Managing Generative AI's Impact on Endpoint Management

Published 15 November 2023 - ID G00803412 - 23 min read

By Analyst(s): Timon Watson

Initiatives: Digital Workplace and CRM for Technical Professionals

As demand for Generative AI grows, technical professionals responsible for endpoint management must be prepared to support their organization's pilot and adoption programs. This research will provide pragmatic advice on how to prepare for the impact of Generative AI on endpoint management.

Overview

Key Findings

- Generative AI (GenAI) pilot and adoption programs place increased demands on the core competencies of endpoint management teams — particularly for application, device and operating system life cycle management.

- GenAI assistants in Unified Endpoint Management (UEM) tools will provide richer insights and operational efficiencies, but increase the risk of inexperienced administrators making mistakes.

- The pace of AI adoption in the broader organization will likely outpace its inclusion in UEM tools, meaning that IT teams must use the tools they have at their disposal now and not wait for future functionality to address increased demand for their services.

- If not properly scrutinized by a competent administrator, AI-generated insights or content, such as scripts, may be inaccurate, unoptimized or produce unexpected results.

Recommendations

- Use Gartner's Continuous Endpoint Engineering (CEE) approach to manage increased demands on endpoint management teams and accelerate update cadence.
- Protect your environment from operational disruption caused by AI-augmented actions or created content by establishing GenAI usage policies, ongoing monitoring and good governance practices (i.e., change management, deployment rings and RBAC controls) within your UEM tool.
- Ensure that your applications are on the latest versions and reduce the administrative burden by using trusted application update services like the Microsoft Windows store or third-party application update services.
- Adopt a "distrust and verify approach" to Generative AI by restricting its access within the UEM tool and having an expert user review insights and content created by AI for accuracy and impact before being used in production environments.

Analysis

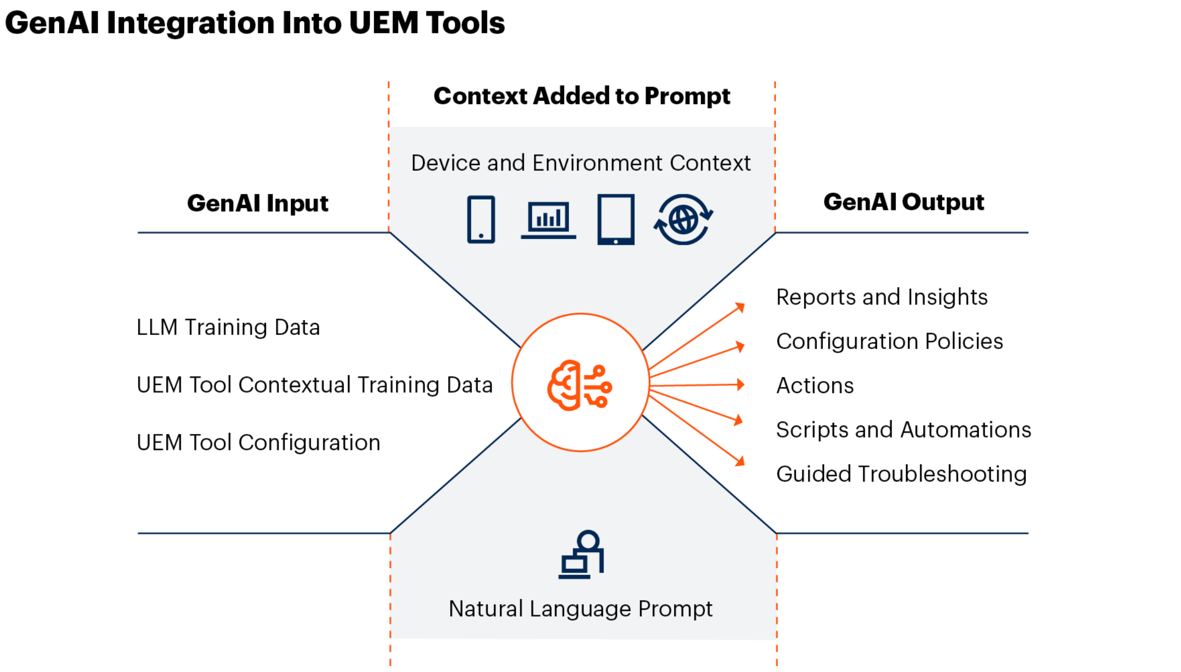
Generative AI (GenAI) is now a top priority for digital workplace leaders due to its potential to enhance operational efficiency and productivity. [1] The impact that Generative AI will have on endpoint management operations is twofold:

- GenAI integration into UEM tools promises to deliver richer insights and operational efficiencies at the cost of increased operational risk.
- GenAI adoption will place additional pressure on core device management competencies.

AI is adept at identifying patterns and anomalies in datasets and taking actions based on programmed behaviors. Endpoint management technologies, such as UEM and Digital Employee Experience (DEX) tools have incorporated various AI techniques for several years. GenAI is different from past AI approaches. GenAI can interpret natural language instructions called prompts to generate entirely new content based on its learning from the training data, or based on data supplied with the prompt.

In the context of endpoint management, GenAI will provide natural language interfaces into endpoint management tools to create configuration policies, content like actions and scripts, and new ways to interrogate device-related data for insights (see Figure 1). GenAI is a significant step toward what Gartner calls Autonomous Endpoint Management (AEM) when combined with other AI approaches. Gartner originally predicted that UEM would evolve into AEM around 2027. With the rapid evolution of GenAI, AEM may be available sooner than predicted, but this level of autonomy has yet to be realized.

Figure 1: GenAI Integration Into UEM Tools



Source: Gartner
803412_C

For example, DEX tools use AI to identify an anomaly in the data or device operation, such as an application crash, and respond with a preprogrammed action using non-GenAI techniques. However, this use of AI cannot create the action itself, but GenAI can. In the future when we have reached AEM, GenAI will dynamically create an action and perhaps trigger the necessary action for the AI based on its training data. In addition, GenAI could create a summary of the incident, document the action, raise an associated incident and change records in the ITSM tool — all in natural language.

GenAI's integration with endpoint management tools is still in its early stages, and will potentially have positive and negative impacts. This research will examine its implementation in adjacent technologies, such as office productivity suites and use cases like software development. Based on what GenAI can do today — and what current development appears to be offering in the near future — technical professionals should adjust their operations to support their organization's GenAI initiatives.

The Impact of Generative AI Integration Into UEM Tools

This section examines the potential benefits and risks that GenAI will introduce to UEM tools in the short term. The examples given are based on the capabilities we can anticipate in the near future and do not make any long-term speculative predictions of future capabilities. Guidance is provided on how to manage the risks, so the benefits of GenAI can be safely realized.

Benefits of GenAI Integration

GenAI will become a standard feature in UEM tools, with most providers planning to include GenAI methods at various places in their product roadmaps. Though the full benefits that GenAI integration into UEM tools promises are yet to be realized, we can look to its integration into adjacent technologies to anticipate the potential benefits it can bring today (see Figure 1).

Natural Language Interfaces Simplify Complex Device Management Workflows

A natural language interface will be the initial use case for GenAI integration into UEM tools through an integrated assistant or chatbot. Instead of referring to the documentation, a query is directed to an integrated AI assistant. For example:

How do I block access to removable USB storage devices?

In response, the AI assistant returns guidance on how this can be accomplished and where to find the necessary settings within the UI to both configure and apply the policy. As well as retrieving information, GenAI can create artifacts like configuration policies. The AI assistant will ask if it should create the required policy on your behalf after providing guidance.

Microsoft demonstrated this functionality in Microsoft 365 Copilot, with Copilot creating Microsoft PowerPoint presentations from simple instructions. [2] Although this functionality is impressive, it uses the product's existing capabilities and effectively automates mouse clicks. The user can create the same content, but it would take significantly more time and may require expert knowledge to replicate the content produced by the AI.

Consider a scenario where a critical vulnerability has been discovered in a widely used application for an example of how this capability could impact device management operations. The endpoint administrator asks the AI assistant to do the following:

> *Identify all devices with the affected application version. Update the application to version XX, prioritizing the devices used by the finance department and leadership team. Block access to the application and corporate resources from the device until the application has been updated.*

This is a complex request, requiring multiple actions and multiple policies (see Figure 2).

1. The impacted devices must be identified and correlated with the primary user and their department.

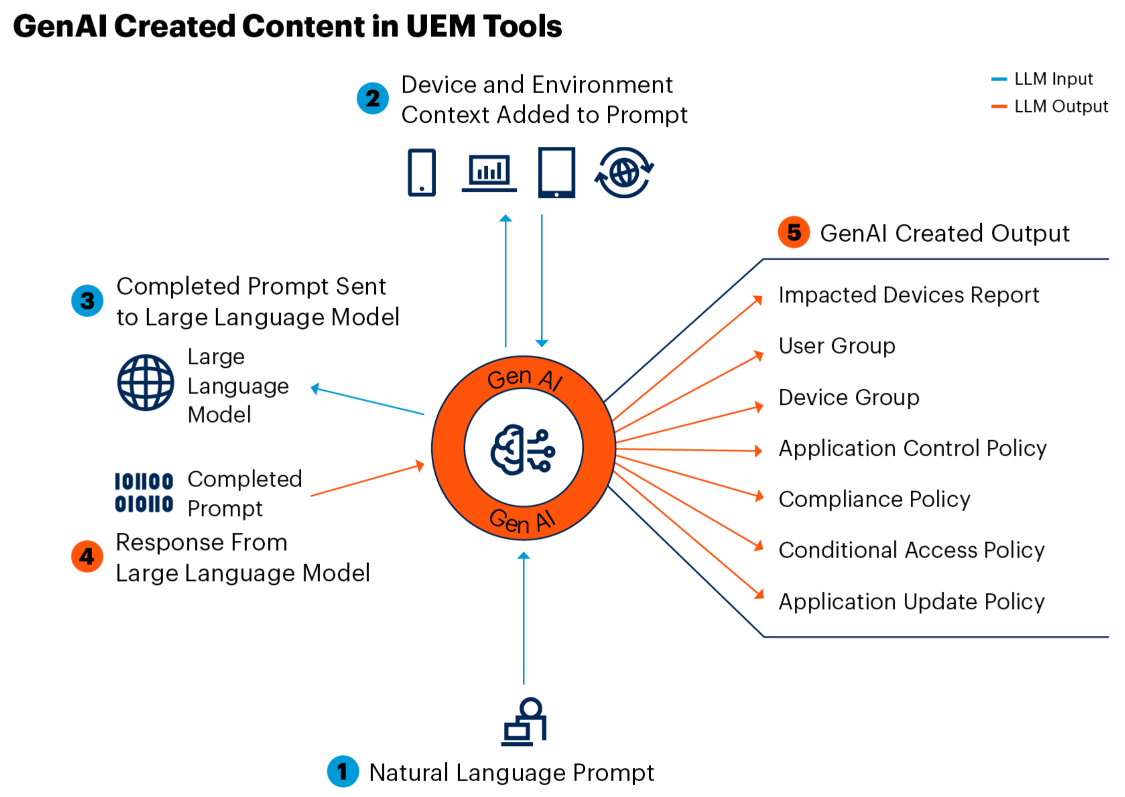
2. A method must be devised to target the policies to the impacted devices and users.

3. A policy must be created to block access to the impacted application version.

4. Conditional access and compliance policies must be created to block access to company resources from an impacted device.

5. A policy must be created to update the application.

Figure 2: GenAI Created Content in UEM Tools


GenAI Created Content in UEM Tools
LLM Input
LLM Output
2 Device and Environment Context Added to Prompt
3 Completed Prompt Sent to Large Language Model
Large Language Model
Completed Prompt
4 Response From Large Language Model
Gen AI
Gen AI
5 GenAI Created Output
Impacted Devices Report
User Group
Device Group
Application Control Policy
Compliance Policy
Conditional Access Policy
Application Update Policy
1 Natural Language Prompt

Source: Gartner
803412_C

The potential impact of GenAI in this scenario is significant. Sophisticated endpoint management operations that would typically require the input of an expert and be time-consuming to complete would be accessible to all endpoint administrators. GenAI would dramatically reduce the time needed to respond to emerging threats, streamline complex changes and increase the agility of endpoint management teams.

GenAI Makes Advanced Reporting and Analytics More Accessible

The demonstration of Microsoft 365 Copilot showed how GenAI can analyze raw data in Microsoft Excel to produce insights and identify trends. Reporting and analytics are essential elements of endpoint management, but the breadth and depth of the inbuilt reporting in UEM tools can be insufficient to meet the needs of endpoint management teams. It is common practice for organizations to extend the native reporting through integrations with Business Intelligence (BI) or third-party reporting tools. Embedded GenAI assistants will enable insights to be produced dynamically from human language input, removing the need for additional reporting tools. For example:

"Which Android and Apple's iOS versions are the registered BYO devices using?"

"How many devices across all platforms have not installed the latest OS patches?"

"Which three applications crash the most on Windows 10?"

"Do the devices with the most application crashes share any characteristics?"

AI can identify and summarize trends and patterns in the data that, if performed manually, would require in-depth analysis and correlation between multiple reports. Using its ability to create new content, GenAI can generate reports from the data in areas that administrators may not have even considered, providing insights and natural language summarization beyond the scope of the precanned reports included in the tool. The dynamism this brings enables ad hoc reporting based on any attribute or parameter the endpoint administrator chooses.

GenAI Augmented Troubleshooting Improves Incident Resolution Times and Knowledge Capture

Troubleshooting application and device performance or stability issues is a time-consuming process. GenAI can accelerate this through its ability to look for and correlate key information from all relevant data sources. This could include data from device, application, UEM and authentication logs to produce a report, summary or suggested action.

Microsoft Security Copilot has demonstrated how GenAI can highlight significant events and underlying trends related to an incident in a natural language summary. [3] In endpoint management, the AI could translate error codes and event IDs into human language and incorporate information from knowledge base articles or known issues to either provide a resolution or suggest the next steps in the summary. Once the incident is resolved, GenAI can create or update knowledge base articles, associated documentation and ITSM objects, such as tickets, change and problem records.

GenAI Helps Generation of New Scripts and Understanding Existing Scripts

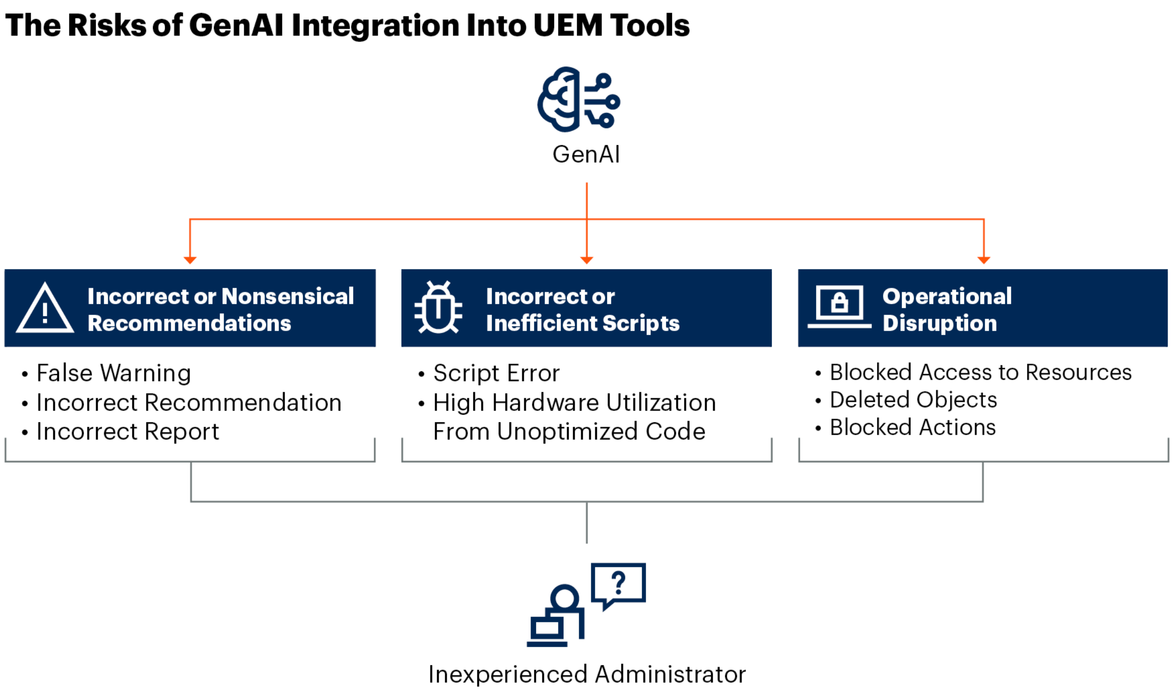
Scripting is an essential endpoint management skill to orchestrate complex application installations and automate repetitive actions. Code generation is a common use case for GenAI, with automated script creation being an early inclusion into UEM tools. GitHub Copilot and Amazon CodeWhisperer demonstrate GenAI's ability to create code from human language prompts. GenAI, in UEM tools, will enable automated or augmented assistance when creating scripts or tool-specific low-code automation, reducing the dependencies on expert users.

Microsoft Security Copilot demonstrated how GenAI could reverse engineer scripts or automation to provide a diagram or simple explanation of their function to people unfamiliar with the scripting language. Maintaining scripts and low code automations can be challenging, and GenAI will simplify troubleshooting, documentation and provide visibility into opaque processes for novice endpoint administrators.

The Risks That GenAI Integration Brings to Endpoint Operations

The appeal of GenAI integration into UEM tools is obvious. GenAI potentially addresses the challenges and needs of endpoint management teams: visibility and insight into their environment, automated, proactive remediation and mitigation for ongoing skills shortages. However, GenAI introduces risks that could cause operational disruption (see Figure 3).

Figure 3: The Risks of GenAI Integration Into UEM Tools



The Risks of GenAI Integration Into UEM Tools

GenAI

Incorrect or Nonsensical Recommendations

- False Warning
- Incorrect Recommendation
- Incorrect Report

Incorrect or Inefficient Scripts

- Script Error
- High Hardware Utilization From Unoptimized Code

Operational Disruption

- Blocked Access to Resources
- Deleted Objects
- Blocked Actions

Inexperienced Administrator

Source: Gartner
803412_C

Gartner

GenAI Produces Incorrect or Nonsensical Recommendations

Inaccurate or incorrect responses from GenAI have been the focus of much attention in the press. Known as hallucinations, they are an artifact of how GenAI and Large Language Models work. GenAI uses a probabilistic approach to predict the correct response; in simple terms, it makes a best guess of the paragraph of text that the user expects. Large and accurate datasets provide the highest probability of an accurate response. When the AI has limited data to base its response, its guess is more likely to be inaccurate, clearly wrong or even nonsensical.

It is impossible to predict how hallucinations will manifest in UEM reporting, but Microsoft called out a hallucination in their Security Copilot demo, where the Copilot referenced Windows 9, a nonexistent OS. Similar hallucinations could see phantom applications, incorrect application versions or nonexistent device models appearing in UEM reports.

GenAI Produces Incorrect or Inefficient Scripts

Hallucinations can also impact code or scripts created by Generative AI. Scripts may contain errors, causing the scripts to fail. Generative AI will produce precisely what is asked of it. Generated scripts may carry out the requested action, but it may perform inefficiently, requiring more resources to run than necessary or produce correct output that is incomprehensible without formatting. Specific instructions and script syntax examples improve the code quality created by GenAI, meaning it works best when augmenting the skills of an experienced script writer.

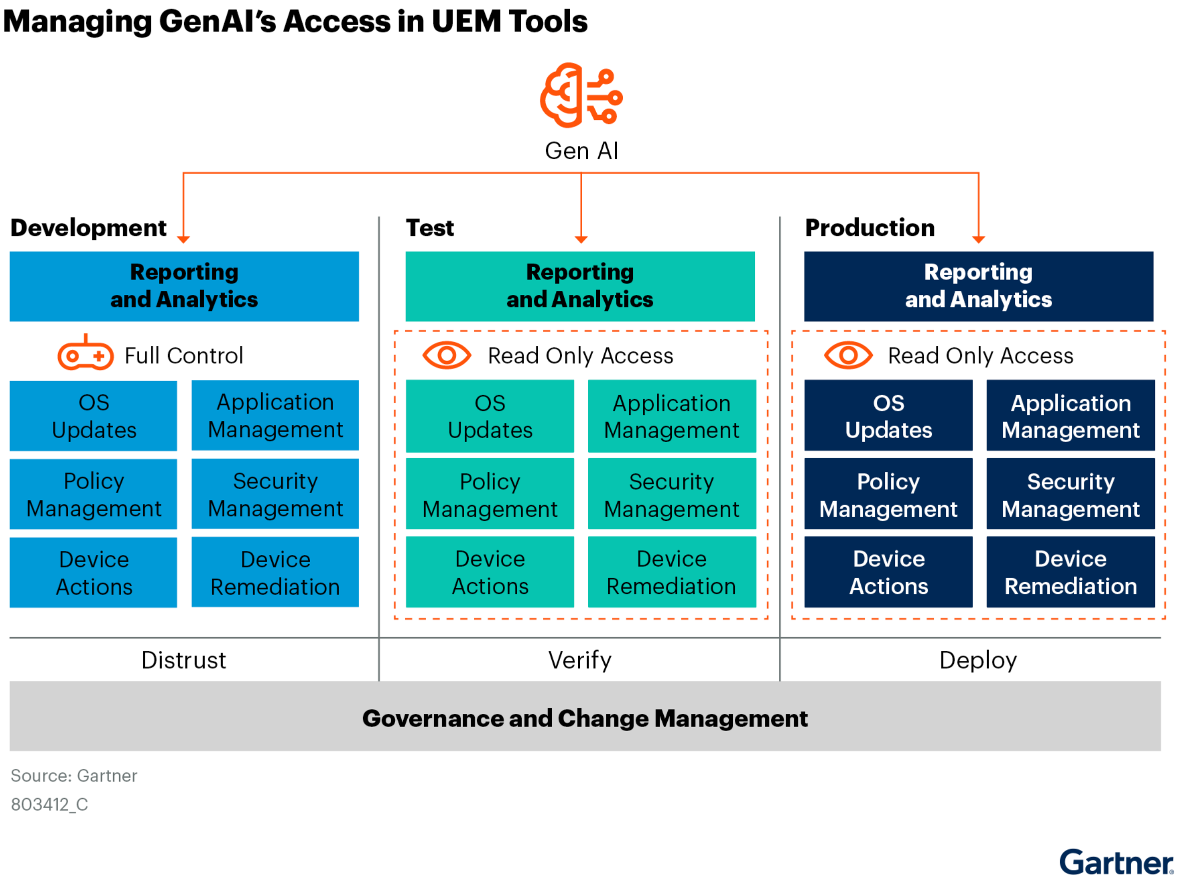
Sophisticated Endpoint Administration Operations Are Universally Accessible

GenAI's greatest benefit to endpoint management introduces its greatest operational risk. Democratizing the ability to carry out sophisticated operations like scripting or creating a series of policies to meet complex requirements mitigates skills gaps and increases agility. However, novice endpoint administrators may lack the skills or experience to identify errors in the AI-generated artifacts, or accurately assess the impact of created actions and policies.

How to Safely Use GenAI

The risks associated with GenAI can be managed through ITSM best practices and by applying good governance within the UEM tool. Restricting the permissions and scope of the AI, as you would with any employee, creates a sandboxed environment where it can be used safely (see Figure 4). Where GenAI is used heavily for the creation and management of scripts and low code automations follow Software Development Life Cycle (SDLC) best practices for version control, testing and deployment.

Figure 4: Managing GenAI's Access in UEM Tools



Source: Gartner
803412_C

Adopt a Distrust and Verify Approach to GenAI

GenAI-created artifacts must be reviewed by an endpoint administrator with the appropriate experience to verify their accuracy and impact. GenAI is a tool to augment existing skills; it does not replace experienced personnel.

Develop GenAI Skills

The quality of GenAI's response is dependent on the quality of the request. Ambiguous prompts place too much reliance on the AI's interpretation, leading to inconsistent and incorrect results. Test and validate prompts during GenAI pilots to define effective prompt structure and usage. Use this to implement internal prompt training for endpoint administrators and develop best practices for how to interact with the AI, such as breaking down complex requests into a series of detailed, well-defined instructions.

Enforce Good Governance Standards

It is imperative to have good GenAI governance standards in place before using GenAI in UEM tools. Restricting the AI is far easier when all elements in the UEM tool are easily identifiable and logically segmented. The following are examples of good governance practices.

- **Naming Convention:** All elements in the UEM tool (i.e., applications, devices, policies) must follow a clear and logical naming convention that quickly identifies their purpose.
- **Groups and Filters:** Devices and policy sets must be logically segmented through the available methods, such as groups and filters, to manage assignments and access permissions.
- **Tags:** Tagging provides further logical segmentation and grouping that can work across the various elements in the UEM tool to provide further granularity to assignments and permissions.
- **RBAC:** Role-based access controls (RBAC) limit permissions to those necessary for the assigned role.
- **Custom Roles:** Extend RBAC by creating custom roles tailored to your requirements.
- **Just in Time Permissions:** Limiting permissions until an administrative action is required reduces the risk of mistaken actions, impacting operations.
- **Multiple Admin Approvals:** Implementing approval from additional administrators enforces a verification step before changes are made to production environments.
- **Environment Segmentation:** Production environments must be separated from development and testing. In UEM tools where there is commonly only a single instance available, segmentation is possible through groups and tags. For example, development policies are clearly identified in the naming convention and have a development tag assigned to them.
- **Environment Hygiene:** The environment must be free of stale devices and user objects, groups and redundant policies to improve the accuracy of reporting and responses from the AI.

Restrict GenAI's Access

All UEM tools include controls to support delegated administration and geographically dispersed IT teams. With the governance standards from the previous section in place, you can limit the AI's permissions and control which content and devices it can interact with (see Table 1).

Table 1: GenAI Access and Permissions Matrix

↓	***Development*** ↓	***Test*** ↓	***Production*** ↓
Reporting	Full Control	Full Control	Full Control
Configuration and Policy	Full Control	Read Only	Read Only
Applications	Full Control	Read Only	Read Only
Devices	Full Control	Read Only	Read Only

Source: Gartner (November 2023)

- **Reporting:** Reporting and insights is the primary benefit of GenAI with minimal operational risk. The AI should be granted permission to read all data necessary to generate reports.

- **Configuration and Policy:** Limit the AI to creating and editing development configurations and policies. The AI must not be able to create or edit anything that impacts the production environment. The AI can have read permissions on production policies for reporting purposes.

- **Applications:** Limit the AI to creating application packages for testing and development. The AI must not be able to create or edit anything that impacts the production environment. The AI can have read permissions on production application deployments for reporting purposes.

- **Devices:** AI must be restricted to only applying actions, configuration and policies to development devices. The AI can have permission to query device information from all devices for reporting purposes.

Follow Robust Change Management Practices

With the governance standards in place and the GenAI restricted to creating artifacts and performing actions in the development environment, endpoint administrators can validate its output safely. Once satisfied that the GenAI-created artifacts work as intended, they can proceed through the change management process into testing and finally into the production environment (see ITSM Best Practices: How to Implement an Effective IT Change Management Practice).

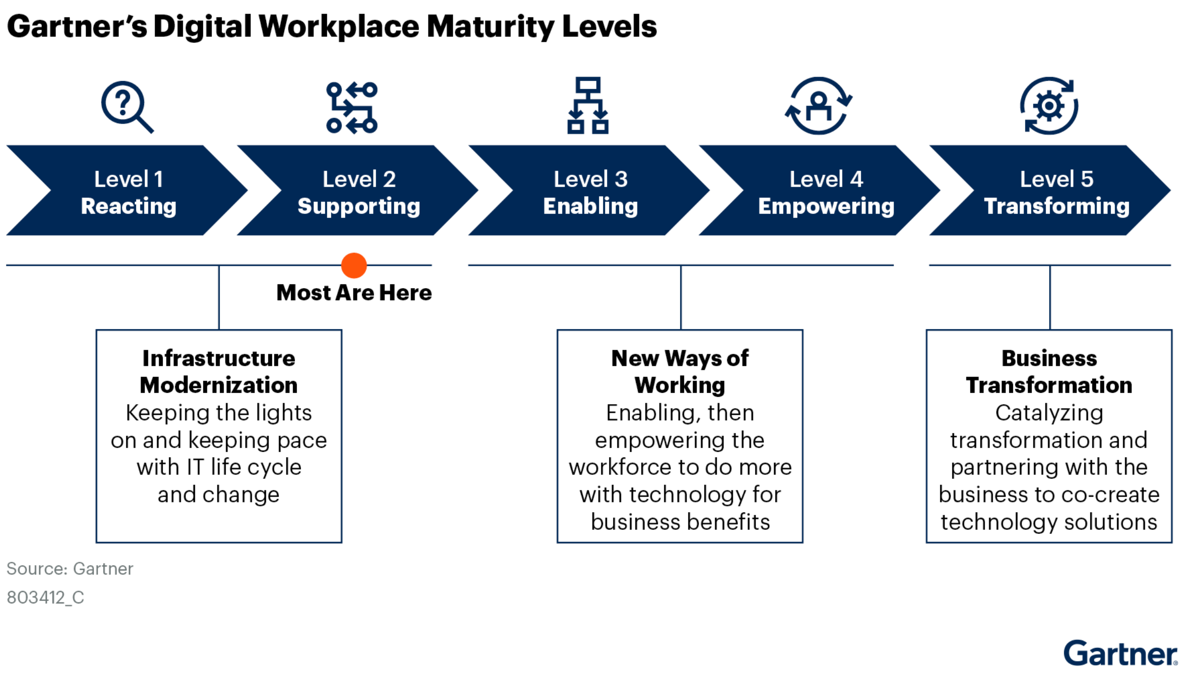
The Impact of GenAI Adoption on Core Device Management Competencies

This section will highlight the impact that GenAI adoption in the wider organization will have on endpoint management operations. GenAI will increase pressure on the core endpoint management competencies of application, device and OS life cycle management through:

- Increased demand for new applications.
- Increased application update frequency and demand for the latest application and OS version.
- Hardware optimized for GenAI will increase demand for new devices.

The impact of these increased demands will be more pronounced for organizations with low maturity levels, as defined in the Gartner Digital Workplace maturity model (see Figure 5). The actions recommended in this research are based on best practices and modern approaches to managing the digital workplace, which are all intended to improve operational efficiency and increase maturity.

Figure 5. Gartner's Digital Workplace Maturity Levels


Gartner's Digital Workplace Maturity Levels
Level 1 Reacting
Level 2 Supporting
Level 3 Enabling
Level 4 Empowering
Level 5 Transforming
Most Are Here
Infrastructure Modernization
Keeping the lights on and keeping pace with IT life cycle and change
New Ways of Working
Enabling, then empowering the workforce to do more with technology for business benefits
Business Transformation
Catalyzing transformation and partnering with the business to co-create technology solutions
Gartner

Source: Gartner

803412_C

See Enhance Maturity and Improve Investment Prioritization Using Gartner's Digital Workplace Maturity Model.

Streamline Management of New Applications

With the hype around GenAI's potential game-changing impact on productivity, some organizations will adopt a gold-rush mentality with a fear of being left behind by their competitors. This will drive them to launch pilot programs quickly. Gartner predicts that 80% of applications will include GenAI capabilities by 2026. [4] However, GenAI integration into currently used applications may be too slow, or not possible, rendering them obsolete. If the promised productivity gains of GenAI are fully realized, legacy applications that cannot support GenAI capabilities will rapidly become productivity bottlenecks, driving organizations to seek replacements.

It is essential that IT teams responsible for endpoint management are ready to support their organization's GenAI adoption initiatives and do not become an impediment to their success. It is critical to ensure that your application life cycle management process can quickly respond to new application requests.

Technical professionals must work with their digital workplace leaders to establish which parts of the organization intend to pilot or incorporate GenAI methods. Assess if this will require an update to an existing application, a new application(s) and the planned pilot time scales. If similar applications are requested from different business units, see if they can be consolidated into a single or smaller number of applications.

Update your documented use cases or user personas to include the GenAI-specific requirements to support those use cases. This might include access to new applications or allocation of additional licenses to enable access to the needed GenAI capabilities.

Use Gartner's Continuous Endpoint Engineering (CEE) Approach to Increase Update Cadence

Due to the increased focus on cybersecurity, IT teams have witnessed a dramatic increase in application update frequency in the last few years. GenAI will further accelerate application updates through:

- **The addition of GenAI capabilities.** Existing applications will require updating to access newly added GenAI capabilities.
- **AI-augmented software development reduces development time.** Quality updates, security fixes and new features will be available faster than before.
- **AI-augmented software development impacts software quality.** Inefficient code and an overreliance on AI from inexperienced developers could negatively impact software quality, leading to instability and requests to revert to previous versions.
- **AI software vulnerability detection.** AI-augmented tools will increase the discovery of new software vulnerabilities, leading to increased software updates.

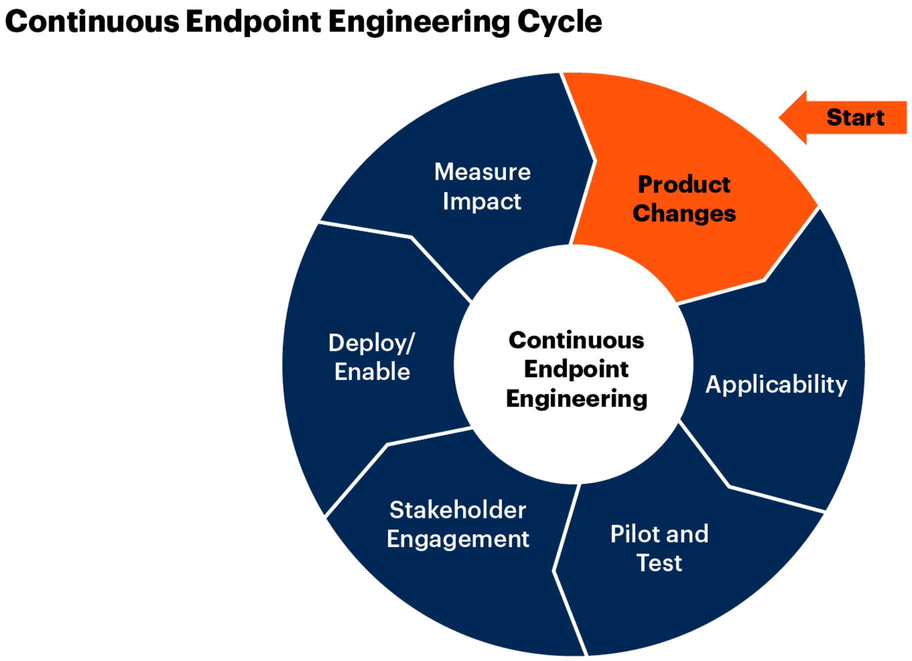
Microsoft requires Microsoft 365 client applications to be on the Monthly Enterprise update channel to maintain support for Microsoft 365 Copilot. [5] Organizations currently using the semiannual update channel will be forced to increase their update cadence to support Copilot. Other vendors will likely follow suit, stipulating that the application must be maintained on the latest client version to support GenAI.

It is reasonable to conclude that GenAI integration into the OS, such as Microsoft Windows Copilot, will have similar requirements, with the latest version providing the best experience or simply being required. Formerly the reserve of the endpoint management team, scrutiny of OS version upgrades will increase within the organization as the focus shifts from maintaining support to obtaining the latest features.

Modern application and OS update approaches, such as Gartner's Continuous Endpoint Engineering (CEE) (see Figure 6), provide IT teams with an agile methodology designed to meet the demands of an increased update cadence. CEE takes a product-based approach to managing digital workplace services. CEE defines a product as a set of applications and services with minimal customization that integrates with business value streams and is defined by the business outcomes it offers.

As a result, applications and OS can both be defined as products because — although they are critical to the organization — the scope, frequency and timing of changes are beyond the control of the organization. Figure 6 illustrates the six stages of the Continuous Endpoint Engineering (CEE) cycle.

Figure 6: Continuous Endpoint Engineering Cycle



Source: Gartner
803412_C

See How to Implement Continuous Endpoint Engineering: An Agile Approach for the Digital Workplace for further information on the CEE cycle, including the roles and responsibilities involved at each stage.

It is common practice to use third-party application repositories to manage commonly used applications, such as PDF viewers, web browsers and collaboration tool clients. Available through UEM tools or third-party providers, they provide prepackaged application deployments for distribution through their client or standard device management tools. This cost-effective approach removes the effort of maintaining low-value applications whose ubiquitous nature makes them a target for vulnerabilities, necessitating frequent updates, enabling IT teams to focus on supporting GenAI applications.

See Note 1 for a representative list of third-party application repositories.

Seek Low-Touch and User-Centric Approaches to Meet Demand for Increasing Device Turnover

GenAI is a computationally expensive process running on dedicated hardware in the cloud. As GenAI matures and becomes ubiquitous, cloud-processing will become a bottleneck for wider adoption, necessitating a move from the cloud to the endpoint. Neural Processing Units (NPU), sometimes referred to as AI accelerators, provide dedicated hardware optimized for GenAI. Like GPUs for graphics, they offload processing from the CPU, enabling enhanced AI operations while reducing CPU and power consumption.

NPUs and AI hardware acceleration will become increasingly important in future hardware generations and will be available in mainstream processors from 2024. Where NPUs provide a clear performance benefit or are required to support desired functionality, organizations will be forced to replace existing devices outside of the regular replacement schedule.

Low-touch device provisioning methods, such as Apple's Automatic Device Enrolment or Windows Autopilot, are hardware-agnostic methods and enable organizations to accelerate the adoption of new hardware. These methods eliminate the need to maintain customized corporate OS images, streamline device onboarding and widen device choice.

Taking a user-centric approach to device management eases the transition between devices. Apply corporatewide baseline configuration, like security settings, to the device. Apply configuration related to the employee job role and business unit to the user. Targeting policies and applications in this way provides a consistent experience across devices, and is less effort for IT to manage.

Alternative desktop delivery models, such as Desktop as a Service (DaaS), could provide access to NPU-enabled desktops in the cloud, eliminating the need to replace an otherwise usable device prematurely.

Recommendations

Adopt modern approaches to managing application and OS updates. Use CEE deployment rings and managed patching services to both accelerate and automate patching operations. Minimize the effort required to replace devices through low-touch device provisioning, such as Apple Device Enrolment, Android zero-touch enrolment or Windows Autopilot (see Maximize the Value of Windows Autopilot for Device Provisioning).

Avoid operational disruption by restricting GenAI Access through governance controls. Enforce good governance standards within your UEM tool. RBAC, groups and tags are essential for managing access and permissions. Identify and segment applications, devices, configuration and security policies into development, test and production to control GenAI's access. Allow it to report on all devices but limit its ability to create and assign content or actions to development environments. Follow change control processes to apply GenAI-created content to production environments.

Reduce the effort required to maintain applications. Leverage third-party application catalogs to maintain commonly used applications. Use your UEM tools integration with native app stores like the Apple App Store, Google Play Store and Microsoft Store, or application repositories like winget to distribute applications without repackaging.

Adopt a distrust and verify approach to content created by GenAI. GenAI hallucinations, bias and poorly crafted prompts reduce its efficacy. GenAI augments existing skills, but does not replace skilled employees who must verify its output for accuracy.

Conclusion

Generative AI adoption will place extra demands on endpoint management core competencies, such as application and OS life cycle management. The pace of AI adoption in the broader organization will likely outpace its inclusion in UEM tools, meaning that IT teams must use the tools they have at their disposal now, and not wait for future functionality to address increased demand for their services.

Adopting the modern device management practices outlined in this research will increase your operational efficiency and mitigate risk, helping to improve your organization's digital maturity and readiness to support GenAI adoption. Adopt a "distrust and verify" approach to GenAI by applying effective governance in your UEM tool to enable safe experimentation and usage of GenAI to augment your endpoint management operations.

Acronym Key and Glossary Terms

AEM	Autonomous Endpoint Management
AI	Artificial Intelligence
BYO	Bring Your Own
CEE	Continuous Endpoint Engineering
CMT	Client Management Tool
CPU	Central Processing Unit
DaaS	Desktop as a Service
DEX	Digital Employee Experience
GenAI	Generative Artificial Intelligence
ITSM	Information Technology Service Management
LLM	Large Language Model
MSI	Microsoft Installer
NPU	Neural Processing Unit
OS	Operating System
RBAC	Role Based Access Control
UEM	Unified Endpoint Management
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure

Evidence

[1] Client Webinar: The Future of Digital Workplace Infrastructure and Operations: This webinar was held on 21 June, 2023 with 433 respondents to the polling. Results of this poll should not be taken to represent all executives as the survey responses come from a population that had expressed interest in digital workplace infrastructure and operations strategy by attending a Gartner webinar on the subject.

[2] Introducing Microsoft 365 Copilot — Your Copilot for Work, Official Microsoft Blog.

[3] Introducing Microsoft Security Copilot: Empowering Defenders at the Speed of AI, Official Microsoft Blog.

[4] How Will Generative AI Impact Digital Workplace I&O?

[5] How to Prepare for Microsoft 365 Copilot, Microsoft Community Hub.

Notes

Table 2: Complementary Tools for Application Life Cycle Management

Category ↓	*Purpose* ↓	*Examples* ↓
Third-Party Application Repositories and Patching	Prepackaged software repository and automated application patching.	▪ Aiden Technologies ▪ Chocolatey Software ▪ Flexera (software vulnerability management) ▪ Ivanti Neurons Patch for Intune ▪ ManageEngine Patch Connect Plus ▪ Microsoft winget ▪ Liquit ▪ Patch My PC ▪ Scappman

Source: Gartner (November 2023)

Recommended by the Author

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

2024 Planning Guide for the Digital Workplace

How Will Generative AI Impact Digital Workplace I&O?

Maximize the Value of Windows Autopilot for Device Provisioning

How to Implement Continuous Endpoint Engineering: An Agile Approach for the Digital Workplace

How to Maximize the Benefits of Windows Modern Management

ITSM Best Practices: How to Implement an Effective IT Change Management Practice

Table 1: GenAI Access and Permissions Matrix

↓	*Development* ↓	*Test* ↓	*Production* ↓
Reporting	Full Control	Full Control	Full Control
Configuration and Policy	Full Control	Read Only	Read Only
Applications	Full Control	Read Only	Read Only
Devices	Full Control	Read Only	Read Only

Source: Gartner (November 2023)

Table 2: Complementary Tools for Application Life Cycle Management

Category	Purpose	Examples
Third-Party Application Repositories and Patching	Prepackaged software repository and automated application patching.	Aiden Technologies Chocolatey Software Flexera (software vulnerability management) Ivanti Neurons Patch for Intune ManageEngine Patch Connect Plus Microsoft winget Liquit Patch My PC Scappman

Source: Gartner (November 2023)