

The CIO's Guide to BYO-PC

Why BYO-PC is the future, how to build a formal program, and what tools can help you bring it to life



CONTENTS

INTRODUCTION	03
THE MOMENT: WHY IT'S TIME TO EMBRACE BYO-PC	04
• FIRST, BYO-PC IS ALREADY HERE	04
• SECOND, BYO-PC ADOPTION WILL ONLY ACCELERATE	06
• THIRD, BYO-PC IS CREATING BIG RISKS — AND BIG OPPORTUNITIES	09
THE PROCESS: HOW TO BUILD A BYO-PC PROGRAM	12
• DON'T REINVENT THE WHEEL — MOBILE PHONES PROVIDE THE MODEL	12
• 8 QUESTIONS TO ASK TO BUILD YOUR FORMAL BYO-PC PROGRAM	14
THE TOOLS: WHAT YOU NEED TO BRING BYO-PC TO LIFE	19
• THE NEED FOR NEW TOOLS: WHY EXISTING BYO-PC TOOLS DON'T WORK	19
• FINDING NEW SOLUTIONS: HOW TO PICK MODERN BYO-PC TOOLS	21
TAKE THE NEXT STEP TO EMBRACE BYO-PC — TODAY	22
HOW CAN VENN HELP YOUR ORGANIZATION SUPPORT SECURE BYO-PC?	23




INTRODUCTION

Your workforce has transformed.

Remote and hybrid work have become a permanent part of most organizations.

Employee computing models that were built for an “office first” workforce no longer work in a “hybrid first” workforce, and it’s time to adapt to a BYO-PC model where employees use their own personal devices for work — without sacrificing security, performance, or fundamental control over your organization’s data and applications.

To help you adapt your models and embrace BYO-PC, this guide will explore:

-  Why BYO-PC is not going away, and why you need a formal program
-  How to build a formal BYO-PC program using mobile phones as the model
-  Why tools like VDI and DaaS are failing, and how to pick modern BYO-PC tools



THE MOMENT: WHY IT'S TIME TO EMBRACE BYO-PC

BYO-PC is not a fad. There are three reasons why BYO-PC is here to stay, and why you must build a formal program to manage and secure the personal devices your employees will inevitably use to access your sensitive data and critical applications.



FIRST, BYO-PC IS ALREADY HERE

Bring Your Own PC (BYO-PC) is a subset of Bring Your Own Device (BYOD). While BYOD can refer to employees using any personal device to perform their work, BYO-PC specifically refers to employees using their personal PCs for work tasks.

BYOD as a whole has grown substantially over the last decade, and is becoming the norm for most organizations in most industries.

Consider a few data points:



Between 67 – 77% of people use their own devices at work

regardless of whether or not their organization has a formal BYOD program in place.



The BYOD market has grown ~1,000% in less than 10 years.

It is expected to have reached \$367 billion by the end of 2022, up from \$30 billion in 2014.



The global BYOD market is projected to grow by \$69.07 billion

between 2021 – 2026 and reach a compound annual growth rate of 15.065 during this period.

Gartner predicts that within this continued growth, BYO-PC will transform businesses over the next few years, largely driven by pandemic policies.

“Prior to the COVID-19 pandemic, there was little interest in BYOPC – explained Robert Smith, senior research director at **Gartner**.

“At the start of the pandemic, organizations simply had no other alternative. The urgent need to enable employees to work from home and a lack of available hardware bolstered its adoption globally. Gartner clients said their adoption of BYOPC is up from less than 5% in 2019.



Additional research found that **58.3%** of employees increased their use of personal devices for work during the pandemic — and all signs point towards that formal and informal adoption of BYO-PC will not only stick; it will accelerate in coming years.

Here's why.

SECOND, BYO-PC ADOPTION WILL ONLY ACCELERATE

BYO-PC is not a fad, and it is not a temporary pandemic-driven measure. It is a once-in-a-generation transition in employee computing that is being driven by three fundamental trends in how work is done and how workforces are equipped.

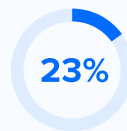
TREND 1

Hybrid Work is Here to Stay, and It's Blurring the Lines Between Personal and Professional Lives

McKinsey recently found that



35% of Americans can work from home full-time



23% can do so part time



58% Adding up to 58% of Americans capable of working from home at least one day per week

Only 13% of workers who have the opportunity to work remotely choose not to, and Americans with the chance to work remotely does so for an average of 3.3 days per week. 65% would prefer to do so all the time.

For these workers, the line between their personal and professional lives is blurring, and their device choices reflect this feeling.



Half of office workers now see their work devices as personal devices



27% use their work device to play games



36% use it to watch online streaming services



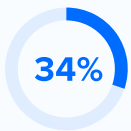
~40% use it for homework or online learning.

The more employees work remote, the more these lines will blur. In the future, most people will either use their personal devices for work, or use their work devices for personal purposes, eliminating most of the point of provisioning employees company-owned PCs in the first place.

TREND 2

Organizations are Using More Contractors, Temps, and Offshore Workers

At the same time employees are working remote or hybrid, the workforce is also rapidly filling up with independent contractors, and temporary and offshore workers.



The number of independent workers grew 34% to reach 51+ million from 2020 to 2021 alone.

These workers typically use their own computers that are neither provisioned by their clients, nor managed or secured by their clients' IT departments.



It's Getting Too Expensive to Provision and Support PCs for Employees

Large-scale remote and hybrid work is making it harder and more expensive to provision and support employee PCs.

In the past — when most employees worked in the office — an IT worker could drop by an employee's desk to hand them a new PC, to collect their device when they left the organization, or to troubleshoot a computing issue that needed physical support.

In today's remote and hybrid world, IT needs to ship PCs back-and-forth between the office and an employee's home every time they need to onboard, offboard, or physically troubleshoot their device.

The cost of shipping PCs to remote and hybrid workers is adding up, and companies are looking to get out of the hardware business of provisioning and supporting their employees' PCs — especially when 95% of workers already have their own device.

In sum: Most organizations now deploy a workforce where many of their people work remote or hybrid most or all of the time. Because of this, it no longer makes sense to provision and manage worker PCs.

This transition is happening for nearly every organization, in nearly every industry — and it's creating significant risks and potential benefits that they must contend with.



THIRD, BYO-PC IS CREATING BIG RISKS — AND BIG OPPORTUNITIES

Many organizations are allowing their employees to use personal PCs for work at least part of the time, which means they already have an informal approach to BYO-PC in place, even if they don't realize it.

While some organizations are using VDI and DaaS tools to manage and secure their employees' personal devices, many organizations are relying on their employees to practice good behaviors for keeping personal PCs safe and performant.

This informal approach to BYO-PC creates a flood of new exposures, including:



Security Risks

Organizations lose control over their most sensitive data and applications — including where it's stored, who's accessing it, how it's protected (or not), and more.



Operational Risks

Organizations cannot update, patch, or configure their employees' assets, and users are less likely to reach out to IT support if they need technical help.



Resource Risks

Organizations have the opportunity to reduce the IT headcount they allocate to support, but they don't know by how much, and how to repurpose their staff.

These risks will increase as time passes, the three trends we listed intensify, and BYO-PC adoption accelerates. Organizations can only mitigate these risks by taking a new approach, embracing BYO-PC, and building formal policies and programs around it.

And with the right BYO-PC program, organizations can do more than just mitigate these risks. They can also capture a wealth of benefits, for multiple roles within their organization.

With the right BYO-PC program:



CIOs and IT Leaders

Reduce the costs, complexity, and headcount needed to provision and manage devices in a remote-first world, accelerate standard time-consuming tasks like onboarding and offboarding employees, and refocus on bigger-picture responsibilities.



IT Admins

Stop deploying new machines, chasing down machines that need to be returned, re-imaging machines, remotely debugging issues, and getting blamed for slowing down employees.



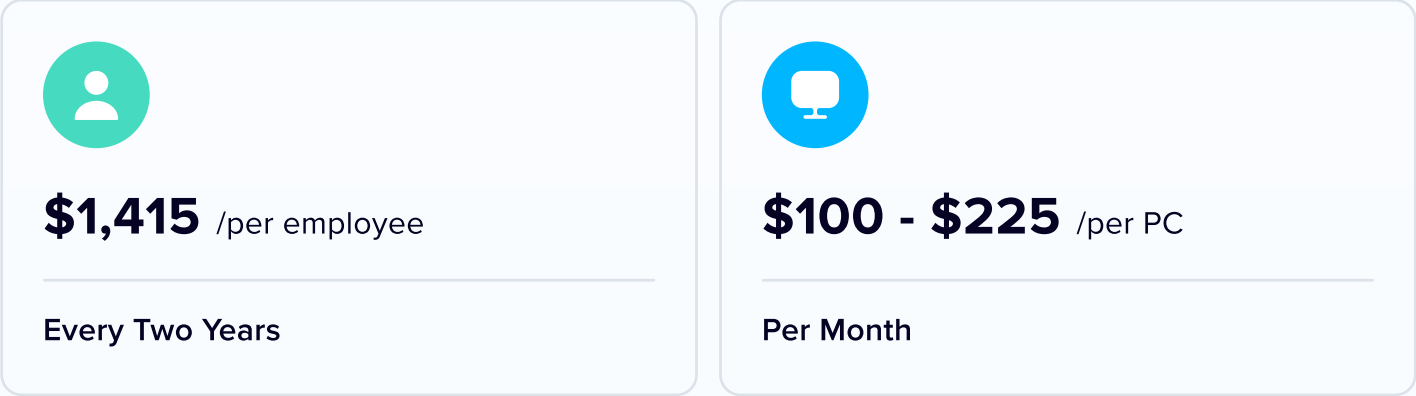
End Users

Stop juggling multiple PCs, gain the freedom to use the PC they feel most comfortable and productive with, and switch between work and personal actions without struggling against security controls.

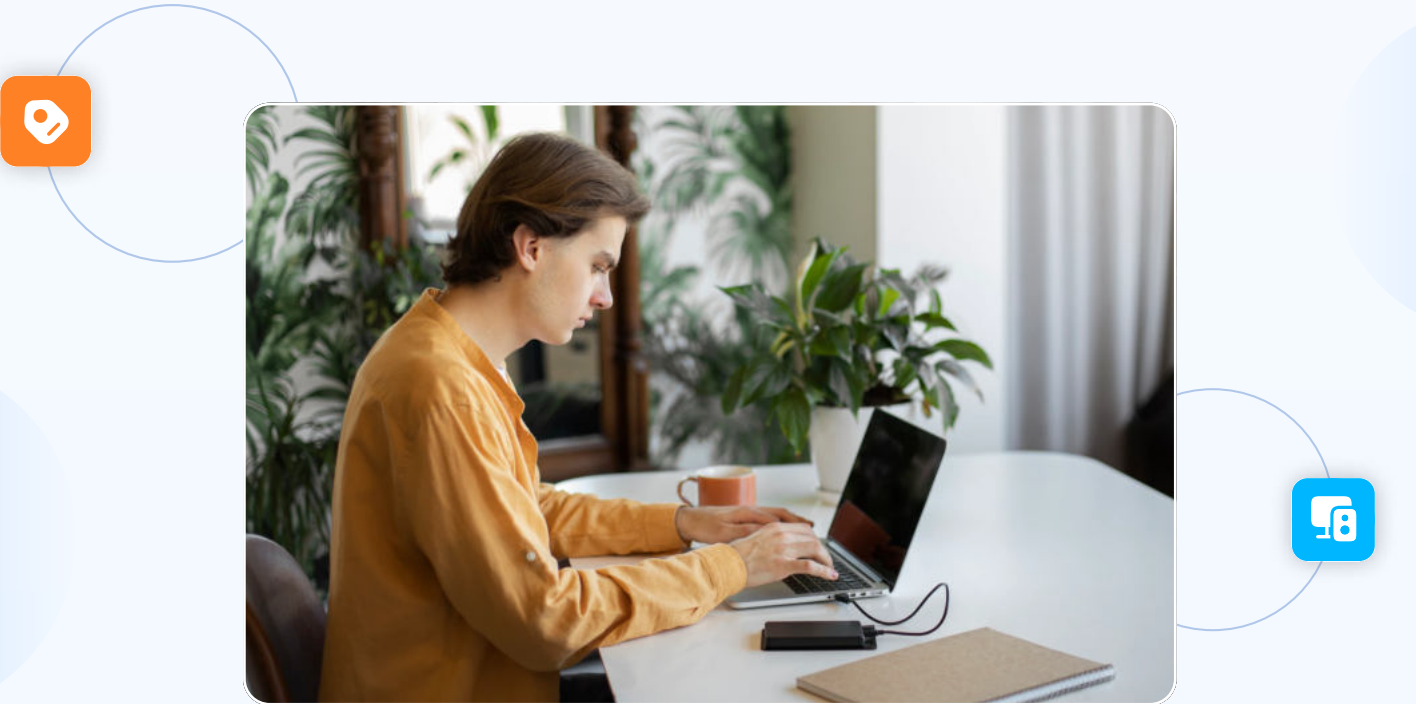
Perhaps most important of all, organizations can save a considerable amount of money — while improving productivity — by embracing BYO-PC and building the right formal program. 42% of employees that use their own devices increase their productivity and efficiency using their own devices.

At the same time, organizations spend an average of \$1,415 per employee every two years provisioning devices — and these costs can be reduced or eliminated entirely with the right BYO-PC plan. Even if organizations support these devices through an external managed service provider, they can expect to pay between \$100 - \$225 per PC, per month, in support fees.

Organizations' expenditures on average:



Ultimately, organizations can only capture these benefits — and close their risk exposures — by embracing BYO-PC and building the right program. And for the rest of this guide, we'll show you how to do just that.



THE PROCESS: HOW TO BUILD A BYO-PC PROGRAM

Organizations have already learned how to secure and manage employee-owned devices thanks to the growth of mobile phones in the workplace. Lessons from these initiatives provide the model for building a formal BYO-PC program.



DON'T REINVENT THE WHEEL — MOBILE PHONES PROVIDE THE MODEL

BYO-PC is not unprecedented. Over the last 10 - 15 years we saw a similar movement occur as employees began to use their personal mobile phones at work.

In the past, employees typically had two mobile phones — a Blackberry that they used for work, and a separate mobile phone and number they used for their personal life.

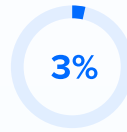
All of that began to change with the launch of the iPhone, and the broader creation of the smartphone. Suddenly, employees' personal phones were capable of the same heavy-duty work tasks as their Blackberry, and they began to use their smartphones for both their work tasks and their personal lives.



While some industries — like Finance — still require their employees to have a dedicated work phone, most organizations in most industries would consider it a waste to provision and support their employees' phones.



Today, **75%** of employees use their personal mobile phones for work



3% of organizations have a formal BYOD program in place to manage those employee-owned devices

There are two lessons to take from this:



Something similar to BYO-PC has happened before.

If you need further proof that wide scale adoption of BYO-PC is likely to occur in the future, realize that many considered the wide scale adoption of BYOD for mobile phones unlikely.



There's a proven model for managing personal devices used for work.

Mobile phones have roughly the same operational and security challenges as PCs, and the model organizations developed to manage and secure them can lay the foundation for how you manage and secure your employees' PCs.

There's no need to reinvent the wheel.

Take the basic principles used to manage and secure employees' mobile phones, and use them as the foundation for your formal BYO-PC program. To help you get started doing just that, we've outlined 8 questions you can ask yourself — with 3 sub questions each — based on the core principles of mobile device management.

8 QUESTIONS TO ASK TO BUILD YOUR FORMAL BYO-PC PROGRAM

QUESTION 1

Which Types of PCs Can Be Used?

Most of your workers will likely use standard, commercial PCs from a limited range of popular options. These PCs will likely be compatible with whatever applications your employees need to do their jobs, and whatever software you might use to secure and manage them.

However, it is possible that some of your employees might wish to use more exotic devices, and it's worth defining what PCs will fit within your program.

To do so, ask yourself:



What applications and software must my workers' PCs operate, and do they have any device limitations or incompatibilities?



Do we consider any PCs to be fundamental security risks, or out of compliance with our regulatory requirements?



Are certain PCs — like gaming rigs — clearly designed primarily for personal use and out-of-scope for support and reimbursement?



QUESTION 2

Who Handles Their Software?

Your employees will likely need to use a suite of applications for their job. In an employer-provisioned program, you would pre-load these applications onto PCs before you provision them, and you would manage them. In a BYO-PC program, you will need to determine how these applications are acquired and maintained.

To do so, ask yourself:



Must employees use our licenses for every application they use, or can they use their own licensed software?



Will employees install all of their own applications on their PCs, or will we manage installations?



Will employees update, patch, configure, and maintain the hygiene of their applications, or will we?

QUESTION 3

What Counts as Business Use vs Personal Use?

As noted, the lines between personal use and professional use blur during hybrid work and BYO-PC. It's up to you to set those boundaries for your workers, and to set expectations that will keep your organizational data safe — without frustrating your users or expecting them to dramatically change their behavior.

To do so, ask yourself:



What applications, data, and activities must each employee deploy in order to do their job?



How can we separate those applications, data, and activities from the rest of their behavior on their PC?



How can we monitor the use of business assets on our workers' PCs without infringing on their privacy?

QUESTION 4

Who Do Employees Turn to For Support?

One of the biggest benefits of a formal BYO-PC program is reducing your IT support costs. Employees are more likely to handle support for their own devices than for employer-owned devices. However, there still may be times when your IT team is needed to step in, and you must clearly define where your responsibilities lie.

To do so, ask yourself:



What hardware and OS issues should an employee resolve by contacting their PC's manufacturer?



What hardware and OS issues will we resolve for our employees?



When will we provide application support to an employee, and when will we expect them to seek support from the vendor?

QUESTION 5

What Incentives and Reimbursements Will We Offer?

Employees expect to be reimbursed for any work-related expense they shoulder, and PCs and other work-related costs created by remote and hybrid work are no exception. You must determine what you will reimburse your employees for, what you will incentivize them to purchase, and how much you will pay them back.

To do so, ask yourself:



At what point in a PC or software license's lifecycle will we reimburse our employees for it, and by how much?



Will we reimburse our employees for anything else related to their PC that can help them with work, such as their home WiFi?



How can we get employees to use high-performance PCs? (e.g. shipping them factory devices, subsidizing PCs that comply with specs)

QUESTION 6

How Will We Reduce Friction for Employees

It's important to reduce friction for employees to ensure fast adoption of your BYO-PC policy, and to ensure a smooth transition to this new way of working. To do so, you must systematically identify and disarm some of the most common sources of employee friction.

To do so, ask yourself:



How can we take our employees' privacy concerns seriously, and make it clear they won't be "spied on"?



How can we ensure our employees won't have to change how they use their PCs, or have limits on what personal uses they can enjoy on it?



How can we keep things simple for our employees and avoid introducing complexity into their lives (while still reducing IT support)?

QUESTION 7

How Will We Offboard Our Employees' PCs?

Offboarding is a challenge for any BYOD or BYO-PC program. After all, you aren't going to collect an employee's PC after they stop working for your organization. Yet, you still need to find a way to ensure their PC no longer holds any of your organization's data, applications, or other sensitive assets.

To do so, ask yourself:



How will we know what organizational data and applications our employees have on their PCs?



How can we remove those applications — or at least end their licenses — and remotely wipe their PC of our data?



How can we find and remove organizational data that remains on employee devices, and prevent it from being accidentally leaked?

QUESTION 8

How Can We Keep Employee PC Secure and Compliant?

Security and compliance sit at the heart of every effective BYO-PC program, and connects to all six of the other questions you must ask yourself. Your program must reduce or eliminate as many of your risk exposures as possible without interfering with your employees' ability to do their job or go about their personal use of their PC.

To do so, ask yourself:



How will we maintain basic security practices — from malware scanning to incident detection and response — on our employees' PCs?



What regulatory frameworks must we meet, what requirements do they have for PCs, and how can we keep our employees' PCs compliant?



How can we limit or eliminate the potential for employees to accidentally share sensitive organizational data or assets through their personal channels?

Answer all 8 questions — and all of their sub-questions— and you will cover most of your bases as you design your BYO-PC program.

Security and compliance sit at the heart of every effective BYO-PC program, and connects to all six of the other questions you must ask yourself. Your program must reduce or eliminate as many of your risk exposures as possible without interfering with your employees' ability to do their job or go about their personal use of their PC.

THE TOOLS: WHAT YOU NEED TO BRING BYO-PC TO LIFE

Existing BYO-PC tools are not working. They were designed for a different reality — one where most employees worked from the office most of the time. You need to deploy new BYO-PC tools that were designed for today's large-scale hybrid workforce.



THE NEED FOR NEW TOOLS: WHY EXISTING BYO-PC TOOLS DON'T WORK

While large-scale BYO-PC is new, the basic idea of managing and securing a remote PC is not. Organizations have used Virtual Desktop Infrastructure (VDI) tools for years to manage and secure PCs used by the relatively small number of remote employees they deployed.

Today, many organizations are attempting to use their same VDI tools — and new Desktop-as-a-Service (DaaS) solutions — to manage and secure PCs for a far greater number of remote workers, and these organizations are learning a hard lesson. While VDI and DaaS tools are sufficient for small-scale hybrid work and BYO-PC programs, they are not designed for the realities of the modern workforce.

Applied to modern large-scale hybrid work and BYO-PC, VDI and DaaS simply do not scale and are creating multiple operational problems.



Applied to modern large-scale hybrid work and BYO-PC, VDI and DaaS simply do not scale and are creating multiple operational problems.

They are:



Expensive

While they promise cost-savings, they require backend servers to run. These servers demand a significant investment to set up and to maintain and their software creates additional licensing costs.



Complex and Error-Prone

They require bandwidth-hogging hardware and software to operate — all of which must be overprovisioned to ensure consistent performance, and all of which must be maintained independently through consistent patching and updating.



Slow and Laggy

They consume significant bandwidth and can struggle under routine operations like launching software updates and malware scans, or running video conferencing applications like Zoom.

In sum: VDI, DaaS, and other legacy tools were built for a different era, and don't deliver the performance and efficiency needed to drive large-scale BYO-PC. They are often frustrating for end users, they still require a significant amount of technical support and oversight to operate, and the costs of standing up and maintaining their backend systems is significant.

Clearly, organizations need a new suite of tools to manage and secure their employees' devices—tools designed for the modern hybrid workforce.

FINDING NEW SOLUTIONS: HOW TO PICK MODERN BYO-PC TOOLS

Most organizations know their VDI and DaaS tools are not working, and that they must update their tech stack to drive their new hybrid workforce. Yet organizations have continued to use these legacy tools because — to date — there haven't been many viable modern alternative solutions.

All of this is changing. Just as new tools were developed to support large-scale use of personal mobile phones in the workforce, new BYO-PC solutions are starting to emerge. These tools will need to cover multiple facets of managing and securing employee PCs, and must meet a few criteria.

New BYO-PC solutions must be:



Simple and Cost Effective

They must reduce or eliminate the cost and complexity of buying, managing, and shipping company-owned PCs — without demanding their own complex, expensive backend infrastructure.



Secure and Compliant

They must protect company data from accidental or malicious exfiltration, compromise, or loss, and provide robust admin control over work applications and data at every stage of the device's lifecycle.



Private and Easy-to-Use

They must let users work normally and not change their habits, allowing them to work from a single computer, and make it easy to separate personal use of the device from professional use — without feeling like their personal use is being monitored.

Most importantly, new BYO-PC solutions must be designed to deliver a high level of consistent performance — while still being easy to deploy and integrate with existing infrastructure and work habits — for a large-scale hybrid workforce.

While tools that meet these criteria are currently few and far between, more emerge every year. And as BYO-PC adoption accelerates, we expect to see more and more of these tools appear over the coming years. These tools will create the foundation for any effective formal BYO-PC program, and create the catalyst for BYO-PC to become the norm for most industries.

TAKE THE NEXT STEP TO EMBRACE BYO-PC — TODAY

BYO-PC is here to stay, and the organizations that get ahead of the curve and embrace this transformation will reduce their risks, and capture significant advantages over their peers.

To do so for your organization, take the right next step:



Take stock of your current BYO-PC position

How many of your employees are remote, hybrid, or contractors? How many of them are using their own devices for work? Do you have a formal plan in place to manage and secure those devices, and how well is it working? Most importantly, will it scale?



Calculate how much you could save with BYO-PC

If you haven't, use our calculator to determine how much budget you are leaving on the table by provisioning and maintaining company-owned PCs. Chances are it's more than you think, and enough to justify a bigger push for a formal BYO-PC program.



Learn more and begin to design your program

Reach out today for a free consultation on how you can bring a formal BYO-PC program to your organization, including how you can best design your strategy, and what modern BYO-PC tools might drive your program.

HOW CAN VENN HELP YOUR ORGANIZATION SUPPORT SECURE BYO-PC?

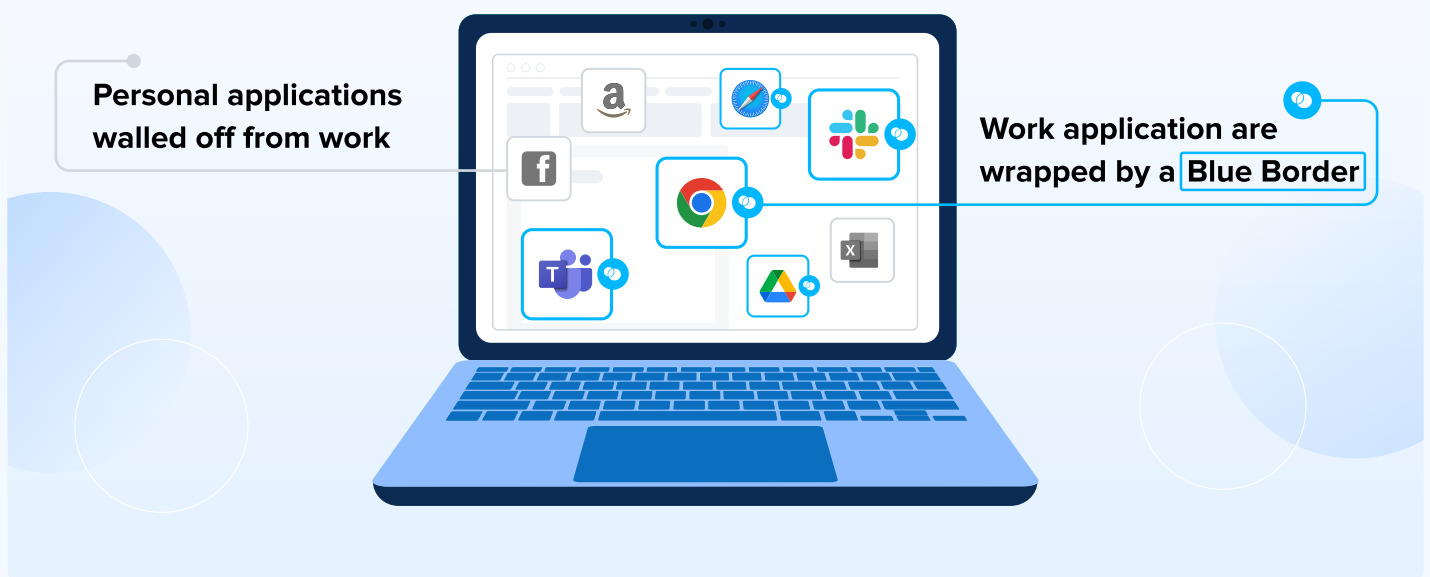
Venn is the first purpose-built patented technology for Secure BYO-PC. Venn secures remote work on any unmanaged or BYOD computer with a radically simplified and less costly solution than virtual desktops or having to lock down every PC.



Similar to an MDM solution but for laptops – work lives in a company-controlled secure enclave installed on the user's PC or Mac, where all data is encrypted and access is managed. Work applications run locally within the enclave – visually indicated by the Blue Border™ – where business activity is isolated and protected from any personal use on the same computer. Company data is now protected without having to control the entire device, and as a result, remote work is secured without the cost, complexity and performance issues of VDI.

As happened in the past with mobile phones, employees want to use their preferred computer – not have one for work and one for personal – while companies are eager for ways to avoid buying, shipping and locking down computers. Security and compliance-driven companies gain protection for what counts and employees enjoy more freedom, flexibility and privacy.

With Venn, Secure BYO-PC technology is now a reality. Over 700 security and compliance-driven organizations, including Fidelity, Guardian, and Voya, trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards.





Thanks for Your Attention!

Want to hear more about how Venn.com can help your company?

[Book a Short Demo](#) >

We invite you to:

- Subscribe to get more insights and tips on this matter
- Follow us for more information about Venn's BYO-PC revolution



[Website](#)



[Blog](#)



[Linkedin](#)



Reprogramming IT security
for remote work



More freedom and choice in
the way we work remotely

