walkme

Security Datasheet

- WalkMe meets the most extensive compliance standards
- WalkMe utilizes Amazon's top-tier secure cloud services
- WalkMe's platform and infrastructure undergo routine pen-tests and are monitored continuously by dedicated teams
- WalkMe's solution is non-obtrusive and does not collect, capture or use confidential data

An Industry Standard

WalkMe's Digital Adoption Platform (DAP) is used by over 1,000 companies worldwide, spanning all industries and sizes, including the Fortune 500, cybersecurity, healthcare and financial sectors.

Compliance

WalkMe is ISO 27001:2013 certified for Information Security, SOC 2 certified to meet AICPA's Trust Security Principals, rated Skyhigh Enterprise-Ready™, and has STAR Certification from the Cloud Security Alliance. The DAP is also US-EU, US-Swiss Safe Harbor and Privacy Shield certified.

Hosting and Infrastructure

WalkMe's Software as a Service (SaaS) solution is available for both public and private clouds utilizing top-tier secure cloud services provided by Amazon and Akamai.

Penetration Tests and Monitoring

WalkMe's front and back-end applications, as well as its IT infrastructure undergo routine annual pen-tests by independent companies. This is done in addition to Amazon AWS's own independent tests, periodic internal tests, and 24/7 monitoring of security-related events by dedicated teams.

Certifications and Accreditations

Security

ISO 27001 Information Security Certification

WalkMe received the International Organization for Standardization Certification for Information Security (ISO 27001:2013). The audit evaluated WalkMe's information security management system from product, infrastructure and organizational aspects, and verified that WalkMe has the necessary information security controls in place to ensure the confidentiality, integrity and availability of sensitive information assets. WalkMe is also certified for ISO/IEC 27032:2012 (Guidelines for Cybersecurity), ISO/IEC 27017:2015 (Cloud Specific Controls), ISO/IEC 27018:2014 (Personal data Protection), ISO 27799:2016 (Security management in health).

SOC2

WalkMe completes periodic Service Organization Control Type II (SOC2) audits – one of the most demanding and strict international standards for security, availability, processing integrity, confidentiality and privacy.

STAR Certification

WalkMe achieved the STAR Certification from the Cloud Security Alliance (CSA). The STAR Certification is an internationally recognized cloud security certification program jointly developed by CSA and BSI, specializing in comprehensive and stringent cloud security.

Skyhigh CloudTrust™

WalkMe's Digital Adoption Platform was awarded the Skyhigh CloudTrust™ rating of Enterprise-Ready™ by fulfilling a comprehensive set of requirements for data protection, identity verification, service security, business practices, and legal protection.

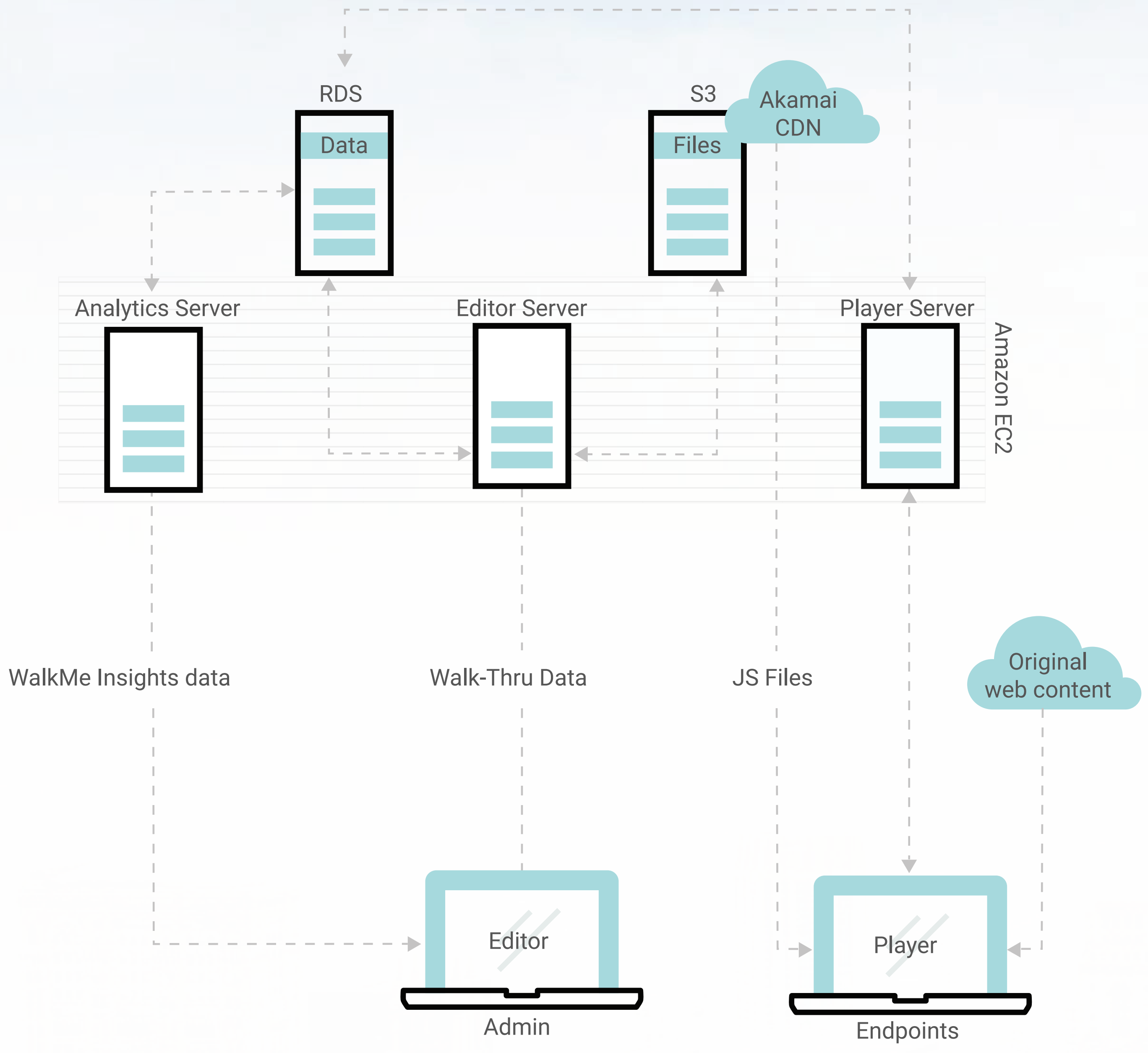
FIPS 140-2 (Level 1)

All of WalkMe's cryptographic modules are FIPS validated.

Privacy

TRUSTe, EU/Swiss – U.S. Privacy Protection
WalkMe's platform is certified according to Safe Harbor and Privacy Shield standards, providing a safe and regulated framework to transfer personal data from the EU to the US. This includes transmitting personal data from an AWS region in the European Economic Area (EEA) to one outside the EEA, in full compliance with EU data protection thanks to Amazon AWS' existing Data Processing Addendum, including Model Clauses (Data Processing Addendum) of which WalkMe is a signee.
WalkMe is committed to the strictest obligations regarding the collection and processing of user data, and does not collect, accept, handle, process, receive, transmit or store any confidential, regulated, personal, private, sensitive, health or credit card information.

Architecture and Delivery – Websites and Web-Apps



WalkMe Modules

Editor (Authoring/Admin Tool)

The WalkMe Editor is the central authoring and management tool used to create, maintain and deploy WalkMe's interactive components to digital platforms such as consumer websites and enterprise management systems. The Editor captures HTML element metadata and assigns them with WalkMe's interactive components. Once published, the Editor generates static JavaScript (JS) files that are usually hosted on WalkMe's Amazon Cloud, and distributed through WalkMe's Akamai CDN for rapid access.

Player (Client)

The WalkMe Player is an independent software module in the form of a snippet code or browser extension, that overlays WalkMe's interactive components on top of websites and web-applications, and embeds WalkMe's interactive components into a workflow or funnel, to guide users and gauge their behavior.

WalkMe's Player snippet is a single line of code inserted into HTMLs, similar to how Google Analytics works. The snippet points to the JS files containing WalkMe's elements and their configurations, which are then downloaded from the Akamai CDN. Once downloaded, the JS files are stored in the browser cache, and are downloaded again only if changes were detected, ensuring minimal bandwidth overhead.

WalkMe's Player extension is a lightweight browser-extension used when the HTML cannot be edited. The extension injects the snippet into the relevant web pages.

Service Models

WalkMe's typical SaaS model is set up on Amazon Web Services (AWS), with management servers located on Amazon EC2, and storage divided between Amazon RDS for secure data, and Amazon S3 for published content, which is distributed by Akamai CDN for fast download rates.

WalkMe can store its files and data (the green elements in the diagram) on an internal server belonging to the customer, It can also deploy WalkMe's servers (the blue elements in the diagram) on a separately dedicated AWS, and in some cases even deploy the entire system in the customer's own datacenter.

Operations and Access Control

Access Control

User Management and Permissions

that WalkMe’s platform has an integrated, comprehensive role-based user management and enforcement system.

Assigning roles to users requires authorization from the relevant parties in WalkMe, and application permissions are granularly controlled per action and screen. Eight default roles are built into the platform, including: administrator, content creator, publisher, analytics access, etc.

WalkMe allows customers to control multiple platforms and deployments, delegate usage and administrative permissions for the interactive components and GUI elements deployed by WalkMe, while maintaining central management of the entire deployment cycle.

Accountability and Security

Compartmentalization and Enforcement

WalkMe’s internal corporate access control is centrally and manually managed based on strict need-to and leastprivileged principles on all levels: Application (strong authentication), Network (segmentation, firewall), OS (access to servers), and Procedural (who is authorized to review/approve code, manage changes, etc.).

All internal duties within WalkMe are segregated based on duties between R&D (code development), DevOps (deployment) and Security (security controls). Access reviews are done quarterly by the security team, including but not limited to: firewall rules, user accounts permissions, etc.

Intrusion Prevention and Detection

WalkMe has an extensive Security Information and Event Management system (SIEM) that collects security audit trail logs across infrastructure components in industry standard formats (CEF and Syslog) using an Intrusion Detection System.

WalkMe’s SIEM alerts are based on comprehensive pre-defined scenarios, including identification of suspicious activity such as failed login attempts, login from unknown and off-premise IP addresses or during off-hours.

SIEM alerts are monitored 24/7 by WalkMe’s Security Operations Center (SOC) team, which then prioritizes them and notifies the security team in real time and acts on them according to severity.

Conclusion

As the Digital Adoption Platform pioneer, backed with an uncompromising commitment to security and privacy, WalkMe is trusted by over one thousand companies worldwide, including the Fortune 500, cybersecurity, healthcare and financial sectors. WalkMe makes sure to comply with corporate, governmental and international regulations, maintaining and abiding by the strictest requirements, regulations and security measures at all levels — from its staff, through infrastructure and down to the finest details of its products and procedures.

WalkMe has received the most demanding international certifications in the industry, and offers customers management tools to enforce corporate governance internally, while providing an overarching security umbrella — hosting WalkMe’s infrastructure with top-tier cloud providers, actively monitoring customer security 24/7, and performing periodic independent pen-tests on WalkMe’s platform and IT infrastructure.