WHITE PAPER

HP Document Workflow Cloud Solutions

AWS Cloud Security and Data Center Standards

Confidentiality, integrity, and availability of your critical data is vital to your business operations. With our enterprise-grade cloud operations, HP Software's driving purpose is to affirm the trust you've put in us, while delivering to and exceeding your expectations.

Adhering to best-practice standards and procedures is the backbone of our cloud-based Software-as-a-Service (SaaS). Enabling connectivity, reliability, speed, security, and scalability across the enterprise, HP delivers impressive outcomes for our customers. HP's data centers provide best-in-class, cloud-delivered security, with superior infrastructure security and integrity, strict standards, true multi-tenant service, high resiliency, and scalability.

Shared security responsibility

Infrastructure standards and procedures

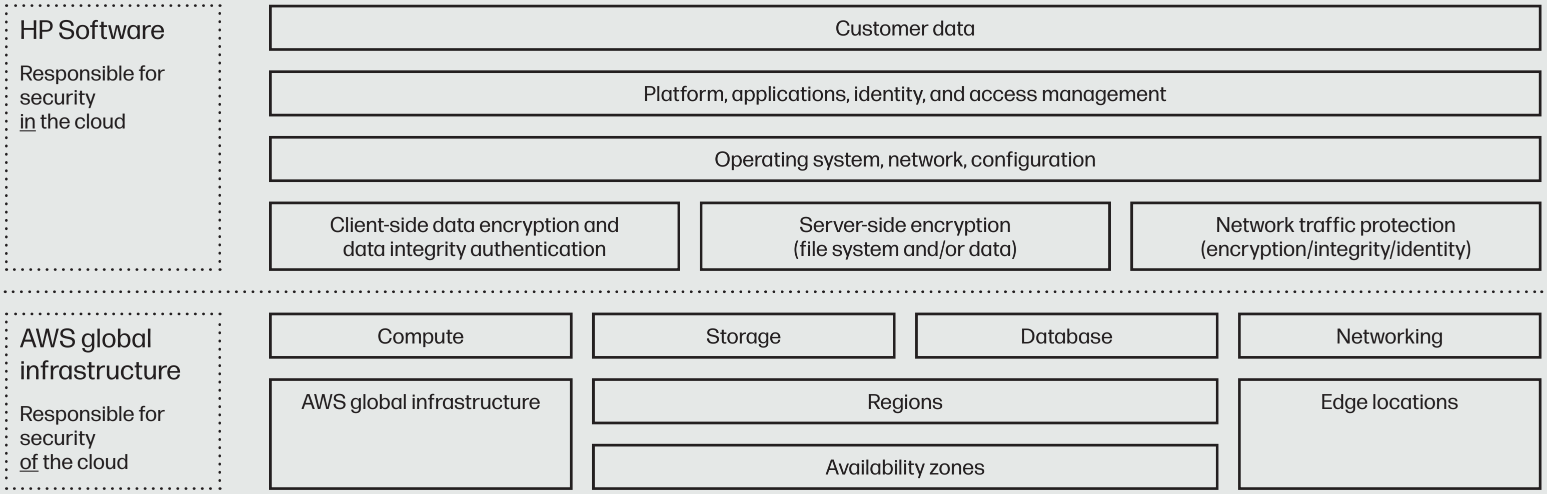
HP Document Workflow Cloud Solutions AWS Security maintains the following standards and undertakes the following procedures in relation to the infrastructure that provides its services:

- Central code repository with automated code quality scoring
- Segmented and secure virtual private cloud (VPC) networks
- Highly restricted, role-based access to production EC2 environments governed by the least privilege principle
- Hardened EC2 instance images
- Two-factor authentication requirements for server and console access
- Redundant servers for critical systems
- Software-based firewalls configured to "default deny"
- High availability built-in, via virtual load balancers
- Unlimited, secure storage capacity with S3
- Continuous monitoring of all components, subcomponents, and internal/external/front-end/back-end applications to assist infrastructure and service integrity

Infrastructure redundancy

HP's AWS primary data centers provide a global average uptime of >99.9999%. This is equal to each of the data centers experiencing outages totaling less than 5 minutes and 15 seconds over the course of a year.

To ensure availability, all HP infrastructures deploy a minimum of N+1 redundancy: every mission-critical component has at least one backup.


HP Software
Responsible for security in the cloud
Customer data
Platform, applications, identity, and access management
Operating system, network, configuration
Client-side data encryption and data integrity authentication
Server-side encryption (file system and/or data)
Network traffic protection (encryption/integrity/identity)
AWS global infrastructure
Responsible for security of the cloud
Compute
Storage
Database
Networking
AWS global infrastructure
Regions
Availability zones
Edge locations

AWS/data center network security

HP Software follows in the defense-in-depth strategy. Our Amazon infrastructure is protected by several layers of network-based security controls including host-based firewalls, intrusion detection systems, F5 load balancers, and virtual firewall technology such as AWS Security Groups.

Encryption is used to protect data in transit, including SSL (TLS 1.1, 1.2) encryption over HTTPS connections utilized for secure communications between HP and customer end users. Authorized IT engineers access production network equipment and data stored remotely, via secure two-factor authentication enabled SSL virtual private network (VPN) tunnels.

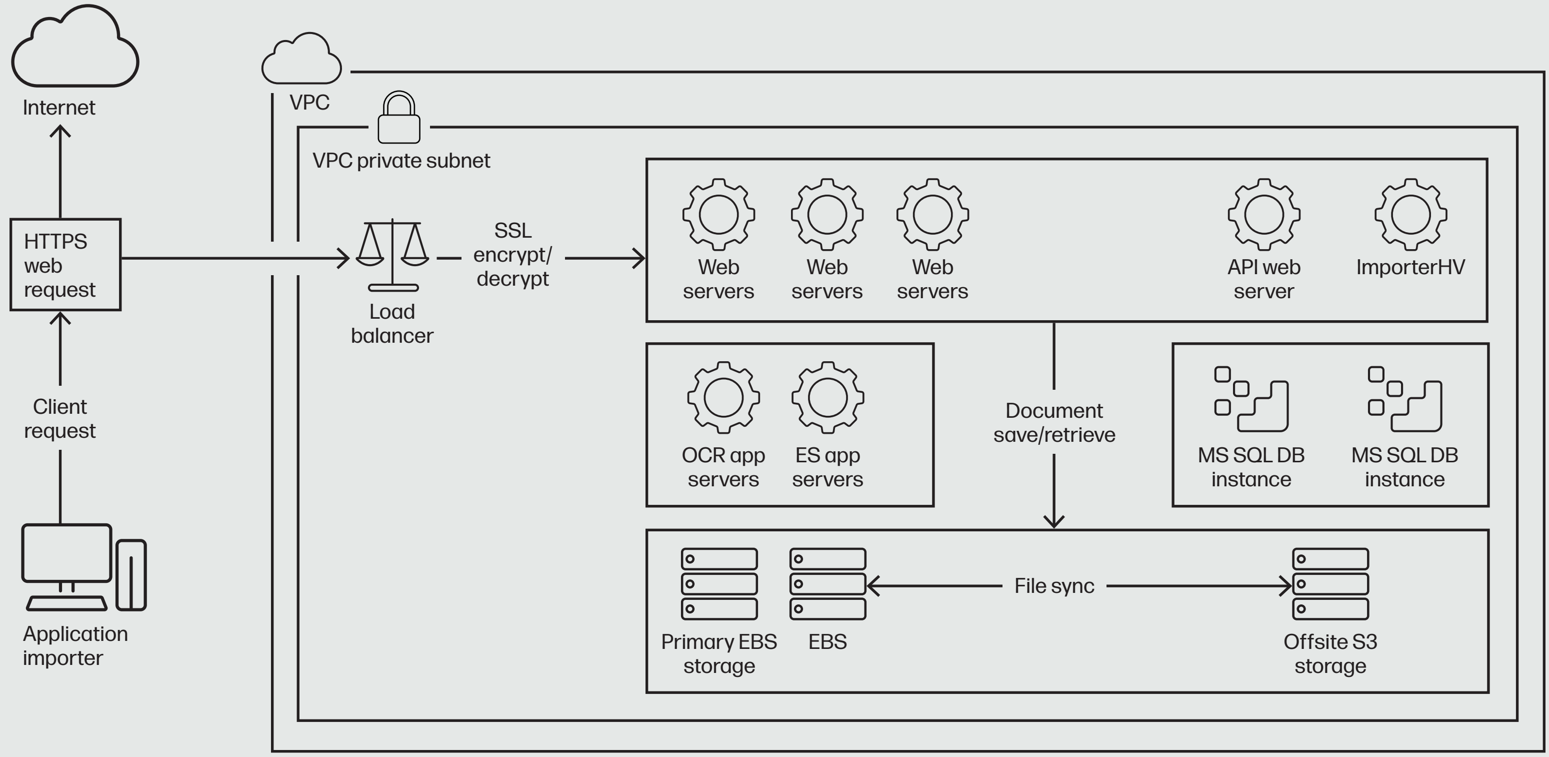
AWS Security Groups

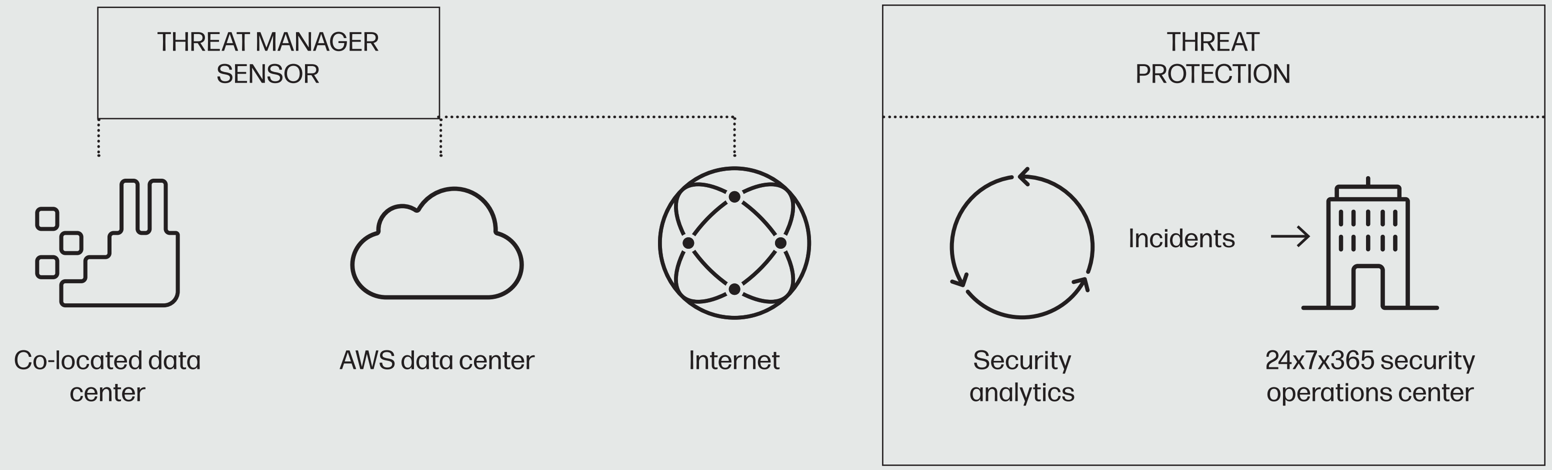
Security Groups are best conceptualized as a distributed, stateful virtual firewall that sits “in-front” of each EC2 Instance. More specifically, this function resides within the Virtual Device Driver layer on the hypervisor.

Some key properties of Security Groups:

- Both ingress and egress packet flows are filtered.
- Rules are ALLOW only.
- By default, security groups DENY ALL ingress traffic until allow rules are created.
- Security group objects themselves can be referenced as source/destination in rules.

This distributed approach to packet filtering is more secure than relying on a single perimeter device, since, in effect, every EC2 instance is protected by its own virtual firewall. Amazon security groups are administered by our dedicated Cloud Operations team in tandem with the Security department.





RISK ASSESSMENT

HP's Security Organization is responsible for identifying risks (compliance, legal, technical, and supplier) that threaten services and systems. We have implemented a process for identifying relevant risks, which includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding upon actions to address them. We have established strategic, operations, reporting and compliance objectives to identify potential risk events. We consider external and internal factors so that our risk assessment efforts can adequately support business decisions and respond to potential threats.

Risk analysis is an essential process to an organization's success. HP's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance or impact of threats that face HP assets
- Assessing the likelihood (or frequency) of threat occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

MONITORING

HP's Security Organization performs monitoring activities to continuously assess the quality of internal controls and security posture of our environment over time. The continuous monitoring activities are:

- Real-time scanning of all web traffic for intrusions and anomalies
- Recurring internal vulnerability scans of hosts in the environment
- Recurring external vulnerability scans of external IP addresses and ranges of the environment
- Continuous, real-time monitoring of all security logs generated on all servers in the environment

Additionally, HP employs Intrusion Prevention Systems to actively block traffic that matches specific patterns. And we monitor synthetic user transactions such as building documents and searching in the library. The results of these activities are made available to our security analysts, operational teams, and management, so analysis and remediation can be performed. Security staff is on hand 24x7x365 to perform this analysis and remediation.

These activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and takes necessary corrective actions to fix deviations from company policy and procedures.

REPORTING

HP Document Workflow Cloud Solutions AWS Security manages incidents by identifying and responding to them quickly, notifying key support and management personnel in a timely manner, restoring service as soon as possible, determining the cause of the incident, and taking appropriate steps to prevent future incidents. Our incident management process also allows us to quickly notify external organizations that may have been affected by an incident, including customers and partners. We employ both internal and external monitoring systems that periodically verify the state of each HP cloud-based solution product.

Along with incident handling, HP understands the importance of having a security incident response process in place. As such, we ensure that any instance of suspected disclosure of sensitive information is reported immediately and escalated appropriately to HP's Information Security Representative and Legal Counsel. The Security Team will handle initial responses and would assume leadership and direction for the Security Incident Response Team (SIRT). Together, these teams—Legal, Security, and SIRT—would effectively coordinate, collect, respond, and report security events.

Universal accessibility

Increased visibility

Complete scalability

Best-in-class security

Benefits of AWS

HP Software maintains the following standards and undertakes the following procedures in relation to the infrastructure that provides its services:

- Broad and deep platform—AWS has more than 70 services and is continually launching new features and functionality.
- Pace of innovation—The AWS Cloud platform expands daily.
- Global infrastructure—42 availability zones in 16 geographic regions worldwide.
- Secure—Comprehensive capabilities for the most demanding information security requirements.
- Compliant—Rich controls, auditing, and broad security accreditations.
- Trusted—Supports virtually any workload for over a million active customers in 190 countries.