FREQUENTLY ASKED QUESTIONS

VMware Workspace ONE Intelligence

Product Capabilities

Q. What is Workspace ONE Intelligence?

A. VMware Workspace ONE Intelligence is a service for Workspace ONE customers that delivers insights, analytics and automation for the Digital Workspace. It provides robust visibility into security risk and digital employee experience through dashboards and reports, with an automation engine that enables faster, policy-based actions.
By aggregating data from multiple internal and external sources and analyzing and correlating the data by applying analytics and machine learning models, Workspace ONE Intelligence enables decision makers to make smarter, data-driven decisions. There are two main areas of use cases for Workspace ONE Intelligence:

- **Improving user experience** – Workspace ONE Intelligence provides EUC admins with the data and analytics they need in order to improve overall digital employee experience. Examples include predicting hardware failures and automating replacement, tracking app analytics and performance and monitoring OS adoption.
- **Embracing Zero Trust security** – Workspace ONE Intelligence enables IT to implement security processes that are aligned with the Zero Trust framework such as calculating risk score based on user behavior and device context for conditional access. Workspace ONE Intelligence also delivers advanced CVE management and endpoint security with a variety of security partners.

Q. What key capabilities are included in Workspace ONE Intelligence?

A. Workspace ONE Intelligence includes the following key capabilities:

- **Integrated insights** – out of the box as well as custom dashboards and reports across the entire digital workspace.
- **App analytics** – app performance and analytics including app engagement and adoption, user flows and network insights.
- **Digital employee experience** – monitoring digital workspace KPIs impacting employee experience.
- **Risk Analytics** – user risk score that is based on user behavior, device context, and historical data.
- **CVE management** – ingesting CVE data from public sources for in-context analysis and always on patching.
- **Trust Network** – Ingest API that enables security partners such as Lookout, Carbon Black, Netskope and others to ingest threat data into Workspace ONE Intelligence.
- **Automation and orchestration workflows** – a powerful automation engine that can automate actions and orchestrate workflows across the digital workspace.

Q. Who is the target audience for Workspace ONE Intelligence?

A. The target audience for Workspace ONE Intelligence includes customers who are looking to take their digital workspace to the next level with insights, analytics and automation. Since the real value of Intelligence is when there is a lot of data, typically customers will be Enterprise, Global, Government, etc. with at least 10K devices under management.

Q. What are some of the key user experience use cases?

A. Here are key use cases for customers looking to improve user experience:

- Predicting hardware failures and automating replacement.
- Insights and compliance across Win10 devices
- OS tracking
- App analytics and performance
- Tracking app migration and adoption
- Workflow orchestration with automation
- Win10 app entitlement and approvals

Q. What are some of the security use cases?

A. Here are key security use cases:

- Managing CVEs with faster and always on patching.
- Calculating user and device risk scoring
- Implementing conditional access
- Streamlining endpoint security
- Device quarantine

Q. What is Risk Analytics and what capabilities come with Workspace ONE Intelligence?

A. Risk analytics in Workspace ONE Intelligence analyzes data from a variety of data sources (such as Workspace ONE

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.

VMware Workspace ONE Intelligence

Access and Workspace ONE UEM) to identify behaviors that may represent risk to a user, their device(s) or to the organization. By leveraging machine learning models and data, Workspace ONE Intelligence calculates user and device risk score based on device context and user behavior, enabling continuous verification and conditional access, which are central to Zero Trust.)

Q. What is Digital Employee Experience Management (DEEM)?

A. Workspace ONE Intelligence Digital Employee Experience Management (DEEM) is a set of capabilities available with Workspace ONE Intelligence that enable EUC admins to better understand factors and digital workspace KPIs impacting employee experience and take actions to fix them. Some examples include:

- Boot and shutdown duration
- Logon/logoff duration
- OS stability (blue screen, slow response times)
- App crashes and hangs
- App performance and network insights
- Hardware health (e.g. battery drain)

Q. Do APIs exist?

A. Workspace ONE Intelligence APIs gives customers access to the rich reporting capabilities in Workspace ONE Intelligence. It also allows customers to export the data from Workspace ONE Intelligence and use it with a third-party system.

Q. What is the difference between Workspace ONE Intelligence and Workspace ONE Intelligence for Consumer Apps?

A. Workspace ONE Intelligence delivers insights, analytics and automation for Workspace ONE environments and app analytics for enterprise applications that are internal to the organization. Workspace ONE Intelligence for Consumer Apps deliver mobile app analytics for consumer facing applications, that are being used outside the organization. Workspace ONE Intelligence for Consumer Apps is a standalone SaaS offering that does not require Workspace ONE.

Extensibility

Q. Can Workspace ONE Intelligence integrate with other security vendors?

A. Workspace ONE Intelligence can integrate with third party security vendors through the Workspace ONE Trust Network. Security vendors can integrate with Workspace ONE Trust Network and ingest threat data into Workspace ONE Intelligence, providing joint customers added value from this integration. By leveraging threat intelligence from Workspace ONE Trust Network partners, IT can become more proactive with deeper insights and automated response and remediation across the digital workspace, further supporting the Zero Trust security framework.

Q. Does the customer need to contract with the third-party security vendor in order to leverage Trust Network?

A. Yes, Workspace ONE Intelligence enables customers to realize more value from their existing investment in security tools. Customers will have to choose their security vendor and contract separately.

Q. Can Workspace ONE Intelligence integrate with other third-party and custom tools?

A. Yes, through Custom Connectors in Workspace ONE Intelligence customers can create integration with any third-party and custom tools that support REST APIs. Out of the box integrations include ServiceNow and Slack.

Security

Q. How can customers guarantee that their data is secure in the cloud?

A. The system has gone through penetration testing by a team of VMware InfoSec professionals. Customer data collected from the Workspace ONE production environment is encrypted using HTTPS (TLS 1.2) for uploading to AWS to ensure confidentiality during transfer.
Only customers can access the data through Workspace ONE login and the Workspace ONE console interface. VMware will not access customer's data without their consent. Various levels of multifactor access control lock-down to only show data at the request of the customer.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.

FREQUENTLY ASKED QUESTIONS

VMware Workspace ONE Intelligence

Q. What about data privacy?

A. The customer has control over all personally identifiable information (PII) sent to the cloud, such as phone number, username, email and private app information.

Q. What data is being collected by Workspace ONE Intelligence?

A. Workspace ONE Intelligence aggregates data from multiple sources. Admins have control over the data being sent (can opt in/out, set up/deauthorize the connection, etc.)

- Workspace ONE UEM: device ID (UDID, IMEI, IP, MAC, Serial Number), first name, last name, email, managed apps list, telecom and network information, apps usage data, security health of devices.
- Workspace ONE Access: user login details including successful and failure attempts, app launch data.
- Workspace ONE Intelligence SDK: app crash details, monthly active users (MAU), daily active users (DAU), app launch, network details, app usage details.
- Common Vulnerabilities and Exposures (CVEs): doesn't contain any PII data. Workspace ONE ingests CVE data from public sources such as NIST.
- Trust Network: Workspace ONE Intelligence ingest threat data from security partners. Data does not include PII information.

Pricing and Packaging

Q. How is Workspace ONE Intelligence licensed?

A. Workspace ONE Intelligence is licensed on per-user or per-device on an annual subscription basis.

Q. What is the pricing for Workspace ONE Intelligence?

A. Workspace ONE Intelligence is available as part of Workspace ONE Enterprise, or as an add-on to Workspace ONE Advanced and Workspace ONE Standard customers. The Workspace ONE Intelligence add-on includes Mobile Flows. For prices in your area please contact your sales team.

Q. What features of Workspace ONE Intelligence are available in Workspace ONE?

A. Workspace ONE Intelligence reporting features that are available to all Workspace ONE customers at no additional cost include:

- Granular reporting capabilities
- Report customization
- Live preview
- Advanced scheduling and sharing

Resources

Q. Where can I find more information about Workspace ONE Intelligence?

A. To learn more:

- Workspace ONE Intelligence *website*
- Workspace ONE on Tech Zone *here*
- Workspace ONE Intelligence *YouTube playlist*
- Workspace ONE Intelligence for Consumer Apps *website*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.