IDC MarketScape

IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment

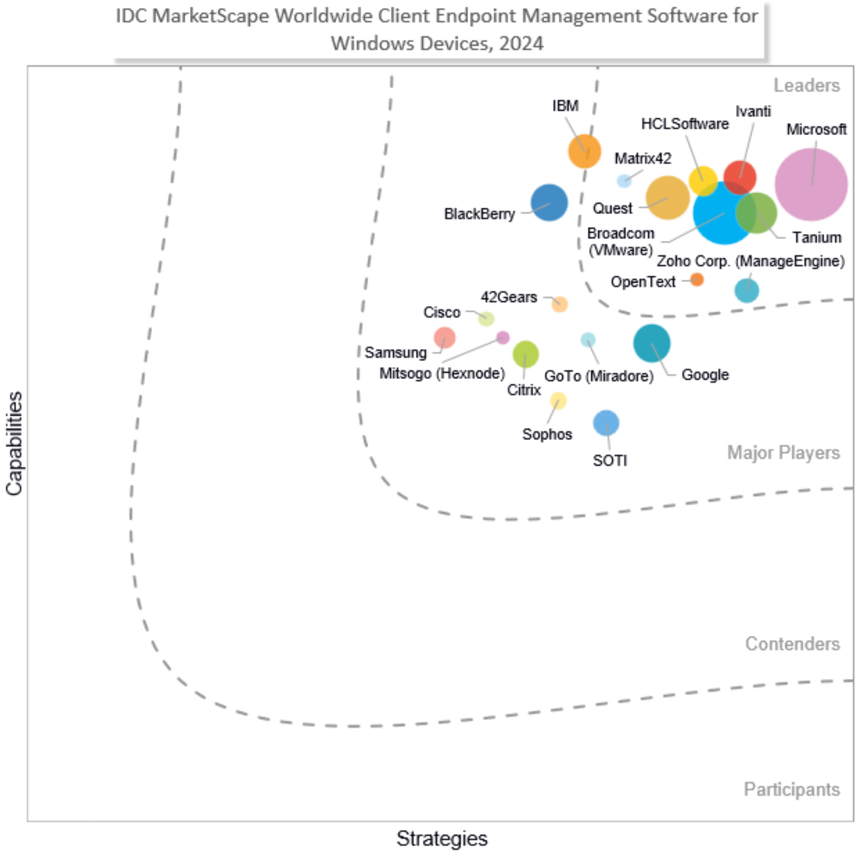
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES TANIUM

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Client Endpoint Management Software for Windows Devices Vendor Assessment



Source: IDC, 2024

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment (Doc # US51234324). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

As enterprises diversify their mixes of endpoint devices and growing in mobile, IoT, and ruggedized device types, it is still a Microsoft Windows world when it comes to the predominant end-user computing (EUC) operating system (OS). According to IDC's Worldwide Personal Computing Device Tracker, 80% of business PCs and laptops shipped in 1Q24 were Windows devices.

Windows, its vulnerabilities, and attack surface are the reasons why PC endpoint security software is a $10 billion market. This makes security, compliance, policy enforcement, and software patching critical functions in client endpoint management (CEM) for Windows devices. Microsoft itself has done a lot to secure Windows, improving OS security and application security and streamlining critical software updates. But attackers still see Windows endpoints as the primary target for attacks such as identity theft, malware injection, ransomware, and other cybercrime activities.

Ongoing endpoint technology functions and operations, such as compliance, anomalous activity detection, malicious code detection, sensitive data detection, and other activities, are critical to endpoint security, and an entire ecosystem and multiple technology markets exist to run these operations across an organization's Windows endpoint fleet. However, in most cases, security starts with good endpoint device OS and application hygiene. Ensuring that Windows devices are updated with the latest software versions for the device firmware, OS, and applications is an enormous part of getting ahead of security challenges. Client endpoint management tools must not only enable security and compliance but also efficiently provision and create productive end-user computing environments for employees. To that end, some critical product functions, and strategic initiatives, for Windows CEM tools are:

- **Support for multiple models of Windows provisioning and management:** Agent-based Windows management is still the norm, as well as PC imaging for device setup. However, with the advent of permanent hybrid/remote workers, offsite/off-network connectivity, and cloud-based everything from an apps and data standpoint, modern device management and over the air/cloud provisioning of Windows are becoming more of a requirement for workers.
- **Strong security capabilities:** Policy enforcement, control over OS state and configuration, and continuous monitoring and application of OS/application patches and vulnerability updates are critical functions of any Windows CEM tool.
- **Integrations and enablement:** A business Windows device usually has an array of client-side agents, processes, and services running. Windows CEM tools must ensure the right software is installed, is configured properly, and does not impede on device performance or worker productivity.
- **Analytics, digital employee experience (DEX), and AI:** Windows CEM tools should be evolving to new areas of functionality, including advanced endpoint telemetry gathering and the measurement and analysis of endpoint telemetry in the context of end-user experiences. AI

should be on any vendor's road map for the specific use cases around vulnerability querying, IT workflow automation and scripting, and proactive/preemptive end-user support actions.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC invited vendors to participate in this assessment based on the following key criteria:

- The vendor has a client endpoint management software product capable of managing devices running Microsoft Windows 10/11 endpoints.
- The vendor has an estimated unified endpoint management (UEM) product revenue of $5+ million for CY23. Revenue was estimated in February 2024 and may differ from forthcoming market share documents.

ADVICE FOR TECHNOLOGY BUYERS

Buyers of CEM tools for Windows should look for the following attributes, capabilities, and relevant use case scenario support from vendors under consideration:

- **End-user analytics and digital employee experience are the future of Windows client management platforms.** With a comprehensive view of a worker's devices, UEM platforms are positioned to collect, analyze, and take action on volumes of available data on the state of an end user's digital experience. Employee behavior, device and application health, usage patterns based on location, time of day, network type, and so forth are all critical in better understanding how employees work with the devices and apps they are given to do work. UEM tools are at the vanguard of providing capabilities around data collection, analytics, and reporting to be part of a larger DEX initiative, spearheaded by UEM technology.
- **Modern management is the future of Windows device management.** Management of corporate PCs is converging around a singular protocol concept — mobile device management protocols (MDM protocols). While OS vendors and device OEMs have implementation of MDM protocols, the central premise and end goal is the same: location-agnostic, agentless, provisioning, configuration, and life-cycle management over the endpoint. While agent-based device management is still necessary in many Windows management scenarios, Windows CEM tool buyers should look to vendors that adhere to the principles of MDM protocol support, as well as automated Windows provisioning technology such as Microsoft Autopilot, with the focus of their development on that support model.
- **Conditional access controls and policy enforcement are table stakes.** This is becoming a critical feature of UEM platforms. Conditional access controls what apps, data, or other resources a user can connect to and consume based on an array of factors, such as location (GPS location and network connectivity type) as well as the day, the end-user identity and role, and the state of or health of the device being used (from the standpoint of a jailbroken/rooted device or an operating system that is out of date).
- **Specialty-use Windows device scenarios — frontline worker, multiuser endpoints, field workers, and deskless workers — should be considered.** Windows endpoints operate in a wide range of roles beyond general end-user computing and productivity apps. Windows 11 PCs run retail POS terminals, digital signage, industrial control monitoring tools, self-service kiosks, and automatic teller machines (ATMs), among other use cases. CEM tools must be able to support management of devices across nontraditional use cases (e.g., beyond basic mobile computing: voice/video calls/meetings, email, calendar, messaging, and productivity tools).

- **Adjacencies and tie-ins to a strong portfolio of complementary IT/system infrastructure software products should be sought.** Solutions such as endpoint security, security and vulnerability management, identity, cloud access security brokers (CASBs), IT service management (ITSM), security information and event management (SIEM), network security, Windows server management, and line-of-business/vertical-specific application platforms are all important for Windows CEM vendor consideration. Since Windows CENM software does not operate in a vacuum, it is critical that vendors go to market either with complementary IT software product portfolios or with strong integrations and partnerships with key industry players.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Tanium

Tanium is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide client endpoint management software for Windows devices.

Founded in 2007, Tanium is an endpoint security and management vendor based in Kirkland, Washington. Its Converged Endpoint Management (XEM) platform focuses on managing and securing endpoints in large and midsize enterprise environments. The Tanium XEM platform provides real-time visibility, control, and remediation capabilities across a range of endpoints, including Windows, Mac, and Linux devices. Tanium's approach to endpoint management integrates with other with IT operations and security tools, promoting a unified strategy for managing risk and compliance. Tanium's decentralized client architecture and real-time data processing capabilities allow for in-depth visibility and control over Windows devices. The XEM platform's efficient patch management system can help organizations achieve high patch efficacy and reduce endpoint attack surfaces across a Windows device fleet. Device inventorying, configuration state, installed app monitoring, user account management, and other telemetry gathering functions can be executed from a single console. The product also works closely with Tanium's incident response, risk and compliance, and digital employee experience offerings, which combined, the vendor calls its Converged Endpoint Management suite.

On the DEX front, Tanium allows its extensive telemetry gathering and analysis capabilities to be used for monitoring end-user experiences with Windows devices, such as monitoring the performance, responsiveness, user feedback, and health of device hardware, Windows OS, app performance, and other measurements, which can affect how well users operate with Windows PCs. Tanium's agent-based product sets are available via on-premises deployments as well as cloud-based delivery.

Strengths

Tanium's XEM platform excels in real-time vulnerability management, sensitive data monitoring, and enforcing security policies across all endpoints. This tightly integrated management/security approach strongly aligns with how modern enterprises are supporting large deployments of Windows, with a focus on risk mitigation and operational efficiency. The products capabilities can also extend to Windows servers, as well as Mac, Linux, and some Unix client and server endpoints.

Tanium's monitoring capabilities can extend to the discovery and protection of sensitive data (structured file data pre-identified as sensitive, as well as identification of sensitive data types) across Windows endpoints, allowing for greater compliance and improved endpoint security posture.

Challenges

The comprehensive capabilities of XEM might present an adoption challenge for smaller enterprises or SMBs with limited IT resources. Integrating XEM into existing IT ecosystems can require an investment of IT practitioners' time for training and may require multiple modules from Tanium in order to realize the platform's full benefits.

Tanium's model for device deployment focuses more on traditional imaging and packaging and less on modern device management approaches. Future integration with services such as Microsoft Autopilot are on the company's road map and would help the company move toward modern device onboarding and management practices.

Consider Tanium When

Organizations with large deployments of Windows devices and enterprises with large, distributed workforces should consider Tanium for its strong integration of Windows endpoint device management and overall endpoint security. Tanium should appeal especially to modern enterprises with teams focused on improving their cyberhygiene, reducing risk, and lowering cost by converging endpoint device management and security operations.

Vendors to Watch

Every IDC MarketScape cycle results in vendors that do not qualify for inclusion in the study. For many vendors, either it is too early in their life cycle, they are undergoing product transitions, or they are simply too small. For this IDC MarketScape, there are the vendors to watch:

- **1E:** A London-based software provider, 1E makes IT infrastructure and CEM products focused on supporting and augmenting existing Windows endpoint device management tools or replacing them. The vendor also has a DEX solution and other employee experience tools.
- **baramundi software:** baramundi software is a Germany-based UEM vendor with a focus on automation and integration of endpoint device management with its portfolio of network management, IoT management, server management, and security products.
- **CrowdStrike:** This large enterprise endpoint security software vendor launched its first UEM product in March 2024, with capabilities for Windows, macOS, and Linux device enrollment, configuration management, and software patching, tied closely to the vendor's larger Falcon endpoint detection and response (EDR) platform, used widely by large enterprises.
- **Fleet:** Fleet is an open source endpoint management platform supporting Windows, macOS, and Linux and expanding to mobile device OSs in 2024. The data-centric platform is targeted at firms with large device fleets and provides APIs for automating software pushes to endpoints and the pulling of data from managed devices (for ingesting into SIEM or other analytics tools).
- **Kaseya:** A Miami-based IT systems software vendor, Kaseya has a broad set of IT products, including CEM, RMM, ITSM, and security management tools. The vendor primarily targets managed service providers that sell to SMBs and enterprises.
- **Scalefusion:** Headquartered in Pune, India, Scalefusion offers a cloud-based UEM platform that manages Windows, Mac, Android, iOS, and Linux endpoints. It provides reporting and

analytics features, security compliance templates, and other tools for SMB/midmarket IT organizations with large, mixed-OS device fleets.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Client endpoint management software and SaaS solutions provide change, configuration, compliance, asset tracking, and software distribution for clients, desktops, mobile devices, some IoT devices, and peripheral hardware and software assets, but not network devices, storage, or server systems.

LEARN MORE

Related Research

- *Five Trends to Watch in Endpoint Device Management in 2024* (IDC #US51763224, January 2024)
- *The Role of Client Endpoint Management Tools in Digital Employee Experience Monitoring* (IDC #US46460821, December 2023)

- *Worldwide Unified Endpoint Management Software Forecast, 2023-2027* (IDC #US47945922, July 2023)
- *IDC MaturityScape: Apple Device Management in the Enterprise 1.0* (IDC #US50671623, May 2023)
- *What's Behind the Windows/Mac Device Management Gap in the Enterprise?* (IDC #US50688223, May 2023)

Synopsis

This IDC study represents a vendor assessment of client endpoint management software for Windows endpoints through the IDC MarketScape model.

"It is still a Windows world when it comes to the primary endpoint computing tool used in most enterprises. Managing large fleets of enterprise Windows devices is not an easy chore," says Phil Hochmuth, research VP for Endpoint Device Management and Enterprise Mobility, IDC. "The stakes are high for both IT operations and security teams when it comes to the deployment, configuration, security, and life-cycle management of Windows endpoints. Client endpoint management tools focused on Windows must help IT and security teams ensure that workers' Windows environments are secure, compliant, usable, and productive."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice