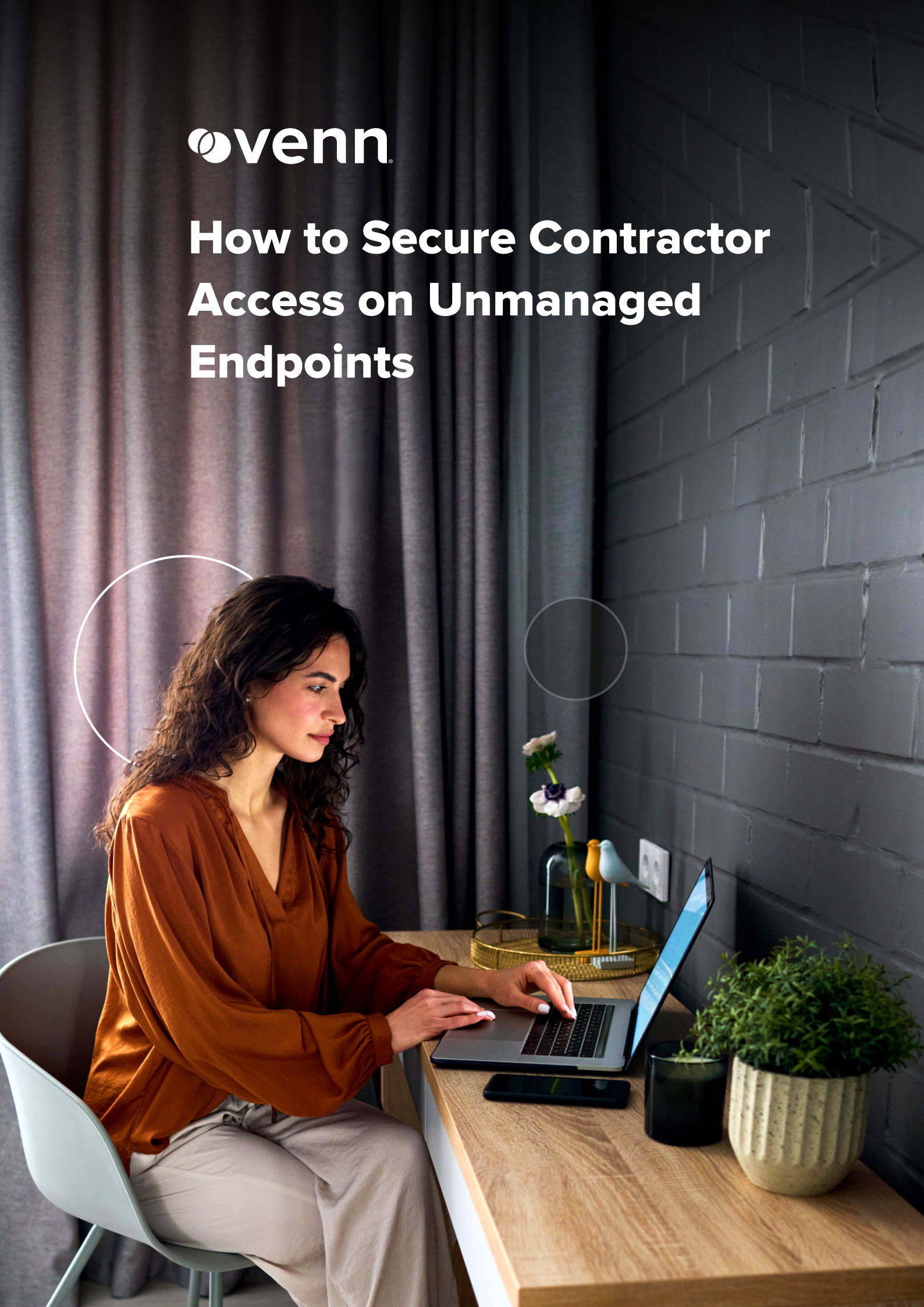
venn

How to Secure Contractor Access on Unmanaged Endpoints



The Rise of Contingent Workforces & BYOD

The nature of remote work has evolved, and with it, the enterprise risk landscape. Today's organizations increasingly rely on contractors, freelancers and third-party vendors to stay agile and competitive. Simultaneously, BYOD practices have evolved as the simpler IT option for this distributed workforce. Together, these trends offer organizations agility, speed, flexibility, and cost savings. However, they also increase exposure to growing security and compliance risks that legacy tools like virtual desktops (VDI) were never designed to manage.

This eBook explores the new reality facing IT and security leaders: a dissolving network perimeter, the proliferation of unmanaged and BYOD devices, and a blurring of the personal and the professional when it comes to access to data and business applications. Visibility gaps are beginning to form and are creating policy enforcement challenges that traditional virtualization, endpoint protection and network access security solutions cannot effectively address.

This perimeter-less architecture opens the door to data leakage, inconsistent security hygiene, shadow IT, offboarding blind spots and unmanaged fourth-party risks. In industries that rely on contractors but operate under stringent regulations (healthcare, finance, etc.), compliance is another major issue to address.

Common risk mitigation strategies, such as shipping locked-down laptops or deploying VDI, have limitations. They introduce cost, complexity – and in the case of VDI, latency and a poor user experience – often leading users to circumvent security measures entirely.

To close the security gap without sacrificing workforce productivity and agility, a new solution is needed: one that offers enterprise-grade security and compliance controls while respecting the work-blended-with-personal realities of BYOD.

Secure Enclave technology offers that path forward. It enables data protection and policy enforcement at the endpoint level, without taking over the entire machine. The result is a balance of security, user privacy and operational efficiency.

The future of remote work is flexible, and so must be the security architectures that support it. For IT leaders, embracing this shift isn't optional. It's fundamental to reducing third-party risk, sustaining innovation and protecting the organization's business-critical data. Read this eBook to discover how you can seamlessly and securely support third-party contractors, turning yourself into a business enabler and leader in an agile and competitive environment.

Table of Contents

The Rise of Contingent Workforces and BYOD

The modern workforce is undergoing a significant transformation. More and more organizations are relying on freelancers, contractors and gig workers to fill skill gaps, scale their operations quickly, and reduce overhead costs. In today's volatile economic and technological landscape, contractors are an essential part of any business attempting to remain competitive and agile.

90+ Million

US workers will freelance by 2028

53%

of freelance GenZ workers are moving to full-time freelancing

$1.27 Trillion

Were contributed to the US economy from freelancing in 2023

Source

This shift is reshaping traditional employment models and challenging long-held assumptions about how work gets done. It also reflects a broader move towards flexibility, autonomy and cost-efficiency in employment practices.

One of the consequential practices is BYOD (Bring Your Own Device), which has now become common in many workplaces. Most contingent workers operate independently and prefer using their own devices, which they are already familiar with. In addition, contractors often juggle multiple clients and wish to avoid the hassle of switching between multiple machines.

On the employer side, allowing BYOD makes business sense. Provisioning and shipping devices is costly and logistically complex (more on this below), particularly for short-term engagements or niche roles brought in for specific tasks.

BYOD, Third-Party Risks, & Security Gaps

As previously mentioned, expanding the workforce provides organizations with significant business advantages, like access to global talent, agility to scale quickly, and reduced costs. But contractors are not only an HR or business issue. They are also an IT challenge.

When organizations bring in external workers, whether for short-term projects or to fill specialized roles, IT becomes responsible for provisioning access, setting up devices and ensuring connectivity to internal systems. This often needs to happen at speed and scale, especially in quickly growing or project-driven environments.

Sometimes, security is brought in, too. (Though more often than not, it's too late in the process, after contracts are signed, access is granted and work has already begun). Security teams need to define access controls, vet contractor devices and environments, monitor activity, automate offboarding and provide security training.

The Aftermath of BYOD Without Security

Not applying security controls (whether on time or at all) when working with contractors and BYOD can result in significant third-party security gaps:

DATA LEAKAGE

Sensitive corporate data can be saved, copied, or transferred to personal apps, cloud storage, or email accounts.

INCONSISTENT SECURITY HYGIENE

Personal devices may lack enterprise-grade security controls like encryption, antivirus software, firewalls, or regular OS and app updates, rendering them vulnerable to attacks.

DEVICE SHARING AND INSECURE USE

BYOD devices might be shared with family members or used in insecure environments (like public Wi-Fi), exposing them to unauthorized access or malware infections.

CHALLENGES WITH OFFBOARDING

When employees or contractors leave, it's difficult to guarantee that all work data is deleted from their personal devices. Sensitive data may remain accessible.

SHADOW IT

Contractors often resort to using their own productivity tools, file sharing services, communication platforms, project management tools, or GenAI systems. These tools can bypass organizational security policies and lead to data being stored outside approved and visible systems.

THE SUPPLY CHAIN'S SUPPLY CHAIN

Contractors might subcontract work to others without the knowledge or consent of the hiring organization. This creates fourth-party risk that is rarely assessed, monitored, or included in formal onboarding processes.

Contractor Requirements for Regulated Industries

Some of the most critical and foundational industries rely on contractors and third-party agencies for specialized expertise, scalability, and operational flexibility.

Businesses that offer these contractor services and the organizations hiring them aren't just dealing with security gaps. They also need to meet the following regulations:

Industry	Examples	Regulations
Healthcare	• Traveling nurses, physicians & therapists • Telehealth providers • EHR specialists • Medical device and IT technicians • Compliance experts • Billing specialists • Clinical research and data analysts	• HIPAA • HITECH Act • GDPR/CCPA
Finance & Insurance	• Seasonal insurance agents • Compliance and regulatory auditors and consultants • Brokers • Investment advisors/Wealth management • Accounting and tax specialists • Loan specialists	• PCI-DSS • FINRA • SEC • SOX • GLBA • GDPR/CCPA
Government	• Seasonal insurance agents • Compliance and regulatory auditors and consultants • Brokers	• FedRAMP • FISMA • NIST
Education	• Researchers • Course developers and curriculum designers • Tutors and special education professionals • Instructional coaches • EdTech support and implementation staff	• FERPA • COPPA • GDPR/CCPA

Why Traditional Security Tools Fail

The traditional security stack should have been able to protect from these security risks and, consequently, help you meet compliance regulations. However, they struggle to do so. This stems from the fact that they were built for a world that no longer exists. They were designed and developed at a time when all employees were full-time and commuted into the office every day for a full day of work.

IT and security teams are facing a new reality:

1. **A Dissolving Perimeter** – Traditional security tools focus on defending the network perimeter, protecting on-premises data, managing centralized systems, and controlling external access points like VPNs. But now, employees work from anywhere, applications live in the cloud, and sensitive data is distributed across countless environments. In the case of contractors, this is amplified even further. The concept of a perimeter has all but vanished, demanding new ways to secure the network, data and access.

2. **BYOD and Unmanaged Devices** – As aforementioned, employees and contractors increasingly use their own laptops, tablets, and phones. These personal devices often lack the hardened security controls of managed endpoints, requiring more modern security tools to enforce policies and tackle blind spots that impact governance efficacy.

3. **Blended Digital Lives** – Security models used to rely on a clear divide between work and personal life. That's gone. These days, employees check work emails on personal phones, join meetings over unsecured home Wi-Fi, and save files across both corporate and personal cloud accounts. In the case of contractors, they juggle multiple clients and personal matters on their devices.

Legacy tools like virtual desktops lack the context-aware controls needed to navigate this gray area, leaving organizations exposed. Organizations need a new way to address these security gaps and data sprawl.

Point of Failure	What's Needed Instead
Perimeter-based thinking	Zero trust approach, access management
Visibility and control of end devices	MDM for laptops
Mixing work and personal	Demarcating work and personal digitally, not physically

What This Means for Technology Leaders

The failure of traditional security models has serious implications for tech leaders. This is no longer just a “security team” problem. It’s a leadership issue that affects innovation velocity, operational risk, customer trust and regulatory standing.

Here’s what it means in practice:

- You’re likely exposed in places your security tools aren’t even looking.
- If security isn’t enabling the business, it’s blocking it.
- Non-compliance isn’t just a legal risk, it’s a business continuity risk.

Organizations need to find a solution that enables securely working with contractors & BYOD.

Attempted Solution #1

Shipping Laptops

One of the most common solutions organizations attempt to implement for overcoming BYOD security challenges is buying and shipping devices to contractors. These devices are pre-configured with endpoint protection, locked down to restrict software installation and external use, and lack admin privileges.

This approach aims to replicate the same controls available for in-house employees, while maintaining consistency in performance, efficiency and security across the organization.

Challenges and Security Gaps of Shipping Laptops

HIGH COSTS

Hardware procurement, international shipping and retrieval logistics are expensive and time-consuming. Physical devices can be lost, stolen, or repurposed for unauthorized use. When the contractors complete working with the organization, devices aren't always sent back.

$260,000+

Source

The annual cost of lost hardware for a 500-agent BPO organization.

NO SCALABILITY

Sending a device to one contractor is one thing. But scaling this model to hundreds or thousands of telehealth contractors or insurance agents during CAT season is quite another. It introduces logistical chaos and turns the IT department into a shipping department, defocusing them from important IT initiatives and projects.

SLOW TIME-TO-PRODUCTIVITY

Provisioning and shipping delays slow onboarding. Contractors may sit idle while waiting for a device, wasting time and creating frustration. In some high-churn environments, like call centers, they might move on to another client by the time the device arrives.

COMPLIANCE & AUDIT RISKS

Shipping devices makes it difficult to maintain control over how data is used and stored, because IT teams lose visibility into whether it is being moved to unauthorized locations and over geographic data residency. In addition, devices might be used in untrusted and unaudited environments, like public networks and shared spaces.

SHADOW IT AND WORKAROUNDS

If contractors find the device too restrictive, they may circumvent controls with unauthorized devices or accounts. This leads to unsanctioned tool use and visibility and security gaps for security teams.

Attempted Solution #2
Virtual Desktop Infrastructure (VDI)

The second popular solution organizations have used to try to secure BYOD is VDI. VDI hosts desktop environments on a remote server that is managed by IT. Contractors can then connect to the virtual desktop through a secure client (often over VPN). In the evolving desktop-as-a-service (DaaS) model, the virtual desktop infrastructure moves from a company-run data center to services hosted by cloud providers.

Challenges and Security Gaps of VDI

SHADOW IT AND WORKAROUNDS

If contractors find the device too restrictive, they may circumvent controls with unauthorized devices or accounts. This leads to unsanctioned tool use and visibility and security gaps for security teams.

Sample VDI Costs for a 2000-employee organization

STOP BUYING COMPUTERS | VDI REPLACEMENT

Number of Employees: 2000

Venn can save you **$912** per employee which sums up to **$1,824,000** a year.

	Annual cost per employee			Overall
Cost Breakdown	**Current Cost**	**Cost if you reduce VDI by 70%**	**Potential Savings per User**	**Total Potential Savings if you Reduce VDI by 70%**
VDI subscription cost	$840	$250	$590	$1,180,000
MS RDP cost	$77	$27	$50	$100,000
Infrastructure cost	$300	$100	$200	$400,000
Headcount cost	$144	$72	$72	$144,000
Total	**$1361**	**$449**	**$912**	**$1,824,000**

USER EXPERIENCE ISSUES

Latency and performance degradation are common in VDIs, especially with bandwidth-heavy apps, like design, video, and real-time apps. In addition, since VDI relies on Internet access, any connection to SaaS apps can be choppy. Finally, VDIs do not support Macs well. This means your Mac contractors might not be able to perform their jobs.

Here's what users have to say about VDI:

> **VDI does it suck as much as i think?**
>
> So just wondering if any one has any opinion on VDI in large (2000+ endpoint) enviroments?
>
> I work as the team leader on a reasonably high level helpdesk for a IT company serving a number of large clients. We deployed VDI over our internal infrastructure over a year ago and after facing huge backlash from users its only now at what I would call a usable level performance wise after over a year of tweaking.
>
> I found it very volatile and hard to support which was the very thing its designed to help.
>
> Against all my advice (not that its taken that seriously) this tech has been sold to our biggest client a leading tertiary institute and already gone 6 months and 100,000 dollers over budget. The lead engineer has left for a competitor and we are facing a very hard time come February when students start using this on an extreme level.
>
> The hardware it sits on is not an issue as it is the best stuff available and more than enough spec wise. Im wondering if anyone has had good experience with VDI and if they have any tips. gotchas etc that could help us in the NY.

MAINTENANCE COMPLEXITY AND OPERATIONAL OVERHEAD

VDI environments can be intricate to manage due to the number of interdependent components. Even minor configuration changes require rigorous testing. In addition, patching and troubleshooting across multiple virtual desktops can consume significant IT resources.

SCALABILITY LIMITATIONS

Spinning up new desktops for seasonal contractors or rapid business growth can overwhelm existing infrastructure. Additionally, each user's resource demands vary, making performance inconsistent without over-provisioning, which increases cost and complexity.

SECURITY GAPS IN ACCESS AND DATA ISOLATION

Accessing VDI from BYOD does not solve security issues that arise from endpoint risks. In addition, misconfigured access policies, weak identity controls, or insufficient segmentation between virtual desktops can lead to data leakage or lateral movement by attackers.

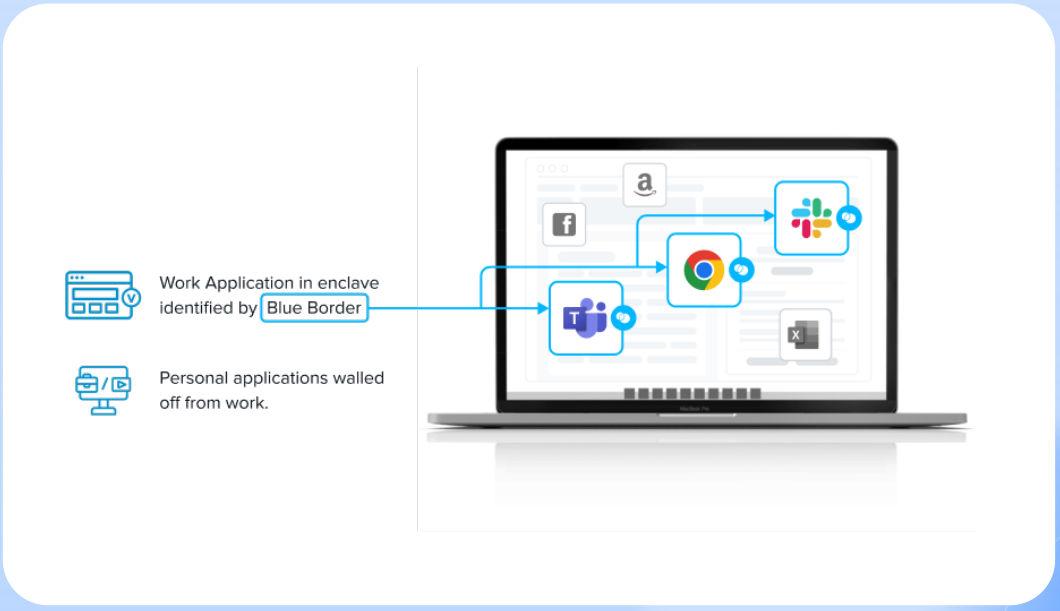
New Solution #3

Secure Enclave Technology

Rather than replicating legacy ways of thinking (shipping devices, remotely hosted desktops) to a modern problem, it's time for a modern solution.

A Secure Enclave is a technological solution that was developed specifically to protect company data and applications on BYOD computers used by contractors and remote employees. 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, protecting and isolating business activity from any personal use on the same computer. Company data is secured without controlling the entire device, all while ensuring end-user privacy for everything outside the Enclave. One such solution, Venn's Secure Enclave, uses a Blue Border to visually signal to users which windows are for work and which are personal.



Core Benefits of Venn's Secure Enclave Technology

COST REDUCTION

No more buying, managing and shipping company-owned PCs and Macs, or spending top dollar for bulky VDI licensing and infrastructure.

SECURITY AND COMPLIANCE

Company data is protected from accidental or malicious exfiltration, compromise or loss. A Secure Enclave also provides turnkey regulatory compliance with industry standards including HIPAA, PCI, SOC, SEC, FINRA and more.

WORKFORCE AGILITY

Contractors can be onboarded or offboarded in minutes. This makes it easy to hire contractors for short-term or seasonal engagements.

ALLEVIATING IT BURDEN

IT resources are focused on important strategic initiatives instead of wasting time managing and locking down employee laptops or supporting frustrated users on complex VDI infrastructure.

USER CONVENIENCE

Contractors can work locally with their preferred installed applications with clear separation between work and personal uses.

USER PRIVACY

Companies have full control over everything inside the Secure Enclave, but don't have access to anything on the machine outside of the Enclave, ensuring end-user privacy.

Key Takeaways for CISOs and IT Leaders

1. **Legacy Security Architecture is Obsolete in a BYOD and Contractor-Driven World**

   Traditional perimeter-based tools were designed for a world where work happened in centralized offices on managed devices. Old tools not only fail to protect, they actively create blind spots, particularly around device visibility, access control, and data sprawl.

2. **Third-Party Risk Is Now a Core Business Risk, Not Just an IT Concern**

   Contractors are not a side channel, they're critical to scaling modern businesses. But without proper access governance, device vetting, and security enforcement, they become the fastest-growing vector for security breaches

3. **BYOD Is Here to Stay. Security Must Adapt, Not Resist**

   Trying to force contractors into legacy IT molds (e.g., provisioning locked laptops or rolling out heavy VDI) leads to high costs, poor experiences, and security workarounds. Security teams need to adapt to this modern way of working.

4. **Compliance Cannot Be an Afterthought in Contractor Ecosystems**

   From HIPAA and PCI to SEC, contractors have access to data that is subject to serious regulatory scrutiny. Organizations that don't extend compliance controls to contractors and their devices are at risk of fines, breaches, and reputational damage.

5. **Secure Enclave Technology Offers a Pragmatic Way Forward**

   Secure Enclaves represent a modern approach to contractor and BYOD security. Instead of attempting to control the entire device (which can spark privacy concerns and slow adoption) or remotely host applications and data (which creates latency and frustration), secure enclaves isolate work environments at the application level and host everything locally. This allows CISOs to enforce enterprise-grade control, like data encryption, DLP, and continuous monitoring, without impacting personal apps or files, or causing latency.

CISOs can then enforce security controls while preserving workforce agility and user privacy. Organizations benefit from faster onboarding, lower infrastructure costs, and an elevated user experience. Compliance is easier to achieve and IT teams can shift from reactive troubleshooting to proactive enablement, supporting workforces wherever they are, with secure, policy-compliant environments that work seamlessly across borders and networks.

About Venn

Venn, the leader in BYOD Security, is revolutionizing the future of remote work. Venn is the innovator behind Blue Border™ – the world's first purpose-built technology that protects company data and applications on the personal, unmanaged, or third-party managed computers used by contractors and remote employees.

Venn's customers are empowered to achieve the cost savings and workforce agility of BYOD, while ensuring robust data protection and compliance with regulations like FINRA, SEC, HIPAA, NAIC, and SOC 2. With Venn, work lives in a company-controlled Secure Enclave – visually indicated by Blue Border™ – protecting and isolating business activity from any personal use on the same computer (PC or MAC.)

Join the 700+ organizations, including Fidelity, Guardian, and Voya, that trust Venn to meet to secure their business critical data. Discover how Venn can secure your BYOD strategy. Visit venn.com.

Book a Demo

venn

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