The number of empty office desks is on the rise, as a growing number of employees work remotely and/or use their own devices. At the same time, the bring-your-own-device (BYOD) movement is evolving to include desktops, laptops, and tablets (known as bring-your-own-computer or BYOC), so it’s no longer enough to secure only mobile devices against intensifying cybersecurity threats.

Many organizations have traditionally used Virtual Desktop Infrastructure (VDI) to provide remote workers with secure access to business apps, data, and files. Today, enterprises are re-examining their use of VDI for remote access because of its relatively high cost and complexity.

A secure remote browser, called out by Gartner as one of the top 11 information security technologies of 2017, is a newer, simpler, more cost-effective alternative. Its stand-out advantages over VDI are ease of deployment, low cost, and better user experience.
The Remote Work Movement and Growing Threats

Work is fast losing its identity as a place you go, and is becoming a thing you do – from many places. The number of people telecommuting in the U.S. increased 115% between 2005 and 2015. Gallup data shows that 39% of employees worked remotely in some capacity in 2012; by 2016 that number was 43%. Remote work is especially common among information and knowledge workers, executives and professionals whose work involves portable data.

A recent survey reported in Forbes found people who work from home are almost twice as likely to love their jobs compared to on-site employees. This fact has not gone unnoticed by companies that recognize the benefits of employee satisfaction, engagement, and productivity. Dell, for example, set a company-wide goal in 2013 of having half their workforce take advantage of flexible work options by 2020, and they reached that goal well ahead of schedule.

This trend has led to ever-increasing employee demands for anytime, anywhere access to business content from various endpoints, which broadens the attack surface for cybercriminals. A recent data breach investigations report by Verizon found the #2 and #3 leading sources of data breaches are user devices and users.
From BYOD to BYOC

The bring-your-own movement has expanded, with more employees using their own Windows 10 (including Surface Pro and laptops) and macOS devices – in addition to their mobile devices – to get work done. Increasingly, that work is happening via critical cloud apps and Office 365 tools.

BYOC has multiple potential advantages for organizations, including greater productivity, flexibility and significant savings on hardware, software, provisioning, and help desk. It’s a convenient, cost-effective option not only for regular employees working remotely but for partners and contractors. Yet BYOC is only beneficial if organizations can safeguard critical data while providing seamless access to corporate content and tools.

Defining the Remote Access Landscape

An understanding of the central terms helps assess the different options for remote access:

1. Desktop virtualization
   • Virtualization technology that separates a user’s desktop from their physical device
   • Based on the client-server computing model

2. Virtual Desktop Infrastructure (VDI)
   • A common type of desktop virtualization where a user’s desktop and apps are hosted on an organization’s central server
   • Users have specialized software installed on their devices and must log in to gain access via an Internet connection
   • No business data is stored on the user’s device
   • Centralizes IT management of desktops and apps

The Harvard Business Review reports that BYOC nearly doubled at high-performing companies (from 44% to 80%) in recent years.
3. Persistent and non-persistent virtual desktops

- Persistent virtual desktops provide users with their own dedicated virtual desktop image file, so any changes they make are preserved when they log out (good for knowledge workers)
- Non-persistent desktops do not preserve changes made to the virtual desktop during a work session (good for workers who don’t need a personalized desktop, like call center workers)

4. Secure remote browser

- Isolates user browsing sessions from enterprise networks and various endpoints, enabling users to access critical tools and get work done securely (even downloading sensitive business documents and data from corporate intranets)
- If the browser gets compromised, the attacker has no access to the user’s device or any sensitive business systems or data
- Feels like regular browsing to users
- Enterprises can allow native browser access to trusted cloud services (whitelisting) while using secure remote browsing for everything else

5. Secure container

- In secure remote browsing, an authenticated and encrypted area of a user’s device “containerizes” sensitive business data away from the user’s personal data and apps
- Prevents malware and other threats from interacting with the containerized app and associated data
- Uses fewer resources than desktop virtualization

The Rise of VDI: A Brief History

The original promise of VDI was to ease the stress and workload of IT individually managing employee-owned devices while improving security and reducing compliance risks. With VDI, IT can centrally manage and protect sensitive data and apps, while giving users anytime/anywhere access.

By the early 2000s, heightened cybersecurity concerns among enterprises and governments led to growing VDI deployments. From 2009 to 2015, there was fierce competition between the two major players in the VDI market. But soon, challenges cropped up, as some IT managers did not fully understand the infrastructure requirements, resulting in some flawed VDI deployments. Still, according to the Tech Republic in 2013, 45% of companies were using VDI, and VDI was present in at least 50% of companies with more than 250 employees.
In the last few years, however, organizations are re-evaluating VDI from an ROI viewpoint and looking for more cost- and operationally efficient solutions.

Remote Access Use Cases

Different types of workers have different remote access needs, and VDI is not always the best option.

For example:

**Task workers (such as call center employees or receptionists)**
- Rarely require mobile or remote connections
- Usually only require non-persistent desktop virtualization, but may like to have a personalized desktop – however, creating a persistent/private virtual desktop could double or triple the per-desktop cost

**Knowledge workers (such as accountants, lawyers, and academics)**
- Rarely 100% remote workers, though they require remote and mobile access
- Upfront costs and ROI do not always favor VDI investment

**Power users (such as software developers or graphic designers)**
- Require powerful hardware and sophisticated software that does not work well on a regular virtual desktop due to possible network latency issues (slow screen updates)

**Part-time/temporary users (such as contractors and external partners)**
- VDI is not well-suited to organizations’ need to quickly and easily provision and de-provision these types of workers
- Need immediate, but often temporary, access to specific corporate resources
- Does not make sense to invest in costly, complex VDI for this group
The Downside of VDI

Today’s enterprises are reconsidering their attachment to VDI for remote access, mostly because it can be prohibitively expensive and overly complex.

Top 5 disadvantages of VDI

1. **Complex deployment**
   - Requires some modification of nearly every aspect of a network, from upgrading servers to adding networking equipment – not to mention necessary cooling, power and cabling improvements
   - A mid-sized VDI instance can require as many as 19 separate components working in tandem to function properly
   - Transitioning to VDI usually involves training for all IT staff involved in designing, deploying and maintaining the system
   - Often requires agreements with multiple vendors (for hardware, software, licenses, etc.)

2. **High cost**
   - The biggest upfront cost is backend infrastructure (servers)
   - Indirect costs include: electricity, building space, consultants, time for implementation and training
   - The additional expense of software licenses and Virtual Private Network (VPN) licenses
   - Many enterprise VDI licenses are consumed by users who are only accessing email, calendar and a secure browser (for Salesforce, SharePoint, NetSuite/Concur, etc.)

3. **Poor user experience**
   - VDI must have a network connection, which leaves remote users without their primary work tool when there is low or no connectivity. While many planes now offer in-flight Wi-Fi, these connections are usually inadequate for VDI and VPN. Likewise, many hotels require costly, premium Wi-Fi connections to enable VDI access. With no offline storage capabilities, VDI can leave users without access to email, calendar, and document editing tool.
   - All screen updates move over the network, so a slow network can lead to frustrating user experience, especially where graphics are involved
   - VDI apps are limited when it comes to processor intensive apps
4. **Difficult to scale**

- Scaling up a VDI solution demands that an organization also scale up the server and networking infrastructure, which can be expensive and time-consuming.

5. **Vulnerable to cyber attacks**

- Some analysts argue that VDI is not, and never will be, a security solution, but an IT solution focused on managing desktop environments.
- Since remote desktops can access the corporate network, if one remote desktop is infected with malware, it can spread across the entire enterprise.

**An Alternative to VDI: Secure Remote Browsing**

A secure remote browser offers users seamless remote access to corporate content while lowering costs and increasing security. For enterprises with large VDI deployments, even a small de-provisioning (10% to 30%) can provide a quick and significant ROI and lowers TCO. VDI can cost as much as $900 to $1,000 per user per year.

A recent Gartner report ("It’s Time to Isolate Your Users From the Internet Cesspool With Remote Browsing") forecasts that 50% of all enterprises will actively implement solutions to isolate internet browsing by 2021, a major increase from the less than 5% of companies deploying secure browsing solutions in 2016. According to the report, almost all successful cyber attacks originate from the public internet, and browser-based attacks are the leading source of attacks on users. While information security architects cannot stop attacks, Gartner says, they can contain the damage by isolating end-user internet browsing sessions from enterprise endpoints and networks.

The news site helpnetsecurity.com says secure remote browsing “represents a new, proactive approach to safeguarding against Internet-borne threats . . . provid[ing] an additional layer of defense without impacting business operations or changing the way users access the web.”

Infosecurity Magazine says many organizations of all sizes – but especially large firms with tens of thousands of endpoints – are evolving to a browser isolation strategy, and "it is only a matter of time before this approach becomes less of a best practice and more of a fundamental requirement."
Top 5 Reasons to Consider Secure Remote Browsing

1. **Simple, lightweight deployment**
   - No new infrastructure required
   - On-premises, cloud-based or hybrid deployment
   - Rapid, easy provisioning for IT via a web interface, while offering extensive management capabilities for fine tuning
   - One vendor
   - No specialized training necessary

2. **Lower TCO**
   - Eliminates the cost of upgrading, adding and maintaining complex hardware
   - Simple, resource-light, web-based architecture
   - Fewer components enable vendor consolidation

3. **Seamless, intuitive user experience**
   - No reliance on a network connection
   - Secure, consistent, unrestricted web access on any device, anywhere, regardless of connectivity
   - User experience is indistinguishable from the original website or app
   - Simple login

4. **Containerized data security**
   - Allows users to browse freely, while never exposing the corporate network to cybersecurity risks
   - Every web session is handled in a sealed virtual container, so even if a user opens malware it has nowhere to go (and then the container is destroyed)

5. **Easily scalable**
   - Quick, cost-effective scaling leverages container and browser virtualization, with no need to scale up any hardware or purchase additional licenses

BlackBerry Access meets the same need as VDI for remote access, yet without the heavy investments in backend infrastructure and licenses or the deployment complexity. It enables users to securely access corporate intranets and web applications – including third-party extensions such as Salesforce – on personal or noncorporate-managed Windows 10 and macOS computers.

**Key Benefits**

- Enables users to securely connect and access the enterprise resources they need directly from their computer—and even multiple computers—and have all the tools they need to work remotely
- Allows quick, easy onboarding and offboarding of both traditional and non-traditional employees (including contractors and partners)
- Enables savings on hardware, software and help desk costs
- Offers full business productivity on personal or noncorporate-managed computers
  - Offline access to BlackBerry Apps, ensuring access to email, calendar, document editing and more anytime; plus offline storage capabilities
  - The intuitive user experience for web browsing
  - Single sign-on
  - Access to Microsoft Office 365 apps online
- Provides end-to-end security to protect against data leakage. Data Path Control, the ability to route data through enterprise firewalls so organizations can enable seamless connections for remote users to sensitive data sources, significantly reducing concerns for data leakage.

- BlackBerry® is the only vendor to have achieved the highest score in 6 of 6 use cases of the [Gartner Critical Capabilities for High-Security Mobility Management](https://www.gartner.com/en)
- BlackBerry® was a leader in the [2017 Gartner Magic Quadrant for EMM](https://www.gartner.com/en)
- BlackBerry® Workspaces achieved 2 of the 5 highest scores in Workforce Productivity and Centralized Content Protection in the [Gartner Critical Capabilities for Content Collaboration Platforms](https://www.gartner.com/en)
- BlackBerry® ranks in the top 10% of all global cybersecurity organizations in the [Cybersecurity 500 ranking](https://cybersecurityventures.com/ranking) published by Cybersecurity Ventures
- BlackBerry® has 80+ Security Certificates, more than any other mobile vendor
- BlackBerry® has thousands of security-related patents
- BlackBerry® is deployed with all 7 of the G7 and 15 of the G20 governments
Conclusion

Organizations must respond to the new and growing reality of remote work by supporting both optimal employee productivity and cybersecurity – all while minimizing direct and indirect costs.

Browser isolation is the next step in the evolution of secure remote access. It helps organizations keep pace with the constantly evolving cybersecurity threats, but with relatively minimal operational demands compared to VDI deployments.

Learn more about how BlackBerry Access allows users to work remotely from personal or noncorporate-managed computers with confidence, efficiency and ease.