Critical Capabilities for Unified Endpoint Management Tools

Published: 18 August 2020  ID: G00464162

Analyst(s): Chris Silva, Rich Doheny, Rob Smith, Manjunath Bhat, Dan Wilson

UEM tools are key to addressing mobile and traditional endpoints, maintaining continuity of end-user computing operations, and delivering seamless IT administration in the era of expanded remote work. This research helps I&O leaders evaluate UEM solutions based on the four most common use cases.

Key Findings

- Gartner’s research identified four common UEM use cases: enterprise PC management, compliance-driven management, role-based device management and unmanaged/BYO.
- Organizations struggling with traditional, network-dependent PC management tools have driven a new wave of interest and investment in UEM tools’ potential to augment or displace the tools currently managing Windows devices.
- To highlight the emerging integration of UEM and unified endpoint security (UES) tools, security capabilities and integrations are given consideration in evaluations, with its highest weight in the compliance-driven management use case.
- Investments in frontline/first-line worker technology deployments represent a growing portion of the IT innovation budget. Gartner added the role-based or role-specific use-case devices for 2020.

Recommendations

I&O leaders responsible for digital workplace infrastructure and operations who are evaluating UEM tools should:

- Enable an increasingly remote workforce by migrating traditional devices — most notably, Windows PCs — into a UEM tool using modern management to improve agility and scalability.
- Consult the unmanaged/BYO use case as a starting point to evaluate these solutions’ fit to address an increase in personal device usage in response to remote work demands.
Avoid the need for additional investment by evaluating vendors based on their performance in relevant use cases. The best all-around solution may not be a fit for more specific needs.

Closely examine macOS and Windows 10 modern management capabilities and a UEM’s ability to support migration from legacy CMT to UEM in use cases where legacy or platform-specific tools will be replaced by UEM.

What You Need to Know

The analysis of the UEM market balances the importance of mobile and PC management, treating the importance of both equally. Gartner has added weight to the management of traditional endpoints, such as macOS and Windows devices, as this use case has increased in importance to buyers. This reflects increased demand for co-management and modern PC management to enable an increasingly remote workforce.

Management alone of endpoint devices is rarely enough to identify and mitigate security issues, such as data leakage and device compromise, and to provide monitoring and alerting. The increased focus on analytics and endpoint security capabilities in this analysis emerges as more buyers demand deeper security capabilities and a strong link between endpoint management and endpoint security tools.

Gartner predicts that growth in IT spending specific to frontline/first-line worker use cases, paired with the aging of existing role-specific devices, will drive interest in using UEM to consolidate and simplify endpoint management.
Analysis

Critical Capabilities Use-Case Graphics

Figure 1. Vendors’ Product Scores for the Compliance-Driven Management Use Case

Product or Service Scores for Compliance-Driven Management

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>3.74</td>
</tr>
<tr>
<td>IBM</td>
<td>3.48</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>3.43</td>
</tr>
<tr>
<td>Microsoft</td>
<td>3.33</td>
</tr>
<tr>
<td>Citrix</td>
<td>3.04</td>
</tr>
<tr>
<td>MobileIron</td>
<td>2.99</td>
</tr>
<tr>
<td>Sophos</td>
<td>2.80</td>
</tr>
<tr>
<td>Ivanti</td>
<td>2.65</td>
</tr>
</tbody>
</table>

As of 13 August 2020

Source: Gartner (August 2020)
Figure 2. Vendors' Product Scores for the Enterprise PC Management Use Case

Product or Service Scores for Enterprise PC Management

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>3.94</td>
</tr>
<tr>
<td>Microsoft</td>
<td>3.83</td>
</tr>
<tr>
<td>IBM</td>
<td>3.75</td>
</tr>
<tr>
<td>Ivanti</td>
<td>3.32</td>
</tr>
<tr>
<td>MobileIron</td>
<td>3.26</td>
</tr>
<tr>
<td>Citrix</td>
<td>3.18</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>2.64</td>
</tr>
<tr>
<td>Sophos</td>
<td>2.43</td>
</tr>
</tbody>
</table>

As of 13 August 2020

Source: Gartner (August 2020)

Figure 3. Vendors' Product Scores for the Role-Based Device Management Use Case

Product or Service Scores for Role-Based Device Management

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>3.80</td>
</tr>
<tr>
<td>IBM</td>
<td>3.42</td>
</tr>
<tr>
<td>Citrix</td>
<td>3.00</td>
</tr>
<tr>
<td>MobileIron</td>
<td>2.93</td>
</tr>
<tr>
<td>Microsoft</td>
<td>2.91</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>2.88</td>
</tr>
<tr>
<td>Ivanti</td>
<td>2.84</td>
</tr>
<tr>
<td>Sophos</td>
<td>2.22</td>
</tr>
</tbody>
</table>

As of 13 August 2020

Source: Gartner (August 2020)
Vendors

**BlackBerry**

BlackBerry continues to demonstrate strength in securely delivering apps and data on managed and unmanaged mobile devices. BlackBerry Access workspace can provide users access to Dynamics-enabled apps, virtual apps and desktops (via its Awingu partnership), positioning the BlackBerry Digital Workplace as a viable alternative to a company-managed device.

BlackBerry UEM lags competing solutions by offering only basic macOS and Windows 10 management capabilities. Its UEM is ideal for organizations seeking robust control over apps and data consumed on BYO and unmanaged devices and those with complex security and compliance needs.

BlackBerry remains strong in the unmanaged/BYO and compliance-driven use cases.

**Citrix**

Citrix offers broad support for OS-native and OEM-specific endpoint management capabilities, leading to strong performance in the role-based device management use case. Citrix offers a solid
UEM product that lacks standout capabilities beyond its branded PIM client and other managed apps, used on unmanaged devices and in BYOD use cases.

The vendor has made changes to support for MDX-enabled applications on shared iOS devices and remote-control capabilities, both of which play a central role in many frontline use cases. The company’s on-premises UEM option remains attractive for regulated industry buyers that have existing Citrix investments.

Citrix demonstrates strength in the role-based device management use case and offers average capabilities in other use cases.

IBM

IBM’s positioning in the role-based device management use case is anchored by the ability to manage multiple mobile and PC OSs, OEM-specific devices and those running Linux (including Raspberry Pi). The company’s PIM client and workspace applications offer strong support for key enterprise features (editing and light content creation).

IBM demonstrates enterprise-class UEM capabilities but is viewed by many buyers as a solid midmarket product. Its lack of on-premises deployment makes the IBM offering a challenge for some regulated customers. The sale of BigFix limits its included CMT capabilities, though MaaS360 can integrate with Microsoft Endpoint Configuration Manager, HCL Big Fix, and Tanium and offers modern management of macOS and Windows.

IBM shows strength in the enterprise PC management and compliance-driven management use cases.

Ivanti

Ivanti offers rich integration of CMT functionality in its on-premises and/or SaaS-based UEM tool. The UEM offering provides rich patch management and delivery, management of nontraditional devices and platforms, and deep integrations to ITSM tools.

Ivanti’s robust discovery and insights (based on analytics) show the vendor innovating in key areas outside core UEM. As of this analysis, Ivanti lags competition in mobile device management capabilities.

Ivanti demonstrates strength in the enterprise PC management use case, in keeping with its client base’s continued demand for traditional PC management.

Microsoft

Microsoft continues to gain buyers’ interest due to its unique capabilities on PC co-management and management of its Microsoft Office mobile apps. Its capabilities to protect content in managed mobile and desktop apps built with the Intune SDK increases Microsoft consideration, even in organizations using a competing MDM or UEM tool “of record.”
Microsoft retains the unique ability to co-manage Windows 10 devices and enable app protection policies in its mobile apps without device enrollment, which provide Microsoft material differentiation for Microsoft Endpoint Manager in use cases where a mix of classic and modern management capabilities are desired. Buyers note that Endpoint Manager includes many dependencies on other infrastructure, such as Azure Active Directory, citing the increased investment required to gain those features if Microsoft 365 licenses are not already in place.

Microsoft offers a strong solution for enterprise PC management and unmanaged/BYO device management.

**MobileIron**

MobileIron continues to offer a broad, deep set of capabilities in managing various mobile platforms as well as macOS and Windows 10 modern management, though it lacks robust CMT capabilities or third-party integration.

MobileIron has made investments in functions to serve frontline users and investments in its management of macOS. A major focus for MobileIron has been development of passwordless authentication for users on managed and unmanaged devices, and integration of third-party and native security capabilities.

MobileIron offers good capabilities in the role-based device management and enterprise PC management use cases.

**Sophos**

Sophos demonstrates continued investment in the endpoint management space to accompany and strengthen existing features aimed at combining endpoint security and endpoint management tooling in a single console.

Sophos has a robust MDM policy support and identity and access management features. Sophos offers limited modern PC management and lacks rich traditional endpoint management functionality in the tool. The vendor’s acquired IP in the endpoint detection and response space has given it a small lead in the use of endpoint security triggers for dynamic UEM policy.

Sophos shows strength in the compliance-driven management use case due to the strong links between its endpoint security and endpoint management offerings.

**VMware**

VMware’s well-rounded UEM offering features robust support for mobile and PC endpoints. VMware has continued to maintain investments in OEM-specific management functions and a broad support for nontraditional devices, including wearable devices used in frontline worker contexts.

The vendor has continued its investment in managing role-based devices through Workspace ONE Assist (remote support technology acquired from Aetherpal), making it one of the few vendors in this market that owns the remote control IP. Despite continued investments in AirLift to help IT admins
migrate to modern management, Gartner clients report mixed results in the tool’s ability to smooth the transition of PCs from classic to modern management.

VMware leads in the compliance-driven management, enterprise PC management and role-based device management use cases.

Context

Each use case emphasizes a set of capabilities in the tool, with weightings adjusted in each case relative to the importance of that set of capabilities to support it. Gartner presents four use cases for the 2020 Critical Capabilities for unified endpoint management tools, evaluating the appropriateness of the tool to address each of the four use cases defined in this research.

Product/Service Class Definition

Gartner’s view of the market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

Gartner defines the UEM tools market as a set of offerings that is composed of mobile device management (MDM) and personal computers, via traditional client management technology (CMT) or modern management, through a single console that combines the application of data protection, device configuration and usage policies. Modern UEM tools:

- Provide a user-centric view of devices across device platforms.
- Enable modern PC management through native Windows 10 and macOS.
- Enable mobile device management through native iOS and Android controls.
- Aggregate analytics and telemetry from users, apps and devices to help inform policy and related actions.
- Provide insights into user experience through aggregation of telemetry signals, events, logs and synthetic transactions.
- Integrate with unified endpoint security (UES) tools to support security policy management, execute administrative actions, and improve integration with identity and access management (IAM) tools.

Additionally, UEM offers direct management of nontraditional devices, including IoT devices and wearables. However, Gartner does not deem these extensions to be core to the market.

Critical Capabilities Definition

Application and Content Management

This evaluates the distribution and management of native and virtual applications for mobile and PC, the ability to provide stand-alone management for applications on unmanaged devices, and
application and data containment. Includes capabilities to segregate or isolate personal and corporate data.

CMT Features
This capability includes the existence of CMT-related features (for example, imaging and centralized patch management) natively in the tool, third-party CMT integration, and other features aimed at supporting CMT migration processes.

Endpoint Analytics
This capability includes the identification, collection, and aggregate analytics and telemetry from users, apps and devices into the UEM tool to help inform policy, automation and related actions.

Light/Zero-Touch Enrollment
This capability focuses on support for Microsoft Autopilot, Apple Device Enrollment, Android Enterprise Zero Touch, OEMConfig, or similar enrollment and provisioning.

Modern Management
Capabilities to directly manage, with or without an agent, the native controls of Microsoft Windows 10 and Apple macOS via MDM enrollment. This also includes the migration of GPOs and automated provisioning.

Nonstandard Endpoints
This capability includes the ability to configure, deploy and manage wearables and rugged devices with OEM-specific management in the UEM tool.

Unified Endpoint Security
This capability focuses on the tool’s features to support integration with identity and access infrastructure, endpoint detection and response, mobile threat defense, and AI/ML to support dynamic policy and contextual access as well as novel authentication methods.

User Support Technologies
This capability includes capabilities to enable remote viewing and control to endpoints and chatbots or digital assistants.

Virtualization Support
This capability includes, among other functions, integration with or support for delivering virtualized app or desktop workloads.
Use Cases

**Compliance-Driven Management**
Capabilities in this use case include the enforcement of regulatory and legal controls.

This includes the creation of controls and reporting of compliance with regulatory and legal requirements and certifications for a given vertical industry, geography or market. The vendors’ approaches to compliance with user-centric privacy regulations are also evaluated.

**Enterprise PC Management**
Capabilities in this use case include modern management of Windows and macOS.

This also guides the migration from legacy client management to modern management, and the enabling of co-management or coexistence with an integrated or third-party CMT. This also includes the use of analytics to inform policy and administrative priorities.

**Role-Based Device Management**
Capabilities in this use case focus on managing nontraditional devices.

This includes devices with limited functionality or utility, a simplified app launcher or dedicated home screens, delivery of native or virtual applications, configuration of devices and OSs, remote visibility for support personnel, and enabling of hands-free workflows.

**Unmanaged/BYO**
Capabilities in this use case include the application of data protections and policy on devices lacking or unable to support a local agent or device management profile.

This also considers the security, privacy and user experience offered on personal devices being used for work tasks. This includes segregation or isolation of personal and corporate data.

**Vendors Added and Dropped**

**Added**
No vendors were added to this year’s Critical Capabilities research.

**Dropped**
The following vendors were dropped from this year’s research:

- 42Gears
- ManageEngine
Inclusion Criteria

This Critical Capabilities makes use of the same inclusion criteria as the related “Magic Quadrant for Unified Endpoint Management.”

To qualify for inclusion, vendors need to present a defensible solution capable of the following:

- A currently shipping, single license product that demonstrates:
  - Mobile device management
  - Apple (iOS and iPad OS)
  - Android (including Android Enterprise)

- Modern Management of Apple macOS and Windows 10, which includes:
  - Device enrollment and provisioning (Microsoft Autopilot and Apple DEP)
  - Device management
  - Application management and deployment in native format
  - Continuous OS updates (enforce/defer OS updates)
  - Direct inclusion of CMT capabilities or integration with third-party CMT
  - Capability to directly support migration from CMT to modern management
  - Direct integration with the Microsoft Intune Graph API for app and data protection

- Provide evidence of a UEM product currently managing at least 10,000,000 devices

- The product must be available as a SaaS-based deployment, regardless of other deployment methods (such as on-premises)
### Table 1. Weighting for Critical Capabilities in Use Cases

<table>
<thead>
<tr>
<th>Critical Capabilities</th>
<th>Compliance-Driven Management</th>
<th>Enterprise PC Management</th>
<th>Role-Based Device Management</th>
<th>Unmanaged/BYO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application and Content Management</td>
<td>20%</td>
<td>5%</td>
<td>7%</td>
<td>50%</td>
</tr>
<tr>
<td>CMT Features</td>
<td>8%</td>
<td>20%</td>
<td>5%</td>
<td>0%</td>
</tr>
<tr>
<td>Endpoint Analytics</td>
<td>5%</td>
<td>10%</td>
<td>5%</td>
<td>12%</td>
</tr>
<tr>
<td>Light/Zero-Touch Enrollment</td>
<td>2%</td>
<td>20%</td>
<td>15%</td>
<td>0%</td>
</tr>
<tr>
<td>Modern Management</td>
<td>10%</td>
<td>25%</td>
<td>10%</td>
<td>0%</td>
</tr>
<tr>
<td>Nonstandard Endpoints</td>
<td>5%</td>
<td>0%</td>
<td>30%</td>
<td>10%</td>
</tr>
<tr>
<td>Unified Endpoint Security</td>
<td>35%</td>
<td>5%</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>User Support Technologies</td>
<td>0%</td>
<td>5%</td>
<td>10%</td>
<td>8%</td>
</tr>
<tr>
<td>Virtualization Support</td>
<td>15%</td>
<td>10%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

As of August 2020

Source: Gartner (August 2020)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

**Critical Capabilities Rating**

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).
### Table 2. Product/Service Rating on Critical Capabilities

<table>
<thead>
<tr>
<th>Critical Capabilities</th>
<th>BlackBerry</th>
<th>Citrix</th>
<th>IBM</th>
<th>Ivanti</th>
<th>Microsoft</th>
<th>MobileIron</th>
<th>Sophos</th>
<th>VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application and Content Management</td>
<td>4.5</td>
<td>3.5</td>
<td>3.3</td>
<td>2.5</td>
<td>4.0</td>
<td>3.5</td>
<td>3.0</td>
<td>3.4</td>
</tr>
<tr>
<td>CMT Features</td>
<td>1.8</td>
<td>3.1</td>
<td>4.3</td>
<td>4.5</td>
<td>4.7</td>
<td>2.2</td>
<td>1.5</td>
<td>3.1</td>
</tr>
<tr>
<td>Endpoint Analytics</td>
<td>3.2</td>
<td>3.0</td>
<td>3.7</td>
<td>3.2</td>
<td>3.0</td>
<td>2.8</td>
<td>3.3</td>
<td>4.0</td>
</tr>
<tr>
<td>Light/Zero-Touch Enrollment</td>
<td>2.8</td>
<td>3.0</td>
<td>3.4</td>
<td>3.0</td>
<td>4.0</td>
<td>4.0</td>
<td>2.8</td>
<td>4.1</td>
</tr>
<tr>
<td>Modern Management</td>
<td>2.5</td>
<td>3.2</td>
<td>4.0</td>
<td>4.0</td>
<td>4.2</td>
<td>4.2</td>
<td>2.5</td>
<td>4.4</td>
</tr>
<tr>
<td>Nonstandard Endpoints</td>
<td>2.9</td>
<td>2.8</td>
<td>3.0</td>
<td>2.8</td>
<td>1.5</td>
<td>2.3</td>
<td>1.2</td>
<td>3.5</td>
</tr>
<tr>
<td>Unified Endpoint Security</td>
<td>4.0</td>
<td>2.0</td>
<td>3.5</td>
<td>2.5</td>
<td>3.0</td>
<td>2.8</td>
<td>4.0</td>
<td>3.4</td>
</tr>
<tr>
<td>User Support Technologies</td>
<td>2.0</td>
<td>2.0</td>
<td>4.0</td>
<td>2.9</td>
<td>2.8</td>
<td>2.5</td>
<td>3.2</td>
<td>3.5</td>
</tr>
<tr>
<td>Virtualization Support</td>
<td>2.5</td>
<td>4.8</td>
<td>3.0</td>
<td>1.0</td>
<td>2.5</td>
<td>2.5</td>
<td>1.0</td>
<td>4.8</td>
</tr>
</tbody>
</table>

As of August 2020

Source: Gartner (August 2020)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.
### Table 3. Product Score in Use Cases

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>BlackBerry</th>
<th>Citrix</th>
<th>IBM</th>
<th>Ivanti</th>
<th>Microsoft</th>
<th>MobileIron</th>
<th>Sophos</th>
<th>VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance-Driven Management</td>
<td>3.43</td>
<td>3.04</td>
<td>3.48</td>
<td>2.65</td>
<td>3.33</td>
<td>2.99</td>
<td>2.80</td>
<td>3.74</td>
</tr>
<tr>
<td>Enterprise PC Management</td>
<td>2.64</td>
<td>3.18</td>
<td>3.75</td>
<td>3.32</td>
<td>3.83</td>
<td>3.26</td>
<td>2.43</td>
<td>3.94</td>
</tr>
<tr>
<td>Role-Based Device Management</td>
<td>2.88</td>
<td>3.00</td>
<td>3.42</td>
<td>2.84</td>
<td>2.91</td>
<td>2.93</td>
<td>2.22</td>
<td>3.80</td>
</tr>
<tr>
<td>Unmanaged/BYO</td>
<td>3.73</td>
<td>3.23</td>
<td>3.36</td>
<td>2.50</td>
<td>3.28</td>
<td>3.05</td>
<td>2.77</td>
<td>3.63</td>
</tr>
</tbody>
</table>

As of August 2020

Source: Gartner (August 2020)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

**Gartner Recommended Reading**

*Some documents may not be available as part of your current Gartner subscription.*

“How Products and Services Are Evaluated in Gartner Critical Capabilities”

“Magic Quadrant for Unified Endpoint Management”

“Prepare for Unified Endpoint Management to Displace MDM and CMT”

“Adopt Continuous Endpoint Engineering and Modern Management to Ensure Digital Workplace Success”

“Essential Considerations When Choosing Separate PC and Mobile Management Tools”

“Solution Comparison for Unified Endpoint Management Systems”

“Mobile OSs and Device Security: A Comparison of Platforms”

“The Cost Argument for Supporting Android Enterprise Recommended Devices”

---

**Critical Capabilities Methodology**

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance.
for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved
2 = Fair: some requirements are not achieved
3 = Good: meets requirements
4 = Excellent: meets or exceeds some requirements
5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. It consists of the opinions of Gartner’s research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see “Guiding Principles on Independence and Objectivity.”