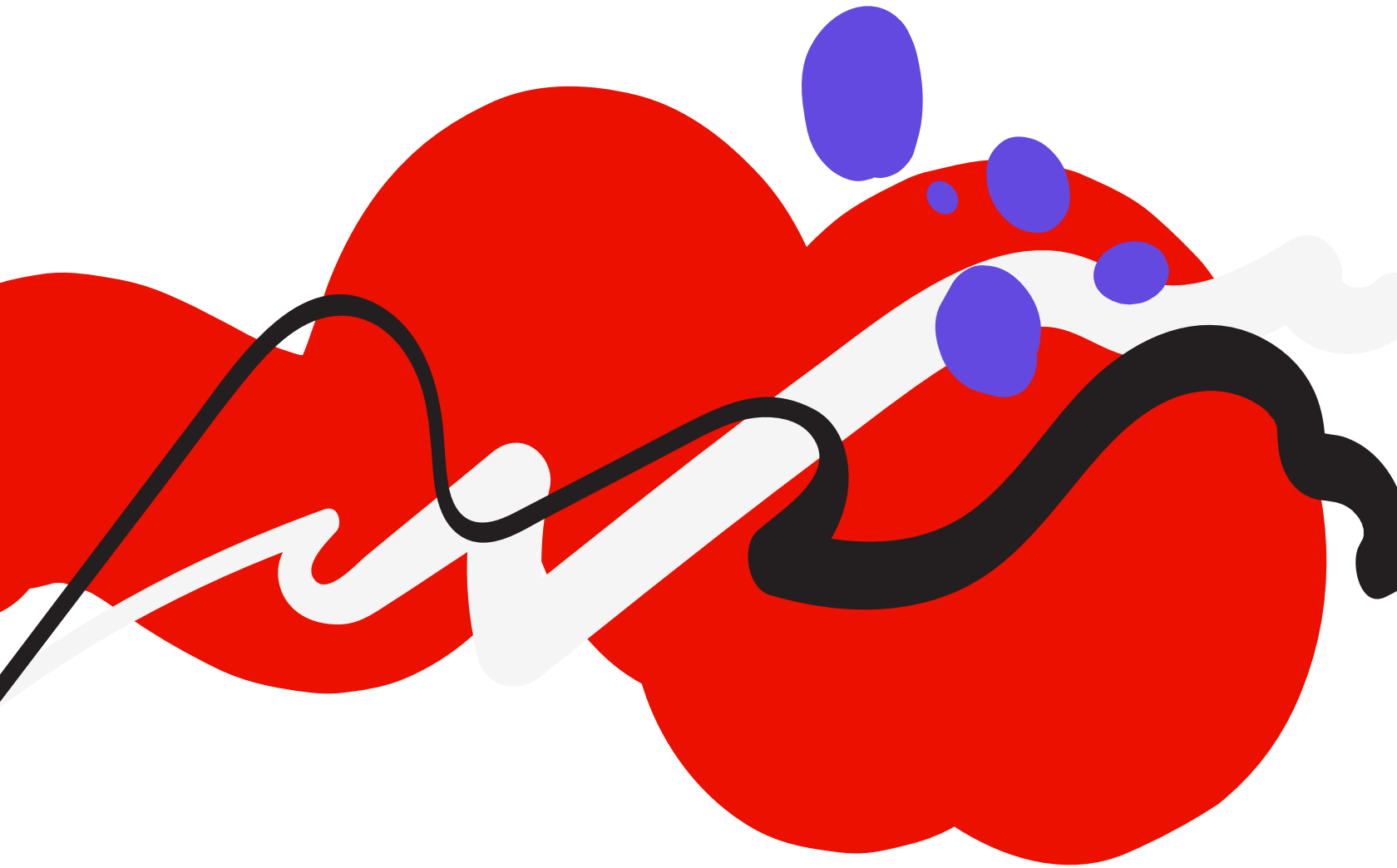
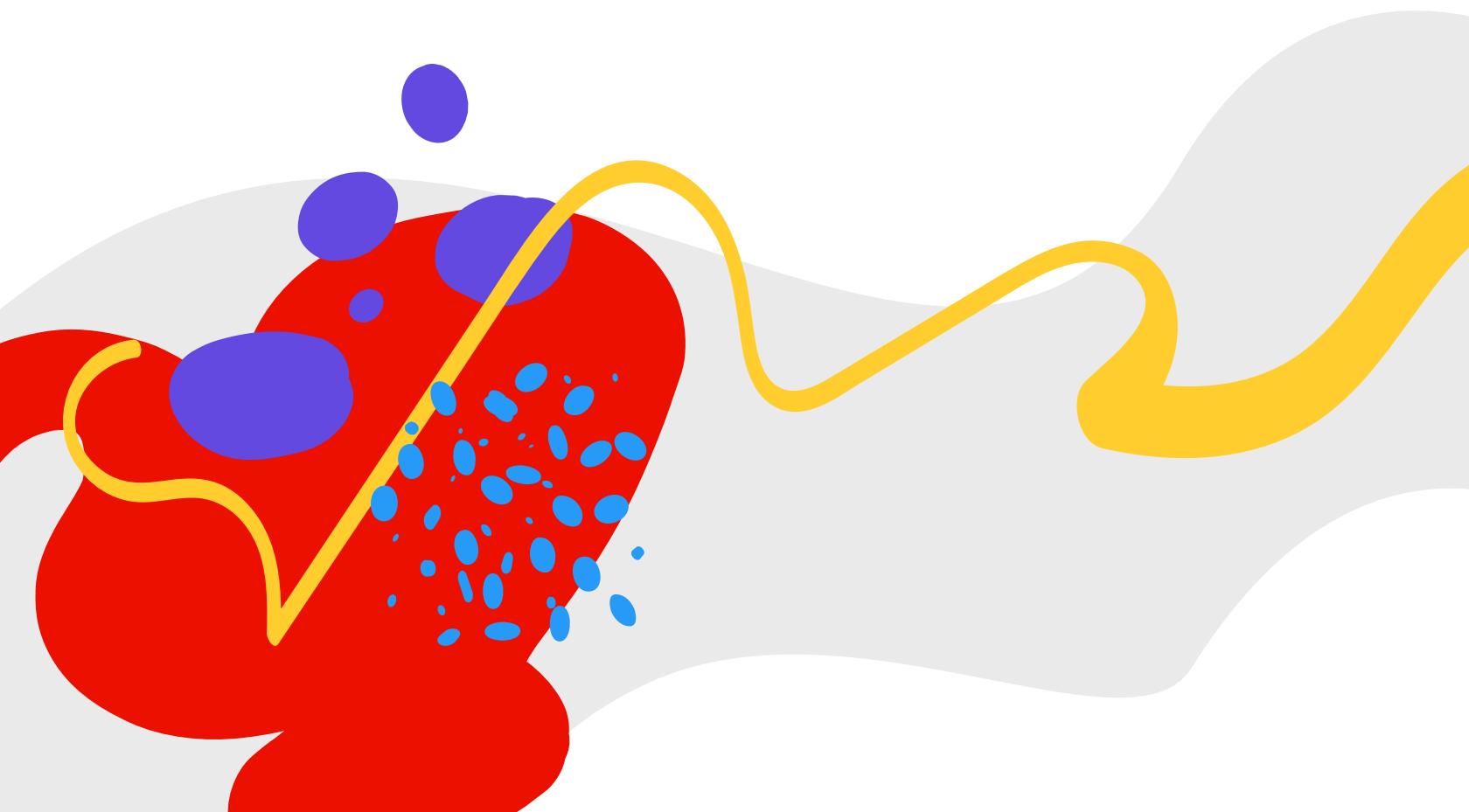


Table of Contents



Introduction

With a cloud footprint that includes public and private clouds across different providers, the Adobe multi-cloud strategy requires consistent and repeatable guardrails that are readily available to our product and service teams. Created by the dedicated Adobe Operational Security organization, the Adobe Operational Security Stack (OSS) is a consolidated set of tools to help ensure that Adobe products and services are designed with security best practices in mind. The Adobe OSS helps product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

This white paper describes the Adobe secure cloud operations strategy, which focuses on securing cloud resources at scale and helping provide for the safety and security of customer applications and data within our continually evolving cloud infrastructure operations.

The Adobe Secure Cloud Operations Strategy

By building security into the core of our cloud processes, Adobe proactively helps prevent potential issues that may occur within the complex security landscape. As our cloud footprint continues to grow and involve multi-cloud environments and technologies, such as containers and orchestrators, standard configurations and security through automation help us reduce human error and provide assurance to our customers that multiple layers throughout the infrastructure are protected from potential weaknesses. Scaling security through automation along with regular monitoring of our security posture and quarterly compliance reviews help Adobe to detect security drift and other issues before they become critical.

A significant part of our next-generation security automation and tooling focuses on "securing the public cloud by default" through enhanced policies and controls that help reinforce our existing cloud protections. With the ability to detect security gaps before and during provisioning, Adobe helps enable the security of our cloud resources before they are even deployed in a production environment.

The Adobe Operational Security Stack (OSS)

Taking the company's multi-cloud security needs into account, the Adobe OSS is based on two (2) fundamental principles: standardization and prevention. To that end, the Adobe Operational Security Stack includes a standardized set of continuous monitoring and workflow solutions that allows service teams to design their private and public cloud environments with security in mind — from the ground up — and helps proactively prevent security risks.

The Adobe OSS operates on a variety of cloud resources, provides security at scale, offers standardized capabilities for the entire organization, and helps ensure security visibility into operational environments for Adobe security, audit, and compliance teams. By adopting the same set of tools and processes across our product and service teams, Adobe can help both prevent security errors and enable applications to adapt to security solutions without needing to reinvent the wheel.

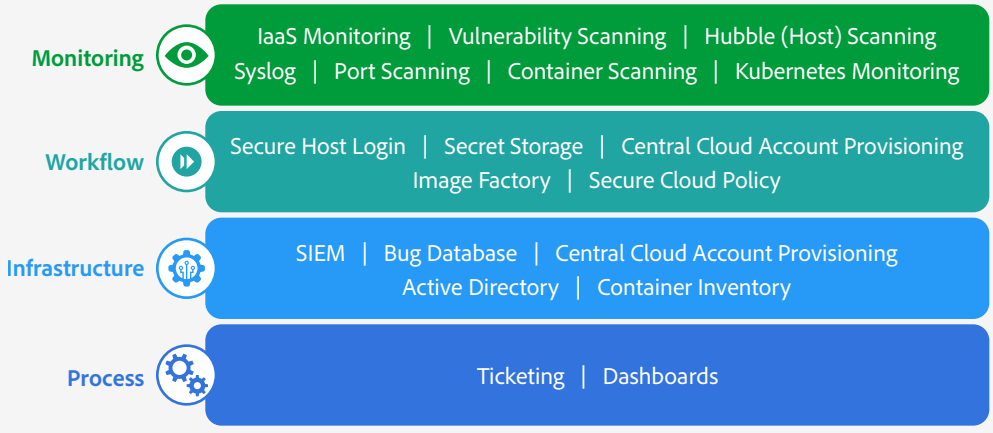


Figure 1: The Adobe Operational Security Stack

With a goal of making the secure choice the default choice, the Adobe OSS includes four (4) distinct layers, each of which includes a broad range of common tools and services that can be leveraged by any Adobe product team and provides them with a way to stay on top of fast-changing security best practices.

Monitoring

The monitoring layer includes tools to help ingest log and configuration data across all Adobe cloud environments and regions into a central data warehouse. Once ingested, the Adobe security, compliance, and Security Operations Center (SOC) teams can analyze this data to help measure security drift and detect security gaps. These gaps can be found either by manual review of the data by the security team or through automated security detection tools.

Additionally, Adobe regularly conducts scans on hosts and containers across our cloud environments, from an application as well as a network standpoint, in order to detect vulnerabilities. Vulnerabilities discovered through these scans and penetration tests are documented, assessed, prioritized, and assigned to a remediation plan, if necessary.

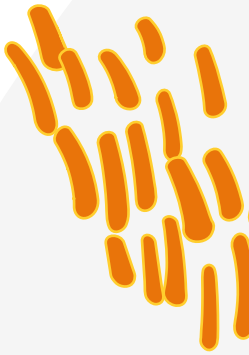
The following list describes the tools included in the monitoring layer of the Adobe OSS:

- **IaaS monitoring** — MAVLink, a public cloud data collection tool developed in-house by Adobe, queries Amazon Web Services (AWS) and Microsoft Azure (Azure) APIs for logging and environment configuration data and then ingests this information into a Splunk data warehouse. By deploying MAVLink, developers enable Adobe Security Engineering to view the state of the public cloud at a single point in time from a security standpoint. Additionally, Adobe internal audit and compliance teams use this data to determine compliance with many elements of both the AWS and the Azure security standards.
- **Vulnerability scanning** — Periodically scan Adobe data centers and our comprehensive cloud footprint, pinpointing potential vulnerabilities before they arise.
- **Host scanning** — Using Hubble, a modular security compliance framework developed by Adobe, written in Python, and open-sourced to the external community, Adobe conducts the following three (3) activities:
  - Auditing – Checks host systems against policy files based on the Center for Internet Security (CIS) standard
  - Querying – Collects system information via osquery to detect intrusions
  - File integrity monitoring – Tracks file changes in key directories
- **Syslog** — Collects system logs and event messages from different machines and stores them in Splunk for monitoring and review.
- **Port scanning** — Scans hundreds of thousands of Adobe IP addresses, reducing the window of time between initial exposure and remediation. Using the nmap scanning pipeline, teams can quickly detect perimeter port exposure.

- **Container scanning** — Detects known common vulnerabilities and exposures (CVEs) in onboarded container images at build and after deployment. Regular scans are uploaded to Splunk and generate a Jira ticket for issues requiring remediation.
- **Kubernetes monitoring** — Provides visibility into Kubernetes orchestration environments by querying the Kubernetes API server to get a complete snapshot of the cluster. Using Faros, an internal application designed to monitor Kubernetes clusters for security, Adobe Security Engineering can pull a Kubernetes configuration snapshot at a predefined time, using custom assessors with read-only access to determine any security gaps.

Workflow

The workflow layer of the Adobe OSS is composed of tools that help product developers and engineers deliver the end-to-end security of Adobe products and the company's infrastructure. Enabling our teams to efficiently implement security policies, the tools available in the workflow layer make it easy to perform secure operations, including:



- **Enabling secure host login** — The Adobe OSS centrally manages credentials and access to cloud objects using the principle of least privilege. In addition, multi-factor authentication (MFA) can be used for l access requirements and provides full logging and auditing of l administrative sessions.
- **Storing sensitive information and managing secrets** — Adobe uses a leading third-party secure vault product to secure, store, and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- **Provisioning new cloud accounts** — To streamline management and governance of the Adobe cloud footprint, product teams can create and manage cloud accounts through a central service, which also allows the Adobe governance team to more easily manage billing of cloud accounts as well as to centrally apply security and operational policies.

Providing a single source of truth for cloud account metadata is critical in order to understand the size and security posture of our cloud footprint, and centralized account provisioning enables us to understand the correct ownership of accounts and intended purpose for which accounts are used.

- **Providing hardened operating system images** — Adobe strives for a secure, out-of-the-box experience for all our product teams by providing centralized hardened images that adhere to the Center for Internet Security (CIS) benchmarks and apply both CIS-approved security updates and the latest security tools. Stored in Image Factory, an internally developed application, images are scanned by our internal security tools before they are released for use to our engineering teams. In addition, product teams can use the Image Factory API to integrate the latest machine image directly into their build pipeline.

- **Securing the public cloud by default** — Adobe uses secure cloud policy to provide an additional layer of security that helps us scale and reduce the cloud attack surface. Cloud-native services, such as Azure Policy, AWS Service Control Policies and AWS Config Rules, proactively enforce security policy and resource compliance requirements across our public cloud accounts. These services help prevent the creation of cloud resources that could violate security controls and reduce the time required to resolve security tickets. In addition, these services bring automated decision-making and remediation into the security process where they are most needed, allowing our teams to focus on developing ways to strengthen our security posture rather than on mundane maintenance issues.

Infrastructure

Regularly refreshed rich metadata is a key component of the infrastructure layer in the Adobe Operational Security Stack, which provides the foundation for the monitoring and workflow layers. The Adobe OSS uses this metadata to assign discovered security gaps to the appropriate team that owns the offending cloud resource.

Other tools within the Infrastructure layer of the Adobe OSS include:

Security Information and Event Management (SIEM) — Using Splunk to search, monitor, visualize, and analyze the aggregated log data collected in the monitoring layer, the Adobe Security Operations Center (SOC) conducts deeper analysis on security-related events and incidents.

Bug Database — To help provide a single source for attribution, Adobe logs bugs in JIRA, using its automated ticketing for accountability and tracking.

Identity and Access Management (IAM) — Adobe uses Microsoft Active Directory in combination with other standard tooling to manage authentication.

Cloud Metadata — Adobe tracks and audits metadata for all public cloud accounts and audits this data on a quarterly basis to help secure the accounts and ensure policy governance. The cloud metadata portal helps product and security teams onboard new cloud accounts according to prescribed workflows. In addition, teams can access the metadata in the data warehouse to filter out noise, eliminate false positives, and help enable the proper prioritization of critical threats.

Container Inventory — A rich set of metadata for the entire container ecosystem at Adobe that helps our product teams gain deeper insights into container orchestration. In addition, teams can use the container metadata to monitor and visualize metrics as well as to gain complete visibility into any Kubernetes environment.

Process

The process layer serves to help Adobe continuously improve our security posture and ensure that we implement security best practices. Data from the three other layers in the OSS is stored in the centralized data warehouse and ingested by JIRA (for security gap mitigation and resolution), by dashboards (for management visibility), and by other internal partners.

We use Key Performance Indicators (KPIs) to measure how well the Adobe OSS is effectively deployed across the company and to identify outliers. Automated JIRA ticketing notifies product teams when their service deviates from a hardened security state and helps our engineering and operations teams meet several control domains in the Adobe Common Controls Framework (CCF), such as configuration management and asset management.

The Adobe OSS in Action

Leveraging automation, system-level controls, and standardization, each layer of the Adobe Operational Security Stack works in concert with the others to help provide for the security of our deployed cloud resources.

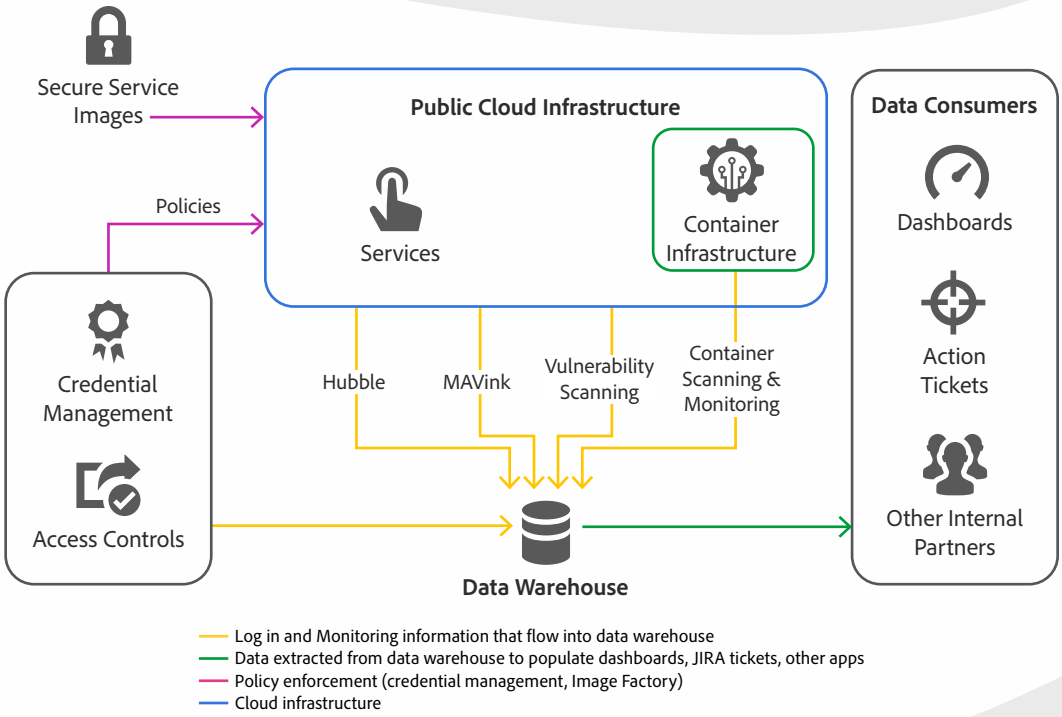


Figure 2: The Adobe OSS Data Flow

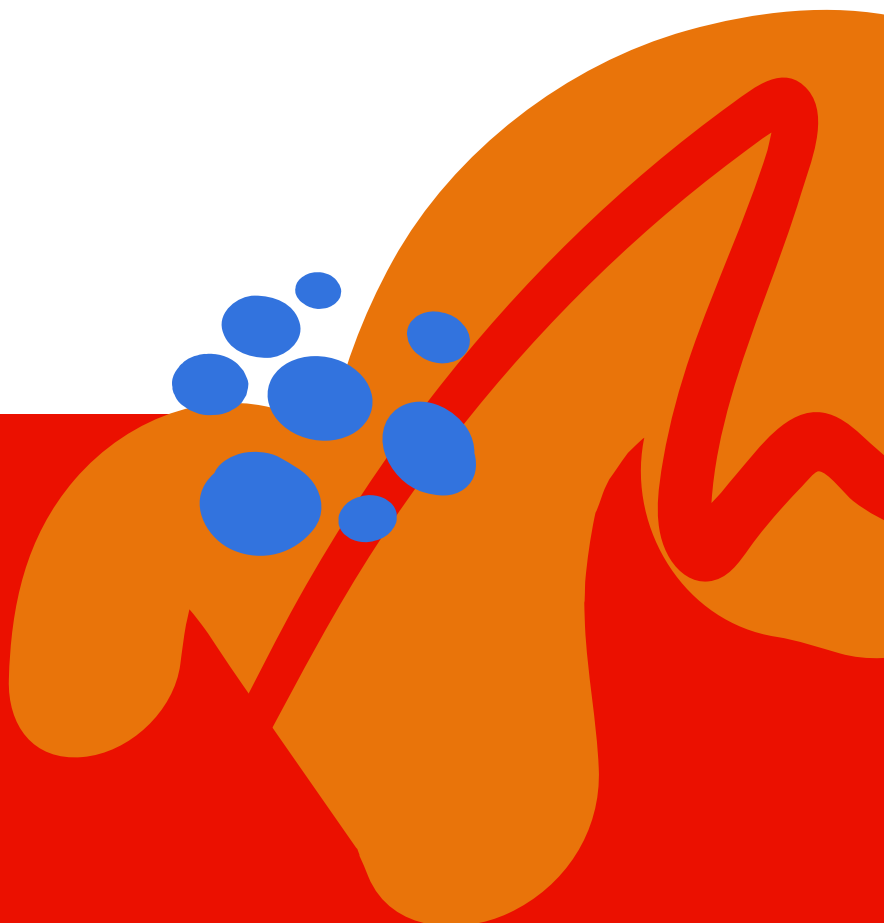
Credentials and access control tooling help enable uniform enforcement of identity and access management policies across our managed cloud services and we store logging information about user activities in our data warehouse We also help ensure teams create, deploy, and manage their services using hardened OS images with our Image Factory infrastructure.

Once services are deployed, monitoring tools continually observe cloud instances — whether applications are deployed as cloud services or in our container platform — and send logs and other relevant information to the central data warehouse. Dashboards, JIRA tickets, and other applications throughout the company extract data from the central warehouse to populate their user-facing applications.

Conclusion

The Adobe Operational Security Stack provides our product and service teams with consistent and repeatable guardrails to help ensure Adobe customer offerings are built with security in mind and adhere to our compliance, privacy, and other governance frameworks. Security automation along with continuous monitoring of our security posture through reports, dashboards, and quarterly compliance reviews helps Adobe proactively prevent security risks and maintain the end-to-end security of both our products and the company's infrastructure.

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.



Adobe