



Step Inside Blue Border™

Venn protects company data and applications on
the BYOD computers used by contractors and
remote employees – without VDI.



The Secure Enclave Built for Enterprise

Venn protects company data and applications on BYOD computers used by contractors and remote employees without VDI.

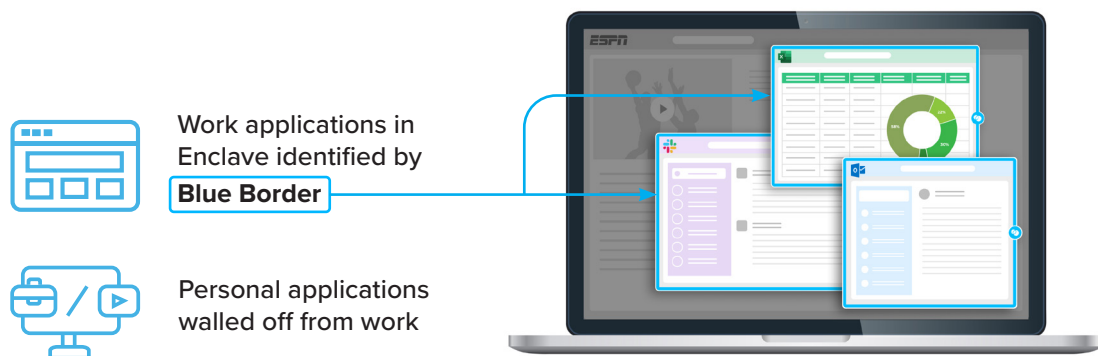
In today's fast-paced business landscape, organizations increasingly rely on contractors and remote employees who use personal, unmanaged, or third-party managed devices (BYOD). Consequently, traditional solutions like Virtual Desktop Infrastructure (VDI), VPNs, and enterprise browsers fall short in addressing the security, compliance, and usability challenges of BYOD.

Introducing Venn's Secure Enclave Built for Enterprise: patented technology that protects company data and applications on BYOD devices. Applications run locally within the Enclave, ensuring encrypted data, enforced corporate policies, and seamless productivity without the latency or complexity of virtual desktops.



Step Inside Venn's Blue Border

Venn's Blue Border™ is similar to an MDM solution, but for laptops. Work lives in a company-controlled Secure Enclave installed on the user's computer, where all data is encrypted and access is managed. Work applications run locally within the Enclave – visually indicated by a blue border – isolating and protecting business activity from any personal use on the same computer. Company data is secured without controlling the entire device while ensuring end-user privacy for everything outside of Blue Border.



What happens in the **BLUE BORDER** Stays in the **BLUE BORDER**

With Venn, anything a user does inside the Blue Border is protected and secure from anything a user does on the personal side. Anything a user does personally on their laptop outside of the Blue Border is not going to be seen, tracked, or monitored by Venn.



Benefits of Venn



REDUCE COSTS

Reduce or eliminate the cost of buying, shipping, managing and securing laptops and/or virtual desktop infrastructure. Zero backend infrastructure.



ENSURE SECURITY AND COMPLIANCE

Venn helps you achieve or maintain compliance on computers that you don't fully manage or lock down. Protect company data from exfiltration and stay in compliance with strict industry standards such as SOC2, FINRA, SEC, HIPAA, etc.



ALLEVIATE IT BURDEN

Refocus IT resources on important initiatives, instead of on locking down employee computers or supporting complex VDI.



WORKFORCE AGILITY

Rapidly onboard/offboard remote workers in minutes. Hire any employee or contractor anywhere, on the PC or Mac of their choosing.



OPTIMAL PERFORMANCE & EXPERIENCE ON ANY PC OR MAC

Unlike VDI, which often suffers from latency and performance issues, especially during video conferencing, Blue Border launches work applications directly on the local computer for optimal performance and a familiar user experience.



SUPPORT USER CONVENIENCE AND PRIVACY

Allow workers to use their personal computer for both work and life with clear separation between the two.

Venn's patented technology provides companies with a new approach to securing remote employees and contractors working on unmanaged computers.

An Alternative to Virtual Desktops

Eliminate the cost, complexity, and usability challenges

Virtual Desktop Infrastructure is not always the best choice for protecting apps and data on remote and unmanaged computers. VDI can be complex, difficult to manage, costly and often leads to user frustration. It's also redundant for browser-based applications and struggles with video performance. With Venn, work and applications run locally on a user's machine, delivering a seamless native experience and superior performance.

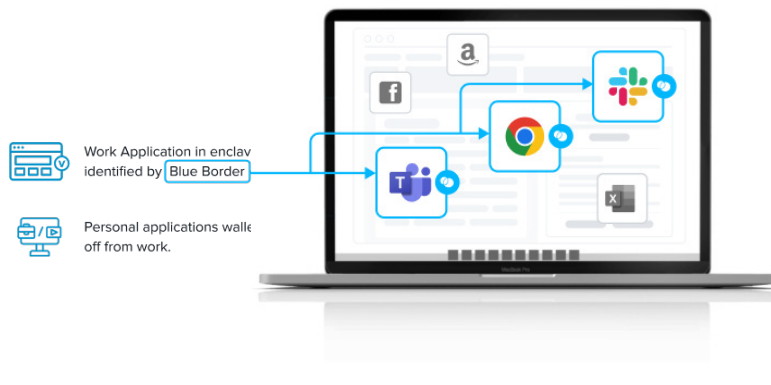


Corporate Device Freedom

Get Out of the Hardware Business

Buying, shipping, managing and securing laptops for every remote employee and contractor is time-consuming and diverts IT teams from more strategic initiatives. With Venn, users can work on any unmanaged device, eliminating the need to manage inventory or chase down devices.

How Blue Border™ protects applications and data



- Centralizes administrative control over work data, application and peripheral use
- Provides ability to remotely enable, suspend, terminate or wipe at press of a button
- Ensures that all network access is policy-controlled and routed through encrypted private company gateway
- Device compliance checks gate access, enforcing hygiene & compliance policy

Application Isolation

Work applications run locally within the Secure Enclave – visually indicated by Venn's Blue Border™ – where business activity is isolated and protected from any personal use on the same computer. Blue Border secures all work applications, including Chrome, SaaS Apps, Office 365, Edge, Adobe, Safari, Web Conferencing (Zoom, Webex, Teams, etc.) and many others.

Fine-Tune Security Policies to Fit Your Organization

Configurable policies allow you to designate specific applications for work, ensuring that only those assigned to a user by an admin are allowed to run within Venn. Applications running within Venn are governed by admin configurable DLP policies that govern functions such as copy/paste, screen sharing, printing, and downloads.

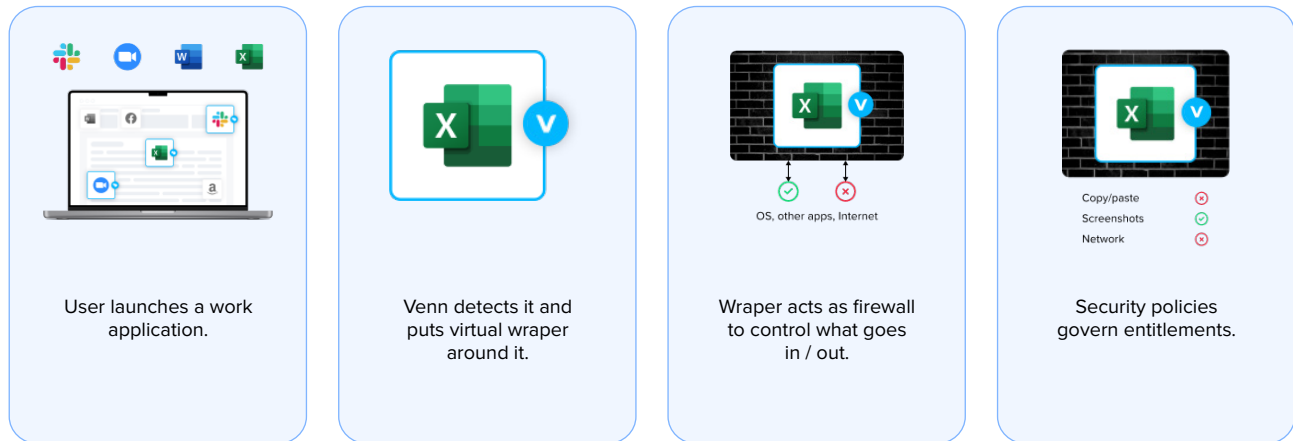


SEC

FINRA

NAIC

How Venn's Blue Border™ protects work

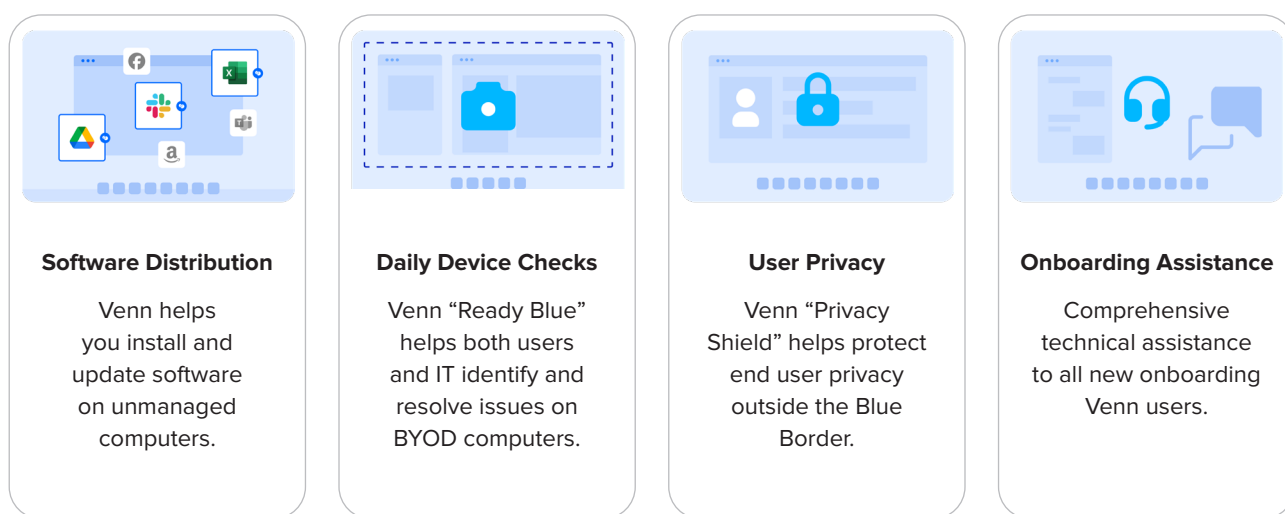


When a user launches a work application, Venn puts a virtual wrapper around it, visually indicated by the Blue Border around each application window. That work application is then running inside of the Secure Enclave, which acts like a firewall, controlling what data can go in or out. Security policies allow companies to restrict actions such as data movement, printing, clipboard copy/paste, screen sharing, uploads, and more. Security policies can be highly granular and applied to individual users or groups.

Unlike VDI, work applications are launched directly from the computer and run locally, rather than from a remotely delivered desktop, ensuring optimal performance and a familiar user experience.

Managing a BYOD workforce is about more than security.

Venn simplifies onboarding for IT teams, helping them quickly integrate new users, meet compliance requirements, and ensure user privacy is protected.



Solving the security and operational challenges of BYOD workforces

Venn's mission goes beyond just securing company data on BYOD laptops; we aim to empower our customers to fully embrace and optimize BYOD. To do this, we continuously enhance Blue Border with advanced tools and controls that address common BYOD challenges.

Venn Application Delivery ensures that software applications are swiftly deployed and consistently maintained across all Venn-enabled devices. With Venn ReadyBlue, device status snapshots allow users and IT teams to quickly identify and resolve issues, keeping operations smooth. Venn Privacy Shield embodies our commitment to privacy through innovative architecture and patented technologies, protecting user privacy outside the Blue Border. These tools reduce friction and make BYOD adoption more seamless and efficient.

Secure Company Data on BYOD and Unlock Freedom, Security, and Productivity

Join the 700+ organizations including Fidelity, Guardian, and Voya that trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards. [Book a demo](#) today and discover how Venn can transform your remote work BYOD strategy by unlocking cost savings and limitless workforce agility.

THANK YOU

Want to learn more about how Venn
can secure your BYOD workforce?

[Book a short demo](#)

And be sure to follow us on socials
for the most up-to-date news.

