Mindcore Use Cases

One-Platform . Security . Compliance . Governance .

November 4, 2024

Privileged Access Management

Mindcore Solution

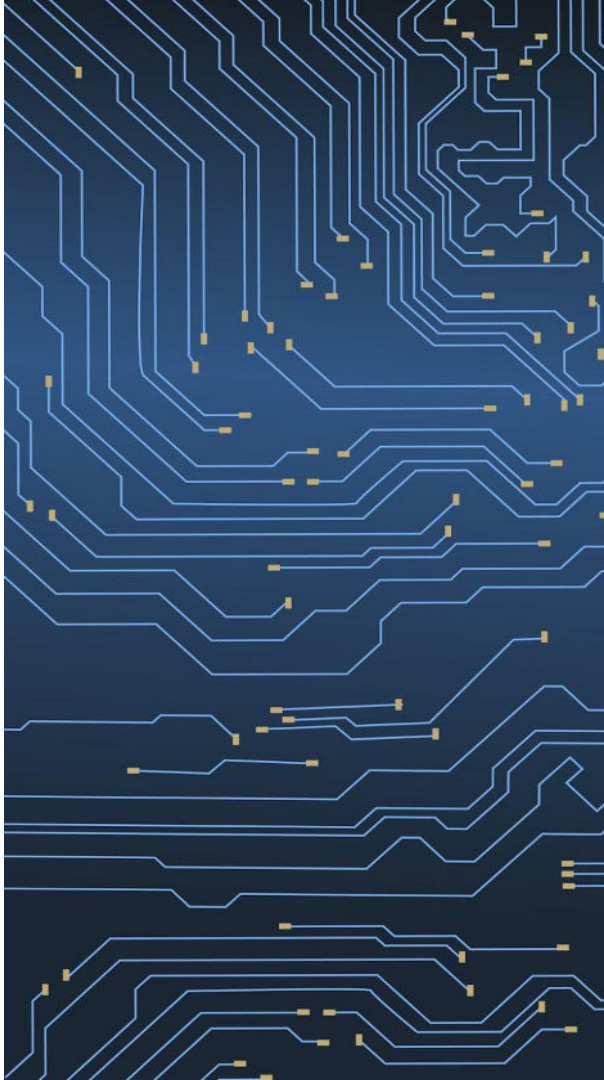
- Permit insiders to safely and responsibly administer highly-sensitive systems such as credit-card databases, financial transaction and trading systems, messaging and invoice approval systems.

Results

- Dramatically reduced threat surface.
- Reasonably foreseeable misuse deterrence.
- Audit trails to support your compliance function.
- Root cause analysis in the event of a meaningful failure.
- Instantaneous ISO 27001 context from within which to perform your administrative duties.
- Over 120 audited controls controls to fulfil your various responsibilities (PCI, 23 NYCRR 500, etc).

Here's how easy it is:

- Create a special-purpose privileged access room on Mindcore. Turn on session recording.
- Connect **only** the necessary systems with access to **only** the administrative ports and services (ssh, Oracle Net Services, etc.).
- Do not enable Internet access on these special-purpose desktops!
- Configure and approve desktops for administration, pre-install approved tooling, establish GPOs forbid device redirection and copy/paste.
- Assign these to privileged users.
- Disable access to administrative and services ports from the privileged users' ordinary (internet-enabled etc.) machines.



Self-Service Transformation

Mindcore Solution

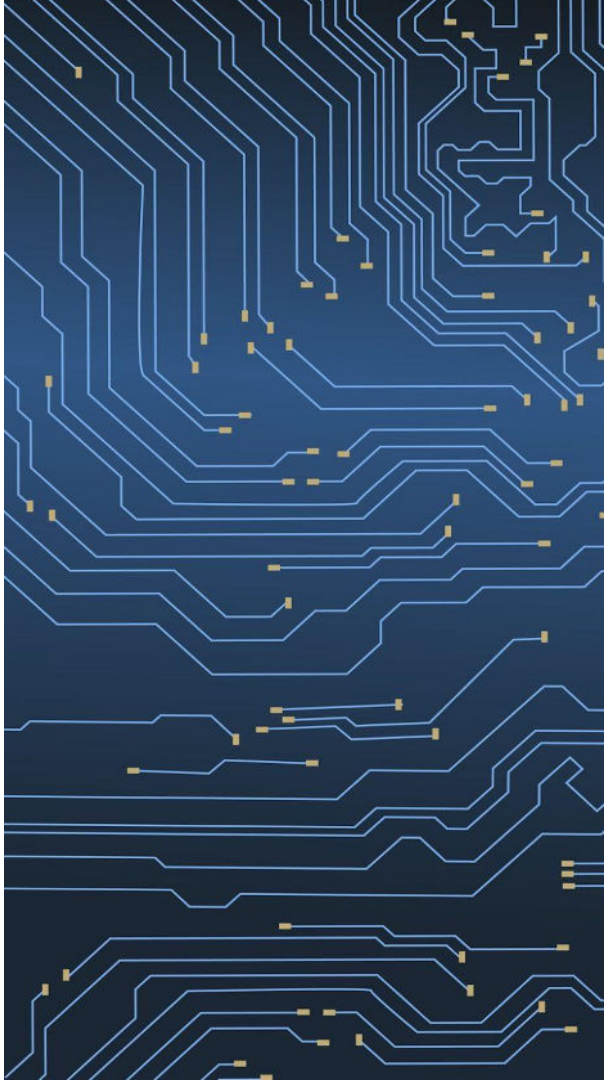
- Mindcore is designed to streamline and empower organizations by giving users the tools to independently manage their access and desktop environments within a secure, cloud-based platform.

Results

- Quickly set up and configure secure, logical groupings for work, we call rooms.
- Built-in Access and Permission management to align with your organizational policies
- Greater agility when it comes to onboarding and offboarding and procuring desktops.
- Reduced IT overhead, allows team to concentrate on other areas.

Here's how easy it is:

- Connect your Mindcore tenant to your IDP and configure it for SAML/SCIM authentication and user provisioning.
- Onboard the Mindcore user(s) and specify which secure room they need access to.
- In Mindcore manager, simply add the username(s) to the desktop template of choice.
- User(s) can now access their desktop in minutes with all of the applicable privileged access requirements.
- Use DIA to manage the entire fleet of desktops with features such as patch management, remote support automation.



Secure Hybrid Work

Mindcore Solution

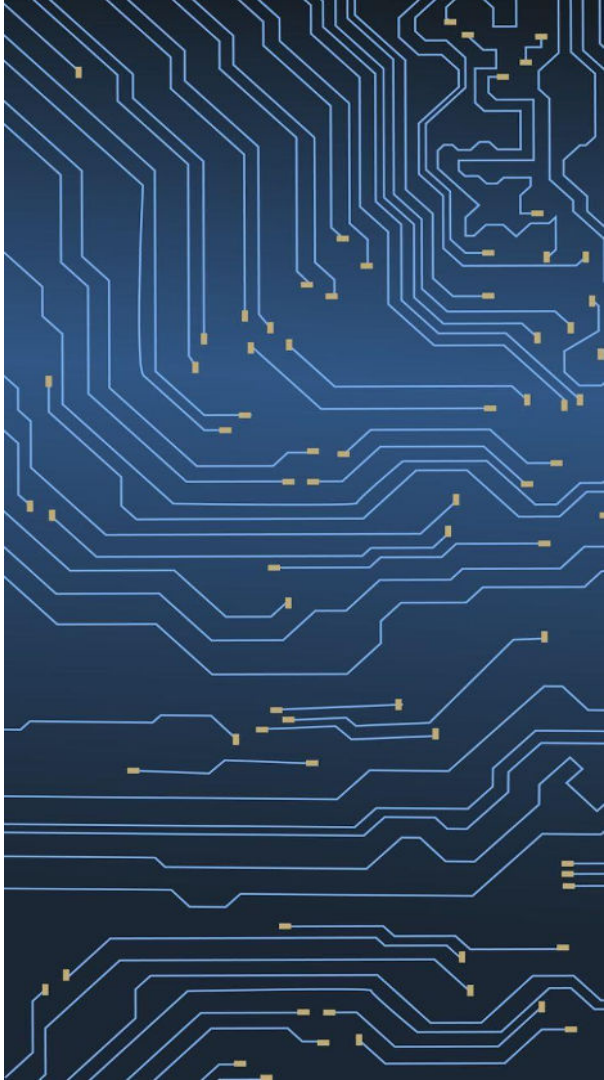
- Provides a fully comprehensive, all-in-one, cloud-based solution that provides safe, reliable remote access to critical systems and data. Mindcore also addresses security, compliance and productivity concerns.

Results

- Access virtual desktops from any location without risking exposure.
- Data and system integrity regardless of where users connect from.
- Privileged access to your corporate resources.
- Audit trails to support your compliance function.
- Onboard and scale with ease without compromising security.
- Transition your business away from the necessity to manage physical end-user computing hardware.

Here's how easy it is:

- Create secure room(s)in any cloud region globally.
- Delegate your rooms to appropriate managers. Teams can then be invited or automatically provisioned using Mindcore's AD-join to access their desktops.
- Connect the secure room(s) to only the networks and data assets appropriate to the segmented workers responsibilities.
- You can connect a single room to as many networked assets as you choose, whether cloud or on premise, and the desktops will enjoy simultaneous access to all of them, no VPN or multi-point hops required.



Auditor and Due-diligence Enablement

Mindcore Solution

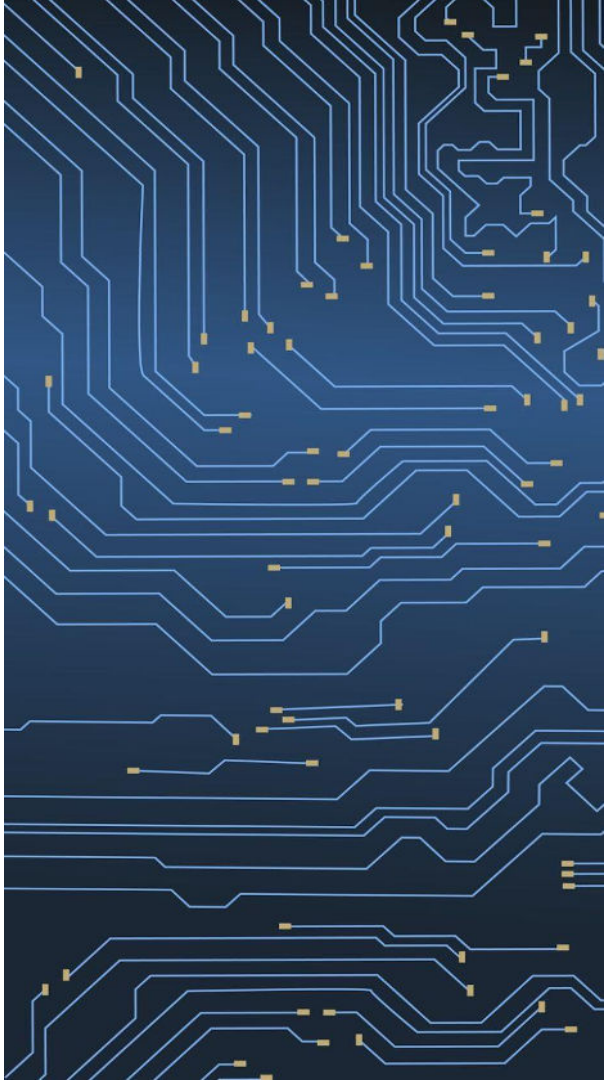
- Permit your auditors and invite authorized due-diligence advisors to access your sensitive data and records though a Mindcore enclave, instead of directly or through a data room that permits downloading files locally (which most do, to the horror of many).

Results

- Data loss prevention and confidentiality enforcement.
- Complete auditability of all data that has been reviewed.
- Permit access without putting, your compliance at risk (since you can prove they did not abuse that access nor walk away with any data).
- Share data with auditors or due diligence advisors with confidence, knowing that you can revoke access instantaneously when the time comes.

Here's how easy it is:

- Create a special-purpose audit or due-diligence room.. Turn on session recording.
- Provide access to relevant network resources. Generally, do not permit or tightly restrict Internet access since that would be a vector for data exfiltration.
- Put only the files appropriate for the effort in the file vault. Do not enable downloading. Make sure your desktop GPOs do not permit external device mounting nor copy/paste unless deemed appropriate.
- Create a third-party organization, invite their leader to nominate access. Approve these one at a time, or permit them to decide who gets access at your option.
- Assign desktops within these rooms to the pentester or auditor.



Third-party and Freelancer Access

Mindcore Solution

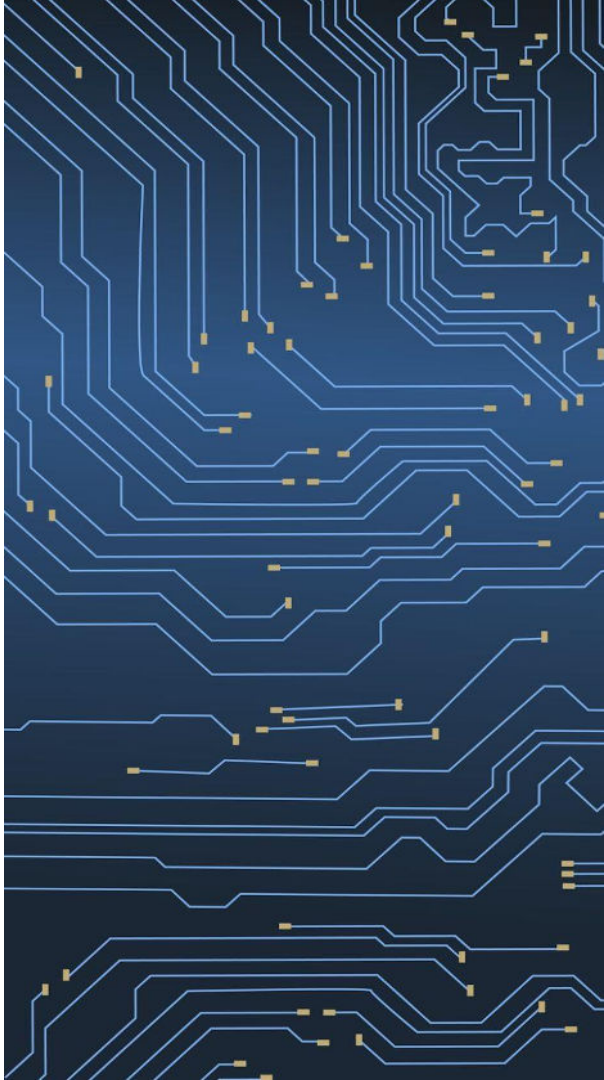
- Engage third parties and freelancers with confidence, even when interacting with sensitive data assets.

Results

- Business transformation for agility
- Support your SOX or other compliance posture even when engaging temporary workers.
- Threat surface reduction.
- Keep your third parties **outside** your internal network configuration.
- Govern your third parties desktops! (no need to “trust” your offshore vendors’ security and compliance any more).
- Get out of the business of issuing and managing far-flung desktops to your IT and other service provider vendors.

Here’s how easy it is:

- Create a secure vendor access room in a convenient cloud location using Mindcore.
- Draft your usage policy, and decide whether to collect policy signatures on every login or once per update.
- Connect it to only the necessary systems with access to only the appropriate ports and services (perhaps your data entry and VOIP systems, on only the https, SIP and TLS ports for a call centre example).
- Configure and approve desktops with pre-installed approved tooling, GPOs etc.
- Create your third party org and invite their administrator.
- They can then nominate their team into the room, and you can either take their nomination as approval or gather your own for each individual.



Cybersecurity and Zero-trust Transformation

Mindcore Solution

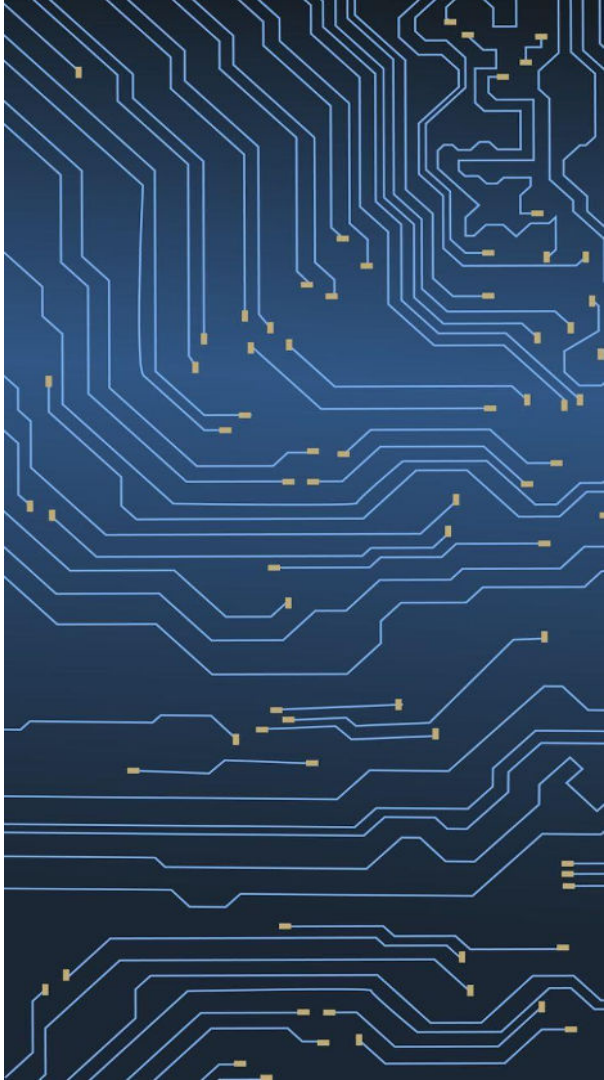
- Overcome inertia and risks inherent in zero-trust transformation projects by creating a networking strategy that is overlaid *on top of* the existing hardened external perimeter and permissive internal network paradigm.

Results

- Rapid time to value as you adopt zero-trust.
- Stop issuing desktops and VPN access that grant access to the entirety of your networks.
- Issue access and credentials to individuals with only the network and app access they require to perform their work.

Here's how easy it is:

- Create secure room(s) in any cloud region globally.
- Delegate your room(s) to appropriate managers, have them invite their teams or use our AD-Join feature to automatically provision and enable users to access their desktops.
- Connect secure room(s) to only the networks and data assets appropriate to the segmented workers responsibilities.
- You can connect a single room to as many networked assets as you choose, whether cloud or on premise,. Desktops will have simultaneous access to all networked assets; no VPN or multi-point hops required.



Pentesting/Red Teaming Enablement

Mindcore Solution

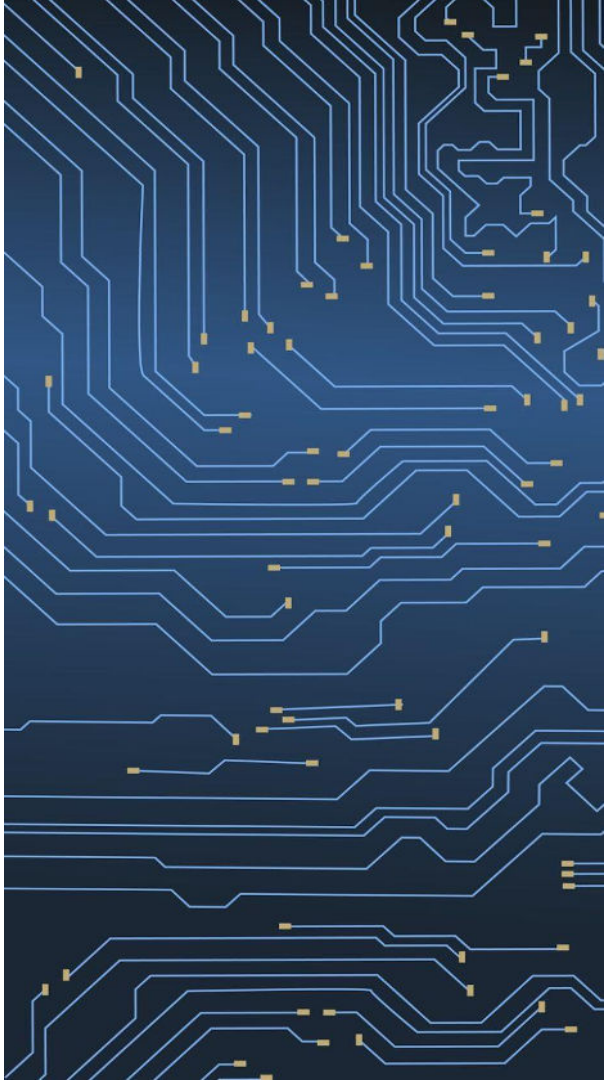
- Act as a secure operational layer for pentesting activities, minimizing risk while supporting all necessary compliance and operational requirements, particularly in sensitive or regulated industries.

Results

- Isolated and controlled testing environments
- Role-based access and granular permissions
- Secure data transfer
- Complete auditing suite
- Network segmentation

Here's how easy it is:

- Create a special-purpose privileged access room on Mindcore. Turn on session recording
- Give the room full internet access
- Configure and approve desktops for administration, pre-install approved OSINT and scanning tools.
- Assign these to privileged users.
- Conduct testing, create and share reports via FileVault.



Business continuity/disaster recovery

Mindcore Solution

- Ensure your organization's technology operations are highly available undisrupted and secure. Achieve resilience across your virtualized and cloud-based systems while maintaining access to mission critical data and line of business applications at all times.

Results

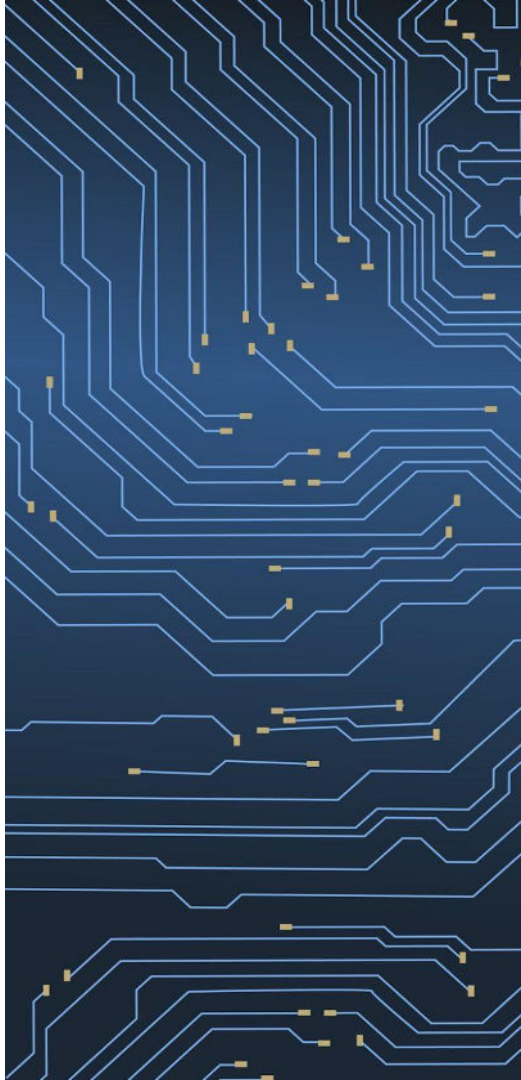
- Quick return to operation (RTO) during disasters to reduce business and financial impact.
- Resilient, globally available services with fault tolerance.
- Focus on more strategic policy plans through a fully managed BCDR service in Mindcore.
- Replicate access across multiple system, images, availability zones, and regions to satisfy your globally distributed and hybrid workforce.
- Achieve operational restoration in under 5 minutes!

Here's how easy it is:

- Create a hot room with Mindcore's custom images and data connections (File Vault or cloud storage).
- Configure as required to relevant Cloud, Region, and Availability Zone.
- Configure network connections in the hot room to data and applications (cloud-based or on-premise).
- Provision primary Mindcore desktops in the hot room and assign to user(s) accounts.
- Configure cold room(s) as required to relevant Cloud, Region, and Availability Zone.
- Make relevant applications and data available in cold room(s).
- Replicate network connections
- Provision secondary Mindcore desktops in the cold room(s) and assign to use(s)..

In case of an event:

- **1 min:** Disconnect and suspend hot enclave access.



Engineering/graphics workstation enablement

Mindcore Solution

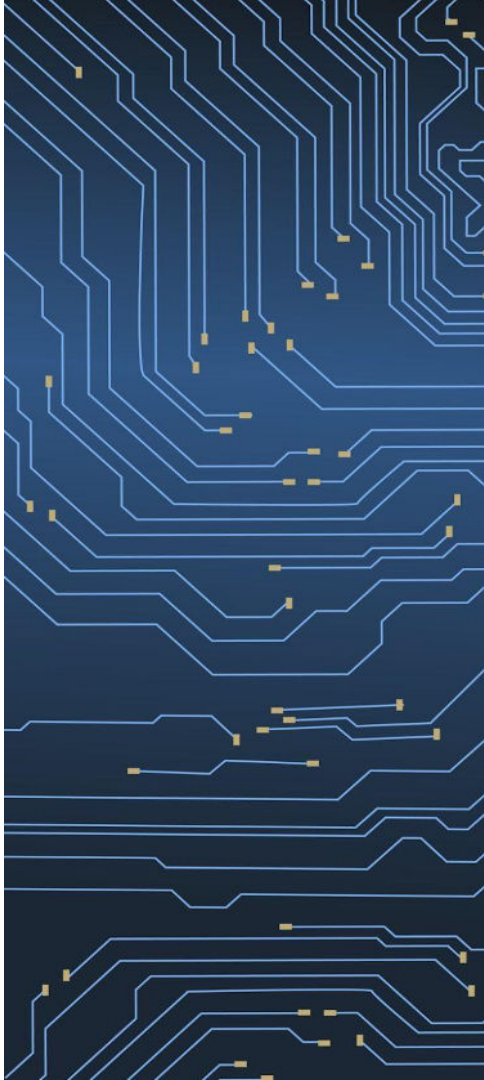
- Mitigate and manage the high-cost and complexity of high-end GPU workloads for functions such as digital engineering, graphic designing, gaming, and media and entertainment.

Results

- Reduce the total cost of hardware ownership and supply chain challenges including leveraging a lower cost hardware (Chromebooks, Android, etc)
- Improve end user experience, productivity and agility with seamless object rendering for digital engineering and graphic workloads.
- Leverage unlimited storage to securely transmit your large graphic-intensive project data from Mindcore's secure room to your local endpoint with built-in data Loss Prevention.
- Protect Intellectual property by satisfying industry standards.

Here's how easy it is:

- Upload your graphic-intensive application deployment files through Mindcore's App Vault.
- Configure Mindcore's GPU specification desktops for your workforce, including VFX and Visual Compute.
- Install the applications and publish them to your end users.
- Achieve instant productivity against any GPU workload with full control for performance vs Image quality via Nvidia Control Panel.
- Allow end users to transfer files between the Mindcore enclave and their local endpoints (can be non-GPU) with unlimited storage capacity for such large size files. All data will go through bidirectional DLP scanner.



AI and Data Governance

Mindcore Solution

- Accelerate the adoption of AI without compromising security or compliance.
- Maximize the economic and productivity benefits of a workforce amplified with market-leading AI tools

Results

- Data loss prevention
- Complete inventory of all data permitted for use with AI.
- Complete audit trail of all interactions with AI, creating opportunities for actual governance and policy enforcement.
- It becomes trivial to prove to regulators that your AI adoption does not intersect with your regulated data.

Here's how easy it is:

- Instead, creating a Mindcore data enclave in the cloud makes it simple to guarantee that zero regulated data can reach the external AI.
- Create a special-purpose AI governance room on Mindcore. Optionally, turn on session recording.
- Establish the network configuration to permit access to only authorized external AI systems.
- You can also implement AI tools such as Deloitte Cortex or Palantir, but make them available only within the enclave.
- On day one, zero enterprise data is in the enclave. You can enable AI with confidence!
- As you establish your data governance function, integrate permitted data assets into the room.