WHITEPAPER

Adobe Enterprise Security Overview

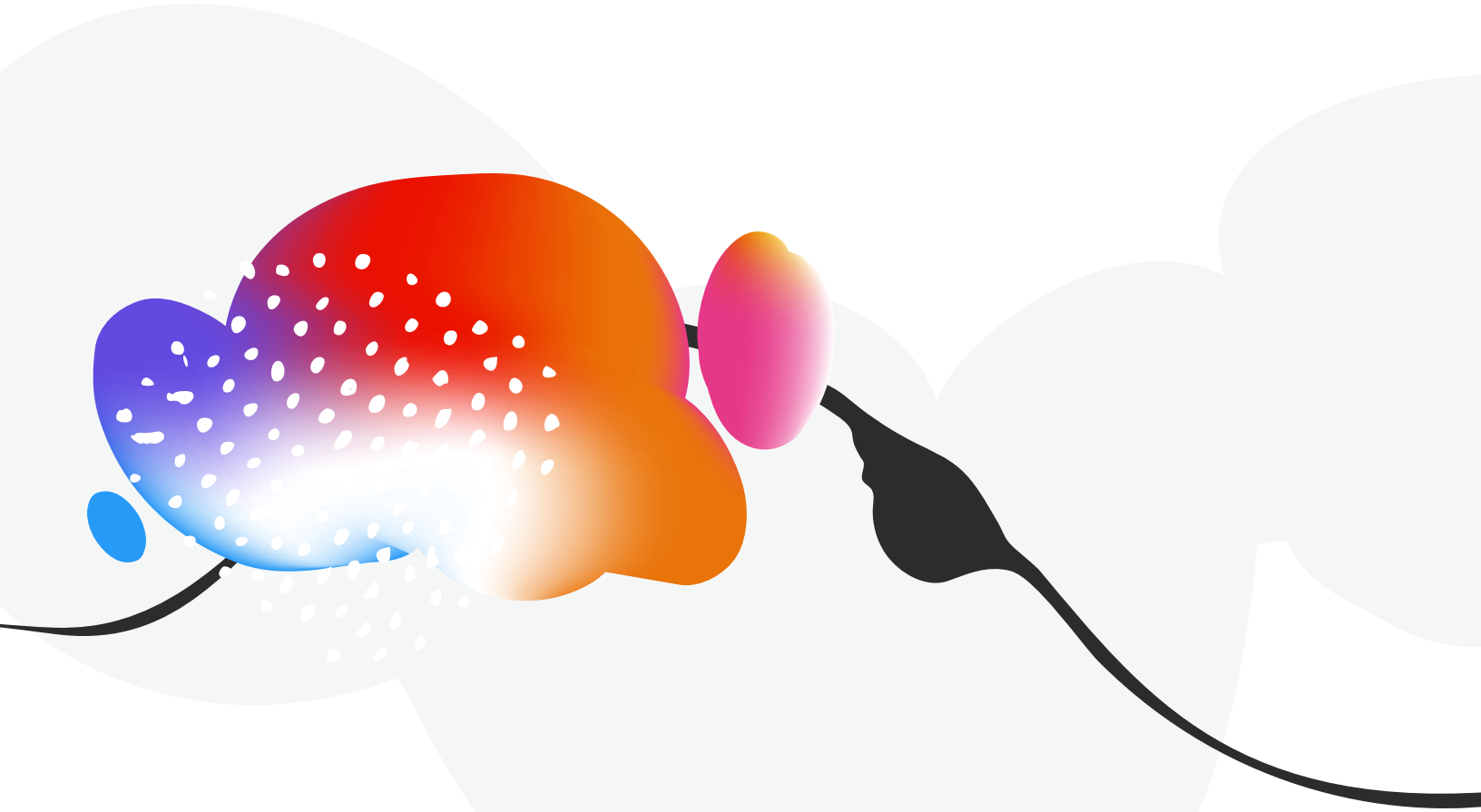
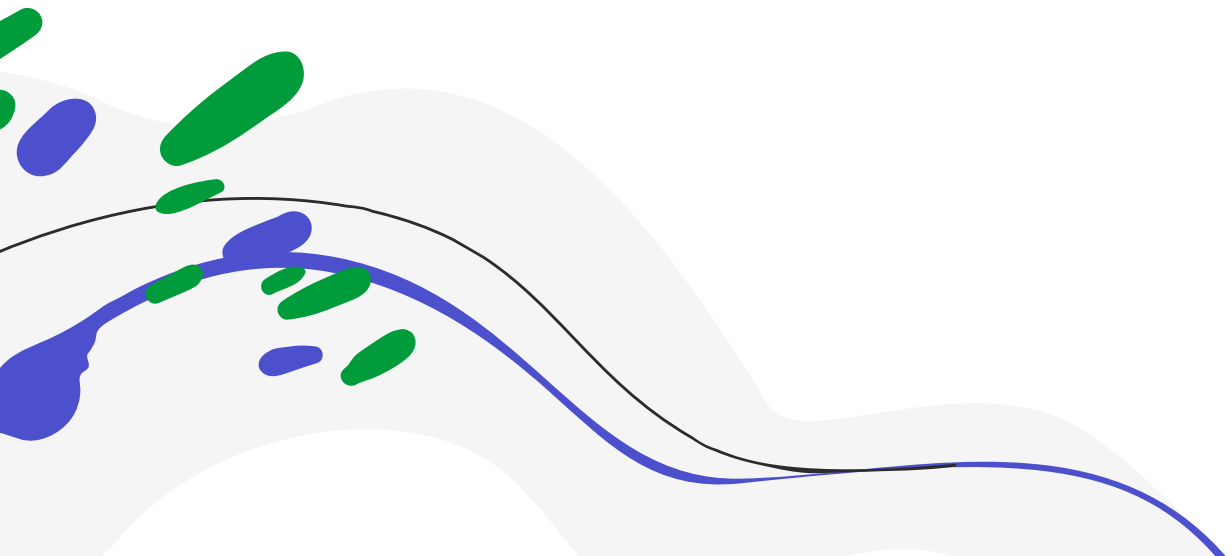


Table of Contents



Adobe Security

With a global corporate presence and a hybrid workforce of thousands, enterprise security is a critical component of Adobe's overall security story. Our enterprise security team focuses on deploying robust security for our internal networks and systems, physical corporate locations, employees, data, and third-party vendors in our supply chain.

This white paper describes Adobe's enterprise security strategy as well as the programs, processes, policies, and tools we implement to reduce risk across Adobe, keep our intellectual property and other digital assets secure, protect employee and customer data, and improve our overall corporate security posture.

The Adobe Zero-Trust Enterprise Network (ZEN) Platform

The Adobe Zero-Trust Enterprise Network (ZEN) platform provides the foundation for our enterprise security strategy, requiring users to be authenticated, authorized, and continuously validated for security configuration and posture prior to receiving or maintaining access to applications and data. A cloud-based application, the Adobe ZEN platform creates easier, more transparent access to resources by eliminating the need for multiple authentications and re-entry of usernames and passwords while also helping improve Adobe's network security.

Using certificate-based technology to enable access to the Adobe corporate network and resources based on the posture of the requesting user and device, the Adobe ZEN platform enables users to access applications and other resources without the use of a VPN (virtual private network) to connect to Adobe's corporate network.

With the Adobe ZEN platform, employees using trusted devices gain a more seamless experience, while application and service owners can be confident that only trusted devices are able to access these resources. The Adobe ZEN platform also helps restrict lateral movement within the enterprise network, further ensuring that only those individuals with explicit authorization can access resources and potentially sensitive data.

Adobe ZEN Platform Architecture

The Adobe ZEN platform architecture includes the following key functions:

- **Access Policy Engine** — Acts as the central authorization service and renders access based on both the device and the user posture.
- **Device Management** — Establishes the authorization chain by securely generating and distributing ZEN certificates to each managed device and configuring the device for the ZEN environment. Managed devices automatically receive a unique ZEN certificate that is used for authentication, eliminating the need for employees to provide their username and password multiple times to access resources. The device management solution is also responsible for certificate lifecycle management, renewing or reissuing certificate on an annual basis to maintain a solid trust chain.
- **Authentication and Posture Check** — Conducts a posture check on each device attempting to access applications or services on the enterprise network and enables web applications to permit resource access using certificate-based authentication.
- **Access Proxy** — Permits users with devices containing a ZEN certificate to access on-premises applications from outside the corporate network without VPN. The access proxy forces encrypted communications, authenticates the user, and enforces control checks to the Access Policy Engine, helping to ensure only authorized devices can reach an internal application.
- **Identity and Access Management (IAM)** — Authenticates users based on their credentials (first and second factor) and authorizes access to an application by initiating a control check to the Access Policy Engine.

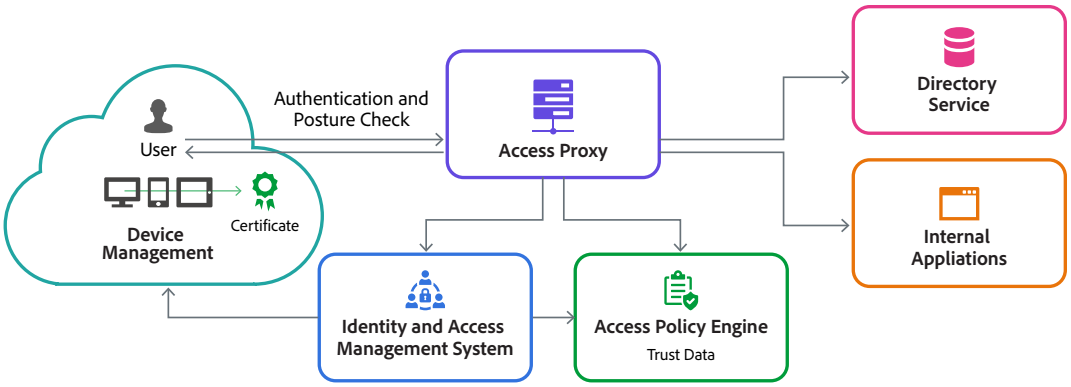


Figure 1: The Adobe ZEN platform architecture

ZEN Device and User Authentication

Upon enrollment in the device management service (DMS), each device automatically receives the following:

- ZEN certificate — Using managed PKI, the DMS automatically and silently pushes a ZEN certificate that includes both the device's unique identifier (UDID) and that of the user associated with the device (UID). This certificate conducts a device posture check with the DMS and authenticates the user each time they access the enterprise network.
- ZEN configuration settings — In addition to the ZEN certificate, the DMS automatically pushes configuration settings that ensure the ZEN certificate is automatically selected when authenticating to a ZEN-enabled platform. If the ZEN configuration was not deployed to a device, the user receives a certificate pop-up window asking them to select a certificate from their machine certificate store.

Once configured, the ZEN certificate is presented to the access proxy and IAM functions. If authorized, the user can access internal applications from outside the Adobe corporate network.

Adobe Enterprise Security Core Controls

Adobe's enterprise security controls are driven by the Adobe Common Controls Framework (CCF). The CCF is a comprehensive set of security activities and compliance control requirements that has been aggregated, correlated, and rationalized from an array of industry information security standards and is applied to help secure both the Adobe corporate infrastructure as well as our applications and services.

The following sections describe the current controls in each area covered in the CCF, including those for our network infrastructure, data protection, user security, and employee and facility security.

Network Infrastructure Controls

Endpoint Detection and Response

Adobe deploys the CrowdStrike Falcon agent on every system at Adobe. The agent is automatically installed on desktops and laptops enrolled in the device management program. Falcon collects information—such as binaries, devices, files, systems, and software inventory—on every endpoint to effectively detect, protect, and mitigate against malicious behavior.

Intrusion Detection

Adobe deploys Intrusion Detection System (IDS) sensors at critical points in the network to alert our security team of any unauthorized attempts to access the network. We validate these alerts and inspect the network for any sign of compromise, regularly updating all sensors and monitoring them for proper operation.

Email Controls

Adobe scans all inbound corporate email communications for spam, malware, phishing, including user and domain impersonation, and scans all outbound email messages for malware and spam. We use an enterprise-wide, managed solution to scan for known threats.

External email addresses delivered to Adobe are identified by a badge or tag with the word "EXTERNAL." This tag indicates the email originated from domains not owned or managed by Adobe and alerts the recipient to use extreme caution before clicking on links or opening attachments with external tags.

The Adobe.com domain is compliant with DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), and Sender Policy Framework (SPF), and uses secure protocols when available.

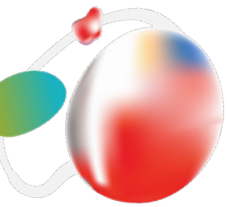
Firewalls (Secure Network Routing)

Adobe only allows inbound connections from the internet to permitted ports. Outbound traffic is only allowed on HTTPS, and network address translation (NAT) masks the true IP address of a server from the client connecting to it.

We review firewall rules on a regular basis and make changes as needed to better manage threats and overall risk.

Adobe has also configured network policy enforcement points (PEP) within its production and corporate networks. All inbound and outbound traffic from the Adobe corporate network and the production infrastructure passes through a PEP, which consists of Adobe firewalls and cloud service provider (CSP) security groups. PEPs are configured based upon the Adobe Perimeter Security Policy requirements, which also define the approved allowlist of TCP connections.

Servers that host Adobe-managed applications for customer and/or public use (e.g., web servers) and are accessed from the internet reside in a DMZ in order to provide additional protection for the Adobe internal network.



Non-routable, Private Addressing

Adobe stores all customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with NAT and internal network policies, prevent servers on the network from being directly accessed from the internet, reducing potential attack vectors.

Distributed Denial-of-Service Protection

Adobe employs a defense-in-depth strategy for Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) protection, using third-party mitigation services with more than one terabyte per second (1 Tbps) scrubbing capacity. In the event of a DDoS attack, Adobe Security alerts network engineering. The on-call network engineer evaluates the attack volume, and if the attack does not include enough volume to disrupt service, we continue to monitor the attack until resolution. Alternatively, if the attack is significant enough to be impactful to data center operations, a pre-scripted change routes the attack traffic through our mitigation service. Once that change is complete, the mitigation service provider filters the traffic and delivers clean customer traffic to our data center.

Data Protection Controls

Customer Data Confidentiality

All customer data is considered confidential and subject to Adobe's internal Data Classification and Handling standard. Each data classification has specific protection and handling requirements. If data falls into multiple classifications, it must be protected according to its most sensitive classification. Customers are responsible for the data governance, including classification, of data they provide to Adobe.

Adobe does not use or share the information collected on behalf of a customer except as may be allowed in our agreement with the customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy. Adobe sub-processors have no access to customer data.

Logical Access

The Adobe Logical Access Policy applies to all environments that collect, store, process, transmit, or dispose of data. Role-based access control (RBAC) follows the principle of least privilege, which states that permissions are only granted to allow the performance of specific job functions. We review and document access rights for both privileged and non-privileged users on a quarterly basis.

Adobe implements a defined and managed logical information access process that addresses access authorization, provisioning, modification, and revocation. All logical access mechanisms must positively authenticate and authorize account types before access is granted to Adobe information resources and must use methods to ensure that authentication credentials are protected in storage and in transit.

Encryption Key Management

Adobe maintains key management and data encryption standards that define our processes for protecting logical access keys from disclosure and misuse. Our key management standard also helps ensure that the encryption technologies we use meet Adobe's published standards. Requirements for securing logical access keys and restricting certain functions — including key generation, key distribution, and key storage only to authorized personnel — are covered in this standard.[1]

Data Loss Protection

Rather than use one specific enterprise data loss protection (DLP) solution or tool, Adobe relies on mitigating controls using a variety of solutions to protect data, which include (but are not limited to) the following:

- Centralized security information and event management (SIEM) solution — Correlates logged events and network activity in production environments.
- Secure bastion hosts — Control administrative access to production environments. Adobe uses a privileged access management (PAM) solution to prevent exfiltration of production customer data out to the network. Reverse tunneling is disabled from the solution, which in turn blocks the movement or duplication of any customer data from production environments to machines on the Adobe corporate network. In addition, any connection requests from the production environment to the corporate network are denied.
- Specific policies and standards — Help ensure only authorized individuals have access to sensitive assets, define operational and data security mechanisms, include CIS hardening standards (e.g., USB ports disabled), and specify quarterly audits for compliance.

Ransomware Protection

Adobe implements several practices to help protect our corporate network from ransomware attacks. As a foundation, every employee must complete annual mandatory security awareness training. This training covers email awareness and includes how to identify and avoid potential attacks. A number of other tools and technologies covered in this document, such as multifactor authentication, endpoint detection and response, web filtering, email scanning, and our SIEM solution, also play a role in helping to protect Adobe from ransomware attacks.

[1] Key distribution requires the use of a secure transport model (e.g., FIPS 140-2).

User Security Controls

Wireless Network Security

Adobe operates a centrally managed wireless network, which is administered by the Adobe Global Network Infrastructure team. Only Adobe employees using a managed device enrolled in the Adobe corporate mobile device management (MDM) environment and configured for 802.1x authentication can wirelessly access the corporate network. Adobe also offers guest wireless access, which requires an Adobe employee sponsor to create and manage a time-based guest account. Guest network access is segmented from corporate networks and is supported by a guest-only internet egress pathway.

Adobe restricts employees from creating or adding ad-hoc personal and non-Adobe-managed wireless networks while in our offices or other facilities. We monitor and track suspect networks and devices using a wireless network management resource and block access to those we discover.

Employee and Facility Security Controls

Hiring Practices

Adobe obtains background check reports when initially considering an individual for employment. The scope of the report includes educational background, work history, court records (including criminal conviction records), and references obtained from professional and personal associates, each as permitted by applicable law.

These background check requirements apply to regular U.S. new-hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable agency, in compliance with the agency's background screening guidelines.

Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Termination Process

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day.

In the event Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, they can no longer access to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Data Center Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Physical Facility Controls

Adobe corporate office locations employ on-site security guards 24x7 to protect the premises. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, check in and out with the receptionist, display a temporary Visitor ID badge, and must be accompanied by an employee.

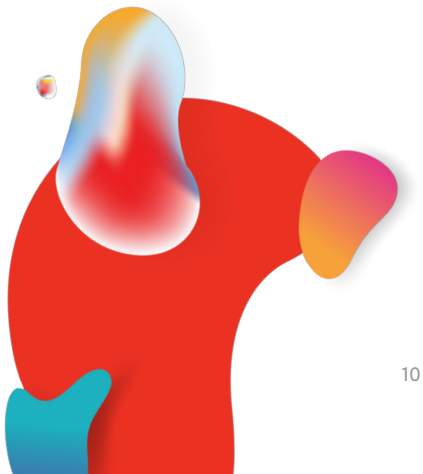
Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems secured in environment-controlled server rooms and accessible only by appropriate, authorized staff members.

More details about our physical security controls are included in Adobe internal published standards, which are audited regularly by independent auditors.

Asset Management

The Adobe System Asset Management Policy outlines how we manage hardware assets (e.g., laptops, desktops, smartphones, and tablets) issued to Adobe employees. Any asset that collects, processes, transmits, or disposes of any Adobe corporate data is governed by this policy, which encompasses the following:

- Asset tracking and inventory
- Acceptable use of assets
- Workstation and mobile configuration and protection
- Software licensing and usage
- Unapproved software
- Asset disposal
- Lost or stolen assets



Vendor Security Controls

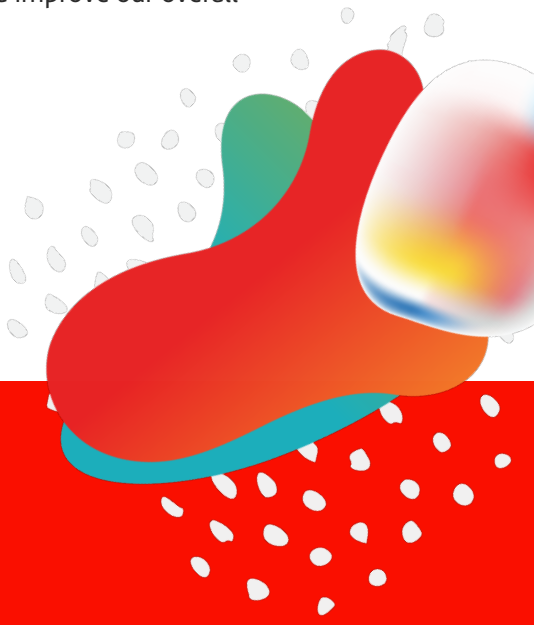
Managed by the Adobe Security organization, the Adobe Vendor Security Review (VSR) program extends our internal enterprise security controls to the various suppliers that work with Adobe. The program provides a set of requirements to which third-party vendors that collect, store, process, transmit, or dispose of Adobe data outside of Adobe-controlled physical offices or data center locations must adhere.

The Adobe VSR program evaluates each vendor's compliance to our Vendor Information Security Standard, providing a risk-based review of the vendor's security practices and enabling Adobe managers to make fact-based decisions concerning whether to enter or continue a relationship with that vendor.

The Adobe Vendor Information Security Standard is available for customer review by request. More information about our VSR program can be found in the Adobe Vendor Security Review Program white paper.

Conclusion

With the Adobe ZEN platform as its foundation, Adobe's comprehensive enterprise security strategy includes robust controls for the protection of our network infrastructure, data, users, employees, and physical facilities. The Adobe VSR program extends our internal enterprise security controls to the various suppliers that work with Adobe, helping protect our supply chain as well. Driven by the Adobe CCF, Adobe's enterprise security controls help reduce risk across Adobe, keep our intellectual property and other assets secure, and improve our overall corporate security posture.



Adobe

4/23