fleet

VMware WorkspaceOne

Overview
VMware WorkspaceOne is an integrated digital workspace platform that manages and delivers any app on any device. It combines access control, application management, and multi-platform endpoint management, catering to a diverse range of organizational IT needs.

Product
VMware WorkspaceOne offers Unified Endpoint Management (UEM) which provides comprehensive device management capabilities. It supports application management and updates, secure single sign-on (SSO), and multifactor authentication (MFA), enhancing both user convenience and security.

Pricing
VMware WorkspaceOne employs a subscription-based pricing model. The cost is tailored to the scale and specific needs of the organization, potentially including various tiers and bundle options that can influence the overall investment.

Integrations
VMware WorkspaceOne integrates extensively within the VMware ecosystem and supports a wide range of IT and security technologies, enhancing its capability to operate within complex IT environments effectively.

	VMware WorkspaceOne	**How Fleet addresses**
Claims	- Marketed as an integrated digital workspace platform. - Manages and delivers any app on any device. (Limited to macOS, Windows, iOS, Android, and IoT devices) - Combines access control, application management, and multi-platform endpoint management.	- Provides a comprehensive, open-source device management solution. - Focuses on cross-platform support (Windows, macOS, iOS, Linux, ChromeOS) with customizable MDM workflows. - Emphasizes real-time monitoring, security, and scalability. - Lower infrastructure

		strain via watchdog on Fleetd agent - “Context is king for device data, and Fleet provides a way to surface that information to our other teams and partners.” - Nick Fohs
Competitor strengths	- Extensive integration with VMware products. - Comprehensive Unified Endpoint Management (UEM) capabilities. - Proven scalability and reliability for large-scale enterprise deployments. - Advanced automation for policy enforcement and compliance.	- Offers unparalleled transparency and customization due to its open-source nature. - “We can build it exactly the way we want it. Which is just not possible on other platforms.” - Austin Anderson - Seamless cross-platform functionality enables Mac administrators to effortlessly manage Windows devices (and vice versa). - Provides strong support through an active user community and dedicated Slack channel. - Utilizes osquery for more in-depth, real-time system monitoring - Identify high fidelity vulnerable software - Compliance & policy checks with device health data
Competitor weaknesses	- Higher total cost due to licensing and subscription fees. - Potential support concerns post-acquisition, leaving	- Offers strong community support and comprehensive documentation to mitigate technical challenges.

	some customers uncertain about future updates and integrations. - Complex licensing models can lead to paying for unused features. - API is slow and hard to use	- Community-driven and world class in-house support model provides rapid responses and collaborative problem-solving. - API-first approach allows for rapid adaptation and integration with existing systems and workflows. - “Something I really appreciate about working with you guys is that it doesn't feel like I'm talking to a vendor. It actually feels like I'm talking to my team, and I really appreciate it.” - Chandra Majumdar

Tanium:

Overview Tanium is a leading provider of endpoint security and management solutions. Their platform offers real-time visibility and control across millions of endpoints, helping organizations improve security, IT operations, and compliance.
Product Tanium provides a comprehensive endpoint management and security platform that includes features such as asset discovery, vulnerability management, threat detection, incident response, and compliance management. While Tanium does not use osquery directly, it offers similar endpoint visibility and control functionalities.
Pricing Tanium follows a customized pricing model based on the specific needs and scale of the organization.
Integrations Tanium integrates with a wide range of IT and security technologies, such as SIEM platforms, threat intelligence feeds, EDR solutions, and network security tools. Their platform is designed to be flexible and interoperable within complex IT environments.

	Tanium	**How Fleet addresses**
Claims	- Marketed as a comprehensive endpoint management and security platform. - Emphasizes managing large-scale, diverse device fleets with capabilities in threat detection and incident response.	- Fleet utilizes osquery for in-depth, real-time system monitoring. - Fleet offers a more adaptable autopatching approach aligned with best practices. - Fleet also manages diverse device fleets (including ChromeOS) and can pull more granular/contextual telemetry more frequently
Competitor strengths	- Established market presence, especially	- Fleet focuses on tailored and flexible

	in large enterprises. - Robust set of management features emphasizing security.	solutions, providing comprehensive management across various operating systems. - Fleet uses an open-source approach, enabling rapid adaptation to new security threats and IT needs.
Competitor weakness	- Lacks direct osquery integration, real-time insights are limited. - Autopatching capabilities may not align well with the latest patch management best practices. - Does not offer a fully comprehensive EDR solution.	- Fleet provides granular control and detailed insights via osquery, enhancing the overall security posture and incident response capabilities. - Fleet promotes easier adoption and greater operational flexibility through a user-friendly interface. - Fleet includes extensive threat detection capabilities akin to an EDR system, leveraging real-time data analysis.

Intune

Overview Microsoft Intune is a cloud-based service in the enterprise mobility management (EMM) space that helps enable your workforce to be productive while keeping your corporate data protected. It manages mobile devices, applications, and PCs through the cloud.
Product Microsoft Intune provides comprehensive device management, application management, and security capabilities across diverse platforms, including iOS, Android, Windows, and macOS. It supports conditional access, mobile application management, and collaborative management with other Microsoft services.
Pricing Microsoft Intune employs a user-based subscription pricing model, which is often bundled with other Microsoft 365 services. This allows organizations to manage costs effectively while benefiting from integration with Microsoft's ecosystem.
Integration Microsoft Intune integrates deeply with other Microsoft solutions such as Azure Active Directory for identity services, Microsoft 365 for productivity apps, and Azure Information Protection for data security, making it a cohesive part of the Microsoft enterprise management suite.

	Intune	**How Fleet addresses**
Claims	- Marketed as a cloud-based unified endpoint management (UEM) solution. - - Manages and secures devices, apps, and identities across an organization. - - Aims to increase end-user productivity while protecting corporate data.	- Fleet provides a comprehensive, open-source device management solution. - Focuses on seamless cross-platform support (Windows, macOS, Linux) with customizable MDM workflows. - Emphasizes real-time monitoring, security, and scalability.
Competitor Strengths	- Integrates seamlessly with other Microsoft products and services. - Robust security features that integrate	- Fleet offers unparalleled transparency and customization due to its open-source nature, ensuring user

	with the Microsoft security ecosystem. - Offers comprehensive device management capabilities with support for a broad range of policies and configurations. - Extensive automation capabilities for deploying apps and managing devices. - Often offered at no additional cost if bundled with other products within the Microsoft ecosystem	trust and clarity in device monitoring and security practices. - Fleet's GitOps workflow ensures consistent and efficient management of security configurations across all devices - Fleet’s API-first approach allows for rapid adaptation and integration with existing systems and workflows. - Fleet is making the Autopilot feature free in Fleet (in progress)
Competitor weaknesses	- Can be complex and costly, especially for organizations not fully invested in the Microsoft ecosystem. - Challenges with learning and managing diverse devices not optimized for Windows.	- Fleet offers seamless cross-platform support (Windows, macOS, Linux) with customizable MDM workflows - Fleet’s community-driven support model provides rapid responses and collaborative problem-solving.

Content notes:

Overview

Fleet MDM

(Website): [Fleet Device Management](https://fleetdm.com/device-management)

Description: Fleet MDM provides comprehensive device management solutions focused on cross-platform (Windows, macOS, Linux), rich endpoint/device data, customizable MDM workflows. Ideal for organizations needing contextual/granular visibility and control over their devices and software.

VMware WorkspaceOne
(Website): VMware WorkspaceOne (https://www.vmware.com/products/workspace-one.html)
Description: VMware WorkspaceOne is an integrated digital workspace platform that delivers and manages any app on any device. It combines access control, application management, and multi-platform endpoint management.

Key Features

Fleet MDM
- Open-Source: Fully transparent and customizable. API first and GitOps focused.
- Real-Time Monitoring: Provides continuous visibility into device health and compliance.
- Security-Focused: Emphasizes robust security measures and quick threat detection.
- Scalable: Suitable for businesses of all sizes, ensuring flexibility and growth. Enterprise ready and load tested for hundreds of thousands of devices.

VMware WorkspaceOne
- Unified Endpoint Management (UEM): Comprehensive management for all device types.
- Access Control: Secure single sign-on (SSO) and multifactor authentication (MFA).
- Application Management: Seamless app delivery and updates.
- Automation: Advanced automation for policy enforcement and compliance.

Strengths

Fleet MDM
- Transparency: Open-source model fosters trust and flexibility.
- Cost-Effective: No licensing fees, reducing total cost of ownership.
- World Class Support: Dedicated Slack channel, fast response time. Strong support from an active user community as well.

VMware WorkspaceOne
- Integration: Primarily integrates with other VMware products.
- Robustness: Extensive feature set covering a wide range of device management needs.
- Enterprise-Ready: Proven scalability and reliability for large organizations.

Weaknesses

Fleet MDM
- Complexity: May require more technical expertise to deploy and manage.
- World Class Support: Less direct vendor support compared to proprietary solutions.

VMware WorkspaceOne
- Cost: Higher total cost due to licensing and subscription fees.

- Complex Licensing: Bundle-based model can lead to paying for unused features.
- Lacking support: After the broadcom acquisition VMware customers have not seen guidance or help figuring out what the future of their VMware offering will be. Many customers being left in the dark.

—

Use Cases

Fleet MDM

- Cost effective and scalable solutions for SMEs and large enterprise
- Tech-Savvy Organizations: Companies with in-house technical expertise to leverage open-source benefits.

VMware WorkspaceOne

- Large Enterprises: Ideal for organizations needing comprehensive and scalable management.
- Diverse Device Environments: Suitable for businesses with a wide variety of devices and platforms.

Conclusion

Fleet MDM is best suited for organizations looking for a cross-platform, customized control, and world class support.

VMware WorkspaceOne is ideal for large enterprises requiring robust, integrated, and enterprise-ready device management capabilities.

For more information:

- [Fleet MDM](https://fleetdm.com/device-management)
- [VMware WorkspaceOne](https://www.vmware.com/products/workspace-one.html)

Additional links:

https://www.techradar.com/pro/broadcom-backs-down-on-vmware-pricing-rules-as-eu-begins-investigation-following-complaints

https://www.techradar.com/pro/vmware-admits-sweeping-broadcom-changes-are-worrying-customers

https://connectedsocialmedia.com/20642/experts-explore-risks-after-broadcom-acquired-vmware/

https://www.techradar.com/pro/broadcom-backs-down-on-vmware-pricing-rules-as-eu-begins-investigation-following-complaints

https://www.verdict.co.uk/broadcom-vmware-deal-remains-risky-for-customers/

https://connectedsocialmedia.com/20642/experts-explore-risks-after-broadcom-acquired-vmware/