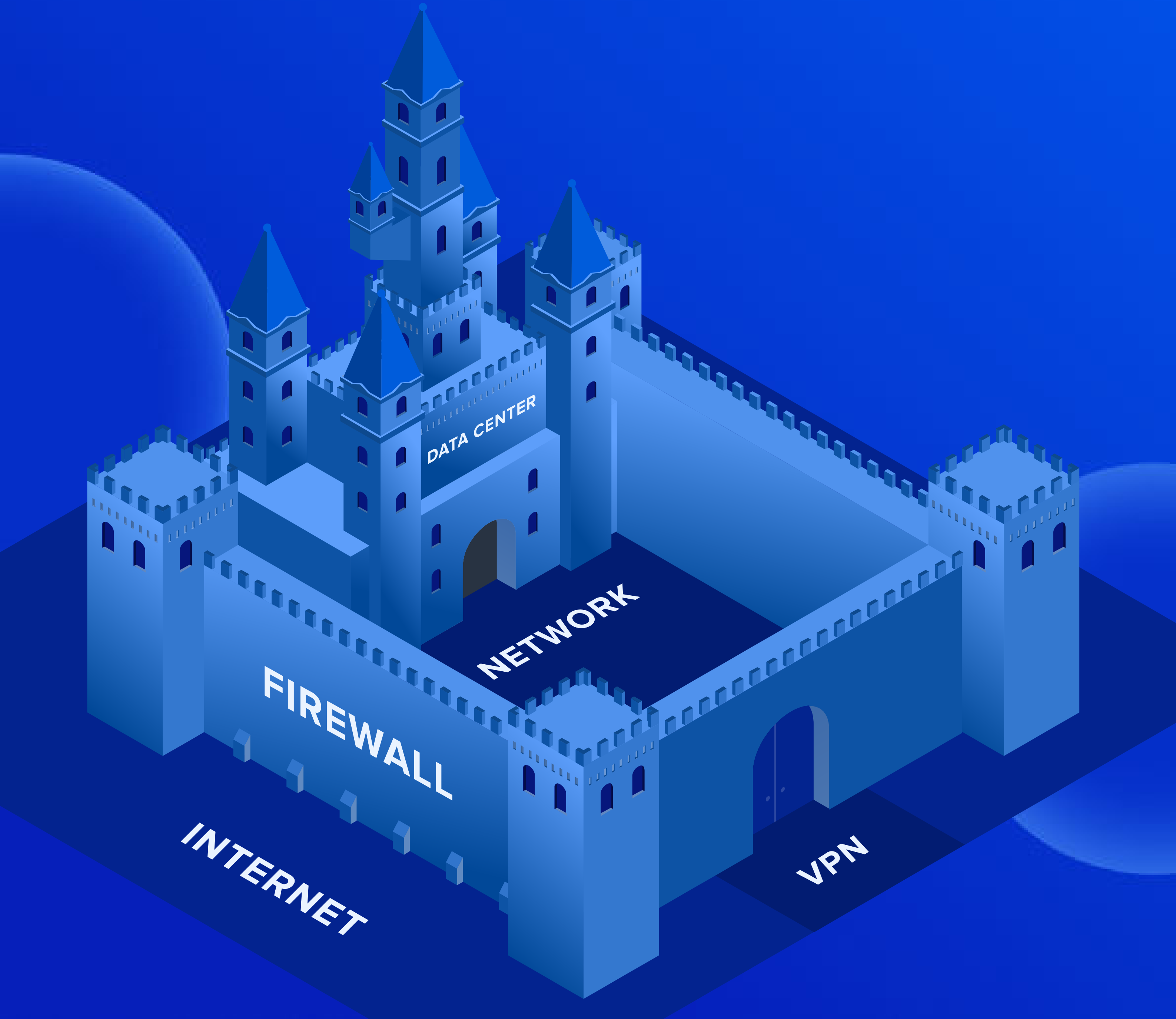
venn

WHITEPAPER

Zero Trust for Securing Hybrid and Remote Workers

One goal, two priorities. How IT and Security can find the winning approach to securing remote work



Modernization can be messy, and that's OK. The key is making it less risky.

Connectivity is complexity. That's its power, linking people, machines, applications, and ideas, across a business. These connections can define the org itself.

Virtualization and the cloud give us more ways to connect these nodes, empowering orgs to meet unique needs with a stack of carefully optimized solutions. But how does all that flexibility fare when it comes to unifying ideas like Zero Trust and how to apply it to securing remote workers?

This ebook looks at how the modern enterprise gets connected and secured, and how these pieces can fit with modern Zero Trust decision-making. We'll examine key connectivity platforms for remote work with zero trust principles, and practical realities, in mind.

ZERO TRUST IS A COOL IDEA AND A COMPLICATED REALITY

As with all things security, if we could ever just press pause, it would be easy. As Bruce Sterling wrote, the future has already been here for some time, it's just been unevenly distributed.

✓ The pandemic closed some of those gaps, forcing organizations to quickly accelerate transformation. That's the good news.

✕ The bad news is, predictably, that bad guys and girls were also working overtime to maximize their reach and impact, carefully optimizing threats and tactics for the specific conditions of the moment.

This means any strategic security response, zero trust included, must be similarly optimized for this new normal and, more importantly, all the possible even newer abnormals that might come next.

Perimeters aren't dissolving, they've effectively disappeared. We're in an era of relentless virtualization, where digital is letting us abstract more and more old infrastructure. It unlocks many more ways for users to connect and collaborate, but it also dramatically increases the attack surface of the modern remote-first, cross-device workplace. And that's not the only thing that's different.

PRODUCTIVITY IS STILL THE WHAT, BUT THE HOW IS CHANGING

As the battle between work from home and return to office continues to rage post-pandemic, it's still hard to see a clear eventual winner between the two. Ultimately, it will boil down to percentages: hours worked on site vs. tasks performed everywhere else.

We know that 60% of organizations have said they're **invested in a hybrid or remote-first future.** This is predictable, and we also know it's increasingly an expectation of new employees. It also gives organizations access to a global talent pool, and they won't give that up easily. This means lots of connections from outside the office. These must be secured.

At the same time, **office sizes aren't shrinking by much just yet.** We've only seen a small reduction in square footage, but continued uncertainty and adoption of more remote work sees other giants like Cisco downsizing. But there will always be some employees accessing applications and data stored on prem, even as the multicloud obviously remains critical.

And, no matter where you work, some of our **tools are getting heavier.** Even with the rise of web apps and the cloud, GPU-heavy apps are growing across the enterprise, including data science. Those platforms are growing at about 7% CAGR. This means those remote connections have special performance requirements too.

BRING UNIFORMED SECURITY TO AN UNRULY WORLD

Just as technology needs evolve, security and compliance demands are shifting in parallel. A combination of new tools and updated strategies are giving organizations what they've always wanted from somebody: a unifying set of best practices and principles.

Zero trust network architecture thinking, also referred to as ZTNA or simply 'zero trust', is just one such triumph of collective action over competitive dynamics.

Giving organizations some fundamentals they can use to shape their own technology and security thinking. To help us understand the challenges of securing remote productivity, we'll focus on three.

To help us understand the challenges of securing remote productivity, we'll focus on three.

Verify explicitly is really the key to operationalizing zero trust. Zero trust essentially implies the need for overwhelming verification—believe nothing, test everything. Building these explicit verifications into systems and hand-offs is critical, and tech can help it happen at scale.

Assume breach is probably the second most essential zero trust fundamental. As strong as our defenses are, we should always assume they can, and have been, compromised. This shifts our focus to defenses in depth, building not to prevent attacks but limit their reach.

The traditional IT default was to over-assign permissions and privileges, creating predictable security risks. The **use least privilege** paradigm re-orients the default to ensure users only get the permissions they absolutely need.

1 **Verify explicitly**

2 **Assume breach**

3 **Use least privilege**

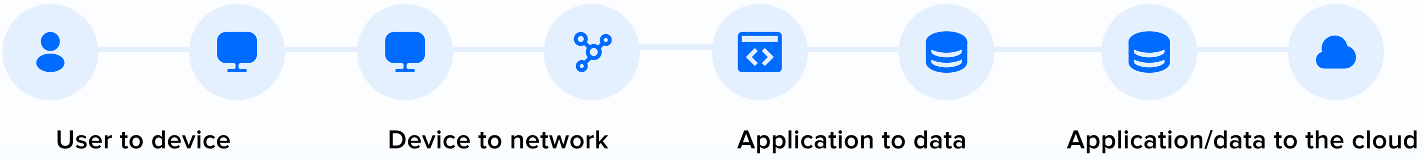
So what?

We focused on these three principles for a couple of reasons. They're not just fundamental to ZTNA success, but also appropriate to the complexities of hybrid and remote.

The less you can trust the network and the device, the more verification you have to do. This means remote exponentially increases the volume of verification required, including permissions and entitlements to thousands of human and machine users.

Using least privilege also gets trickier, because you're managing permissions across more places, and it sure would be easy to just max everything out globally and stop worrying about it. Finally, assume breach takes on new urgency as work life and home life collapse. A breach of a personal device, password or network suddenly also puts enterprise assets at risk.

IMPACT ON IT INFRASTRUCTURE: WHAT IT ALL MEANS



Embracing zero trust principles as ideas is easy enough. Implementing them in practical, mission-oriented ways—that's where the fun starts. The new hybrid reality, all those connections, all those use cases, all adds up to a lot of complexity on and off prem.

IT is tasked with building and running those connections, and it's security's goal to keep them all protected. While the rise of DevOps and SecDevOps drives closer and closer collaboration, the two teams are still optimizing for similar-but-not-the-same outcomes.

ONE PRIORITY, TWO PATHS
DIGITAL MODERNIZATION IS THE GOAL. BUT THAT MEANS DIFFERENT THINGS TO SECURITY AND IT

IT environments must be always on and responsive, delivering excellent application experiences across all combinations of connectivity listed above.	**Security teams** are focused on keeping information secure, leveraging IT consistency to develop repeatable controls.
• **Embracing consistency** where possible, moving from complex legacy systems to larger pieces of platform. • **Understanding and building for intent** when designing network and application experiences. • **Virtualizing more and more** of the network and all of its utilities, reshaping branch office connectivity and larger network topology at the same time.	• **Building a unified view** of threats across the whole environment, using consistent tools for detection and response • **Creating richer and richer data-driven context** for understand user behavior and anomalies • **Virtualizing traditional hardware controls** and building new ways of managing users and identities across multiple environments and clouds

Consistency is huge-but it only gets us so far. Ultimately, there's last inch customization required for reasons such as compliance or performance. And that's where the stack to support hybrid and remote work starts to get rich, and a little unsteady.

But we can use these outcomes as a lens for understanding why orgs build the remote connectivity stacks they do—and then how we might be able to map some of that chaos to the Zero Trust principles discussed before.

TOURING THE STACK

You're probably using some combination of these applications across your organization. That's a key takeaway here. Try as we might, there's really no one-size-fits-all approach to securing remote connectivity. This explains the need for IT and security teams to deploy a mix of old and new technologies as they try to secure the connections critical to productivity.

Secure Desktop:

GUARDING THE WORKSPACE: SECURE DESKTOP

Secure desktops segregate certain applications or data inside a separate virtualized workspace.

- Users log into their physical device, and then a separate virtualized 'container'.
- Sensitive data can't be shared or copied beyond the virtualized perimeter.
- Ideal fit for organizations keenly focused on PII security.

For IT	For SECURITY
IT teams must install the solution and manage access between applications and the secure desktop.	**Security teams** get easy visibility into where PII lives, how it moves, and who has access.
Users struggle with the highly restrictive nature of the secure desktop, especially in today's multitask-mad world. Moving between secure and unsecure applications can be complex.	Secure desktops do an excellent job of segmentation, a ZTNA fundamental. But user identity and device access still need to be carefully managed elsewhere.

VPN:

SECURING THE CONNECTION: VPN

VPNs use software to secure the connection between the desktop and proxy server.

- Users log into the VPN client on the device.
- Traffic between the device and the application is encrypted.
- Ideal for frequently remote users connecting from managed devices.

For IT	For SECURITY
IT teams can install/require installation of the VPN on managed devices.	**Security teams** have long relied on VPN to bring traffic safely to and from the network.
Veteran remote users are probably familiar and comfortable with VPNs, although complaints about latency and performance are universal, especially on new tools and video platforms.	VPN tunnels simplify how information is protected as it moves from user to application and back again, but only the pipe is protected, leaving the user and device wide open elsewhere.
	VPNs do add a layer of security to remote access, adding additional checks to standards Windows authentication of users, although only access to the pipe is secured.

VDI:

VIRTUALIZING THE DESKTOP: VDI

Virtualized Desktop Infrastructure (VDI) delivers applications and data inside a self-contained software environment, delivered from shared resources managed via a hypervisor to a 'browser' on the endpoint.

- Serves distributed needs from dense resources (pre-cloud), using VM to deliver applications.
- Really well-suited for environments with limited application needs/frequent user turnover and on prem deployments.
- Ideal for environments where most users are still on prem, especially businesses that have shift workers or manage lots of contractors.

For IT	For SECURITY
VDI is great for users who can be productive with a limited and restricted set of tools. It's not ideal for environments where users expect-or need-any flexibility in how they get their job done. Latency and performance issues can also impede productivity and hamper user satisfaction.	VDI secures the desktop, but not the user operating it. They're still wide open to all the other tactics used to compromise endpoints. VDI also requires specialized security on the hypervisor to mitigate the risk there.

DaaS:

A CLOUDIER VDI: DAAS

Desktop-as-a-service, or DaaS, is a ‘cloud native’ take on VDI that skips the hypervisor and deploys the desktop as a service from a private or public cloud. This is often a managed service.

- Delivers everything from the cloud, no special hardware required.
- Gives IT granular control over application access and performance.
- Ideal for environments where on/off prem consistency is important.

For IT	For SECURITY
Users love DaaS when it lets them get what they need done, but advanced users can complain about lack of control and customization. Bandwidth is obviously a huge obstacle, especially when users spend long hours on video, and users again don’t get the flexibility they need to work in ways they expect.	Like VDI, DaaS doesn’t implicitly protect end-users from social attacks and other tactics, although security has better visibility into behavior—and that’s huge when trying to verify explicitly, especially between users and applications.

SASE:

BUILDING FOR SECURITY PLUS PERFORMANCE: SASE

Organizations rolling out new sites or branch offices or rethinking office space, are using Secure Access Service Edge to optimize for both performance and security across all modern tools and workloads.

- Combines SD-WAN network control and integrated virtualized security features.
- Lets organizations rethink how data moves between users, devices, and clouds.
- Ideal for organizations rethinking network and environment design.

For IT	For SECURITY
SD-WAN performance gains are critical for users relying on high-bandwidth tools, and SASE helps orgs rethink how they use square footage.	While SASE unifies visibility and control for IT and security, the user is still the missing 1 link, and endpoint controls are needed to secure data, although integration with DLP is easier here.

TOURING THE STACK
A NEW APPROACH: VENN

The missing catalyst for Secure BYO-PC has been an easy way to protect company applications and data without having to buy, manage and lock down every PC.

VDI and DaaS, which has long been the de facto approach to protecting apps and data on remote and unmanaged computers, is increasingly being recognized as a less-than-ideal choice. VDI is complex, expensive and often frustrates users. It's redundant for browser-based applications and doesn’t perform well with video applications.

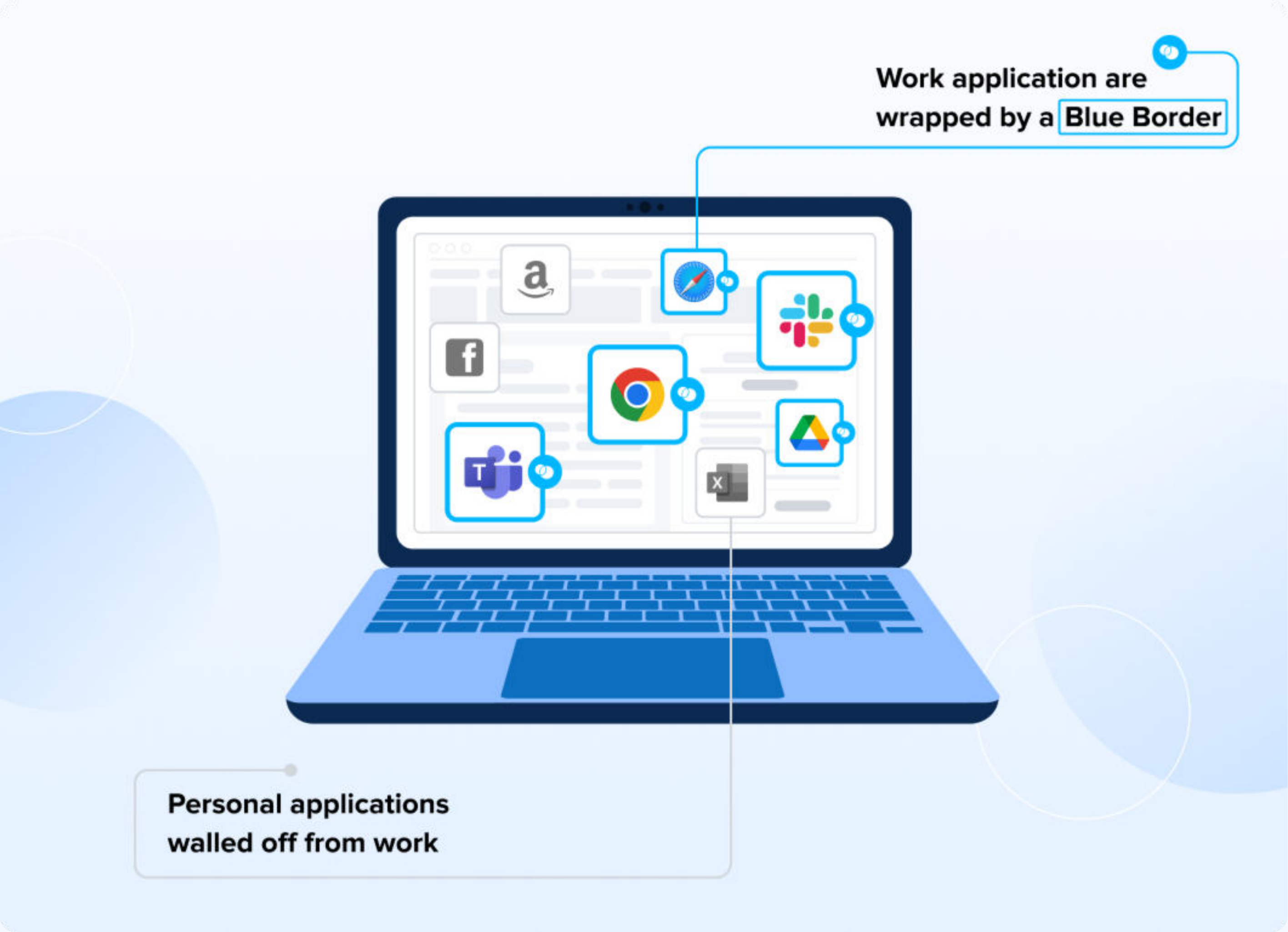
A new approach is needed. Introducing Venn. A new way to apply Zero Trust principles to remote and hybrid workers.

A SECURE WORKSPACE FOR REMOTE WORK

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 business activity is isolated and protected from any personal use on the same computer.

- Supports any unmanaged or BYOD PC or Mac to provide user flexibility on how and where they work.
- Secures data, applications and the network.
- Ideal for organizations embracing remote work, offshore workers and other 3rd party workers.
- With Venn, applications are launched directly from the computer, not remotely delivered, providing optimal performance and a familiar experience that drives productivity and eliminates employee frustration.

For IT	For SECURITY
Users love Venn because they get the freedom to work on the device of their choice without the latency and performance issues of VDI. For IT, users can easily be onboarded and offboarded in minutes. Robust administrative controls can be customized over work applications and data, network access, peripheral use, copy-paste and remote wipe, all without locking down the entire PC.	Designed for security and compliance-driven organizations to protect company data from accidental or malicious exfiltration, compromise or loss. Data stored in Venn is always encrypted and inaccessible to any application outside of the Venn secure enclave, while data in transit is routed through a built–in encrypted private company gateway or a VPN/network security system already employed by your organization. Access to Venn can be enabled, suspended, terminated or data remotely wiped, with a click of a button.


Work application are wrapped by a Blue Border
Personal applications walled off from work

BALANCING YOUR STACK: MOVING FROM COMPLEXITY TO CONFIDENCE

Complex business needs drive equally complicated technology environments. This can feel like common sense, but we still see IT and security teams spending too much time searching for a silver bullet that solves everybody's problems with zero compromises.

The reality is, no matter what new technologies come online, there will never be a single best practice for keeping the modern distributed enterprise productive and secure. That's the core of zero trust as well: deploying diverse defenses in depth to protect, ensuring users and data stay protected no matter how (and where) they're connecting.

Focus on the what, not the how

All of the technologies discussed excel in some use cases and fade in others. Add them all together and you get a 'complete' stack that still has gaps and overlaps. A smarter approach is to focus on what needs to get secured data and build everything out from there.

When we look at our stack, we see data-specific protection is lacking in many of those layers, but we also see more opportunities to slow attackers down on their way towards that data. That is the promise of defense in depth, and the key to meaningful zero trust no matter how, where, and why your users are working. That's how a world of complexity gets a little more confident, one connection at a time.

venn

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