Enable BYOPC for Business Continuity While Managing Risk

Published 16 September 2020 - ID G00724744 - 14 min read

By Analysts Nathan Hill, Rob Smith, Stephen Kleynhans

Initiatives: Digital Workplace Infrastructure and Operations and 2 more

The unprecedented surge in remote work requires a tactical response that goes beyond an always-on VPN with fully managed notebooks. To sustain business continuity, I&O leaders must expand access to unmanaged and untrusted devices, while also adapting their security models and usage policies.

Additional Perspectives

- **Invest Implications: Enable BYOPC for Business Continuity While Managing Risk**
  (22 September 2020)

Overview

Key Challenges

- In response to COVID-19, organizations are tasked with supporting remote work at a scale that cannot be met with traditionally managed endpoints. To continue business operations, I&O leaders need more flexible alternatives that have clear policies for use.

- Using unmanaged, personally owned PCs — commonly known as bring your own PC (BYOPC) — increases an organization’s risk of security breaches, leading to potential data loss and reputation damage.

- BYOPC alone is insufficient to solve organizations’ remote access needs. Rather, this approach complements a digital workplace I&O delivery strategy by extending access options.

Recommendations

Infrastructure and operations (I&O) leaders responsible for digital workplace I&O must:

- Sustain business continuity by creating BYOPC acceptable usage and support policies that clearly state permissible use and end-user obligations for both short-term emergency usage and long-term BYOPC usage, to differentiate between both usage types.

- Minimize security risks by treating BYOPC as an untrusted endpoint computing model and implementing security strategies to protect user-owned PCs.
Enable remote work at scale by allowing remote employees to use BYOPC as an access device to connect to cloud and hosted content when they do not have a managed device.

Strategic Planning Assumption
By the end of 2022, more than 50% of I&O leaders will enable BYOPC, up from less than 20% at the start of 2020.

Introduction
BYOPC is a subset of the bring your own device (BYOD) strategy that focuses on PC platforms, including Windows, Macintosh and Chrome-based devices (see Update Mobile and Endpoint Policies to Reduce GDPR Risk and Address Bring-Your-Own-Device Policies).

Prior to COVID-19, few organizations expressed interest in BYOPC initiatives. PC platforms provide a broader set of end-user functions and a much broader attack surface compared to most devices, which could expose the corporate network to security vulnerabilities. In a Gartner survey of IT and IT-business professionals conducted in July 2019, only a quarter of respondents said that they planned to offer their employees BYOPC, and these were respondents from organizations with a formal digital workplace strategy in place in their organizations (see Note 1).

COVID-19 dramatically increased the scale and urgency of remote work for many organizations. As a result, organizations are revisiting BYOPC strategies to support remote workers. While organizations must embrace new strategies for enabling remote access, they cannot ignore security and use policies. Without these safeguards, malware and ransomware can lead to data loss and have a negative impact on an organization's brand.

I&O leaders must solidify their BYOPC usage, support, security and cost models while maintaining the practical value of BYOPC. This approach will help I&O leaders to promote business continuity and enable “anywhere operations” (see Workforce Resilience in the Eye of the Pandemic: Overcoming the Current Remote Work Situation While Planning for the Future and How to Keep End Users Connected to the Digital Workplace During Disruptions).

Figure 1 summarizes the common BYOPC approaches (indicated by the orange dots) and their relative level of organizational control. These approaches are explored in the Analysis section.

Figure 1: Common BYOPC Approaches and the Level of Organizational Control
Create BYOPC Use and Support Policies for Both the Short and Long Term

As organizations pursue a short-term emergency response to COVID-19 by enabling remote work, BYOPC has been essential. For some employees, BYOPC has been a full-function, full-time requirement where their personal device has become the sole access point for corporate data and application access. This use case is not new, but has exploded as a result of the pandemic. For other users, BYOPC has been a part-time requirement or choice. Use of personal devices can play a role in the digital workplace, but must have clear policies and guidance for use in short- and long-term use cases.

I&O leaders must establish a short-term BYOPC policy to define the scope of which services they are willing to provide (or make accessible) via BYOPC.

The short-term BYOPC policy should address:
BYOPC is specific to a traditional computing device such as a desktop or laptop, but BYO impacts more than just the PC itself. Devices like monitors, printers, keyboards and mice could all be part of the workspace equipment that users require to do their job. If employees use their own PCs, should the company provide accessories? I&O leaders must account for equipment-related expenses when

- **Usage duration.** This is the length of time you expect users to continue to use their own PC (for example, in an emergency or on weekends only). This will have a bearing on the risk profile of introducing unmanaged access devices.

- **Privacy considerations.** These include an explanation of how management and/or security controls may impact employee privacy and ensure that management of the local device is not impeding user privacy.

- **Application architecture.** Applications have specialized hardware or performance requirements that might require local installation and execution. For example, a videoconferencing tool will have dependencies on cameras and microphones that might require local drivers or applications. Local execution of applications presents significant problems related to data security, which is harder to mitigate when distributed to the endpoint.

- **Management model.** While modern management, using tools like unified endpoint management (UEM), will allow for support of a broader selection of platforms, these tools will require updated skill sets and recreating policies from legacy PC management tools used for company-owned PCs.

- **Hardware dependencies.** Determine the limits of what hardware will be acceptable. Survey employees to determine what devices they have and pinpoint potential problems. Set a baseline for what will be acceptable.

- **Network dependencies.** Home fiber broadband is often described by clients as performing better at home than the corporate network in the office. Given the surge in remote workers, however, this performance advantage may not hold up. There has been increased contention on ISP links, and many users struggle to retain the necessary Wi-Fi bandwidth when multiple users are on the home network. High-priority, time-sensitive traffic, such as video streaming and online gaming services, are especially taxing on the network. Network sensitivity is especially important when pairing BYOPC with a virtual desktop infrastructure (VDI) or desktop as a service (DaaS) architecture, as user experience will be directly dependent on the quality of the network connection. The network policy should cover the network capacity needed to enable effective and productive remote work.

- **Environmental factors.** Usage duration has a bearing on health and safety, especially in concert with personal monitor use and capable screen resolution. While not all of these factors will be BYOPC-related, some will be dependent on remote work conditions (including seating, desk height and posture).
calculating the total cost of ownership (TCO) of BYO. To build a workspace equipment policy, they can segment users by work settings to define who would be aligned to BYOPC versus corporate endpoints (see Optimize End-User Services Through Segmentation of Work Settings).

When creating their BYOPC policy, I&O leaders must determine the level of support that IT will provide. The default position could be zero support for a personally owned device. However, that position may not be in the interest of their organizations, as it would classify the employee as unsupported, in contrast to a limited policy that only supports company apps and data on a BYOPC device, but full support for content hosted on VDI or DaaS. Furthermore, a zero-support position makes it difficult to troubleshoot whether the device or the service itself is causing a connectivity or service access issue. The lack of visibility and endpoint management creates major support challenges.

I&O leaders must expand their long-term, strategic BYOPC policy to better describe the value to employees and the business.

The employee BYOPC value proposition should convey the following benefits:

- **Convenience of using his or her own device at home.** Personally owned PCs supplement the employee’s use of a company-issued system. For example, employees may not want to carry a corporate notebook home or may need quick, remote access to perform basic functions such as checking email, contacting a co-worker or checking a benefit.

- **Flexibility to use a different device from the company-provided notebook.** This benefit is not usually an employee need, but rather a want. Employees want a more flexible, customizable experience. This approach is typically only considered for higher performers or those in specific roles. For example, employees may want to use Mac devices in an organization that supplies Windows devices, use a smaller or lighter device, or use a device with a touchscreen or pen. Traditionally, IT organizations would not allow these devices, but are increasingly equipped to manage non-Windows devices as investments in UEM for company-owned assets grow.

I&O leaders should view the pandemic as a catalyst to accelerate their shift to a digital workplace that optimizes the employee experience.

The business BYOPC value proposition is often related to endpoint supply constraints. I&O leaders should communicate the potential for BYOPC initiatives to:

- **Save money by reducing hardware-related capital expenditures.** This approach does not resonate with employees or governments, many of which require a stipend or other
compensation to defray endpoint costs. The stipend model may be especially unworkable in countries where this is considered a taxable benefit and/or hardware costs vary greatly among the regions in which the organization operates. It is incumbent on the organization to ensure that all users have the right tools to perform their role. Investigating the financial realities of BYOPC must go beyond the expected savings generated by avoiding hardware acquisition. The need for stipends, the impact of decreased employee productivity, and the cost of implementing additional security tools and approaches can cancel out any hardware cost savings.

- **Enable users to use a personal device for limited need during an emergency.** Organizations are struggling to adapt to sudden remote work scenarios and global disruptions to the PC supply chain. The emphasis on future business continuity planning forces organizations to embrace BYOPC as a short-term option (if not a long-term employee access strategy).

Minimize Security Risks by Treating BYOPC Devices as Untrusted Endpoints and Implementing Security Strategies

Few organizations have installed traditional virtual private network (VPN) software on unmanaged endpoints due to security concerns. Most organizations are hesitant to extend their network to an untrusted, unmanaged PC. However, some organizations have taken a “semimanaged” approach to VPNs by stipulating the installation of specific security products on these personal devices to enable access to company resources.

BYOPC introduces some practical challenges. Not every employee household will have a PC, and many home PCs do not meet the technical requirements for application needs. Ultimately, organizations cannot compel employees into BYOPC. Even if they do have a personal device at the right specification and performance level, existing licensing terms may prohibit use of personally owned devices for certain software products (e.g., use of software in a specific geography), and thus employees who need these products should be exempt from BYOPC.

Posture assessment for remote access via BYOPC gives limited information unless I&O leaders install a management agent on the device. I&O leaders who embrace the privacy challenge of a management agent installation will gain security posture insight on the endpoint; however, remediating noncompliance remains a challenge. Helping remote workers to remediate security vulnerabilities from their noncompliant endpoint is far more difficult than identifying noncompliance. Following this path, BYOPC can complicate delivery of IT support, driving up support costs and complexity.

A more practical approach is to conduct posture assessment at the network and access gateway layer – especially using conditional access (see Enhance Remote Access Security With Multifactor Authentication and Access Management). These solutions assess the device before it is allowed access. Then, they grant granular access to resources based on device posture and user profile. Understandably, posture assessment is less reliable with unmanaged devices, especially when trying to detect advanced threats.
Quick Answer: How to Securely Enable Access for Unmanaged Devices provides direct, practical guidance to improve the security of BYOPC access using a broad spectrum of approaches including zero trust network access (ZTNA), multifactor authentication (MFA), security monitoring and network sandboxing approaches. These are based on low, medium and high levels of control that are appropriate to the sensitivity of the use case and the security policy of the organization. This allows us to expand the level of control shown in Figure 1 to include the relative risks, along with guidance on which approaches are best for short- and long-term usage, as shown in Figure 2. I&O leaders should apply these approaches while being sensitive to the employee situations described above, especially pandemic-enforced teleworking. For all scenarios, deploying corporate applications to unmanaged and untrusted devices without some form of network security or virtualization solution will be prohibited.

![Levels of Control and Risk Associated With Different BYOPC Strategies](image)

Enable Remote Work at Scale by Allowing Employees to Use BYOPC Devices

Many organizations have successfully augmented their managed PC, VPN-based remote access with unmanaged BYOPC remote access via remote control access to in-office PCs, VDI and desktop as a service solutions (see Solving the Challenges of Modern Remote Access).
These technologies shift the utility of a device to an access platform rather than an execution platform. This does not remove security risks, but it does change them. I&O leaders should reduce the risk surface by centralizing and securing the application execution environment and data access platform. This shifts the focus to protecting the authentication process and stopping data leakage from the working environment to the endpoint.

Posture assessment is still an important access step. However, even if the device posture is not fully compliant with remote access policies, certain content may be accessible (with full access reinstated when the posture anomalies are addressed). For example, keyloggers intercepting the keystrokes for a username and password cannot gain system access when MFA is deployed using a second factor password via a code or hardware token. Any compromised device should be cleaned, and the compromised account should be reset with a new password that adheres to password complexity requirements (two tasks that can be hard to execute in remote scenarios). This process prevents third-party access even if it fails to prevent device compromise, giving I&O leaders time to cure the compromised device while sustaining business continuity. Establishing untrusted endpoints represents a higher degree of risk with which many I&O leaders and CISOs are not comfortable. ZTNA is a key endpoint security principle in these scenarios, and BYOPC is the extension of a zero-trust network (see Market Guide for Zero Trust Network Access).

To support a remote execution and access device architecture, I&O leaders must adopt at least one of the following delivery architectures: remote control, server-based computing (including remote browser), VDI or DaaS. These architectures enable I&O leaders to implement security measures that work around the untrusted endpoint. Using these end-user computing architectures also narrows the network attack surface by only passing keyboard, mouse and video traffic through a transport layer security (TLS) VPN rather than a full-function IPsec VPN.

With remote computing solutions in place, I&O leaders must assess several security approaches:

- MFA, including a factor independent of the untrusted device.
- Policy restrictions on data movement outside of the managed workspace (such as disabling network clipboard, and client drive mapping from the hosted environment to the endpoint).
- Restrictions on using communication ports, such as virtual USB functionality and mapping the hosted port to the physical port of the access device. This will limit peripheral capabilities.
- File upload controls and security, if uploads must be allowed.
- A management tool and approach that will allow for the restrictions noted above, while also providing separation of user and work apps and data.

Some organizations are willing to tolerate an increased level of risk and use the local capabilities of an untrusted device to get work done. In this scenario, the best approach is to limit access to the browser and implement cloud security and browser isolation techniques. Many organizations use
this approach to connect to web applications and SaaS applications such as ITSM, CRM, ERP and cloud office.

**Evidence**

- Gartner client inquiries during COVID-19 period
- Input and collaboration from Gartner’s security team

**Note 1: BYOPC Adoption Pre-COVID-19**

The survey called “How Prepared Is Your Infrastructure to Implement a Digital Workplace” was conducted online from 1 July to 29 July with 61 Gartner Research Circle Members — a Gartner-managed panel of IT and IT-business professionals who had a formal digital workplace strategy in their organization. The survey was developed collaboratively by a team of Gartner analysts, and was reviewed, tested and administered by Gartner’s Research Data and Analytics team.

**Recommended by the Authors**

- Designing Security for Remote-Work-First Enterprises
- Solving the Challenges of Modern Remote Access
- How to Keep End Users Connected to the Digital Workplace During Disruptions
- Magic Quadrant for Unified Endpoint Management
- Critical Capabilities for Unified Endpoint Management Tools
- Workforce Resilience in the Eye of the Pandemic: Overcoming the Current Remote Work Situation While Planning for the Future
- How to Build a Successful Business Case for Desktop Virtualization
- A Comparison of Remote Network Access Products for Enterprise Endpoints

**Recommended For You**

- Three Elements to Successfully Enable Remote Work
- Magic Quadrant for Unified Endpoint Management
- Update Mobile and Endpoint Policies to Reduce GDPR Risk and Address Bring-Your-Own-Device Policies
- Critical Capabilities for Unified Endpoint Management Tools
- Quick Answer: How to Securely Enable Access for Unmanaged Devices