MINDCORE TECHNOLOGIES

MINDCORE TECHNOLOGIES GCR - LOCAL GVT CYBER-INSURANCE

MATT ROSENTHAL
CEO, MINDCORE TECHNOLOGIES
Phone: (973) 903-1102
Website: https://mind-core.com

Cyber-insurance: Common and Costly Roadblocks

Security-control requirements that insurers now treat as non-negotiable

- Multifactor authentication (MFA) everywhere
- Endpoint detection & response (EDR) and 24×7 monitoring
- Segmented, immutable, offline backups
- Privileged-access management & patching cadence
- Formal incident-response (IR) plan, tabletop tests and log retention

Structural and budgetary challenges unique to local government

- Fragmented IT ownership
- Procurement law and union contracts
- Aging infrastructure & unfunded mandates
- Rapidly rising premiums and lower sub-limits
- Misrepresentation risk on applications
- Third-party / shared-services exposure

Massachusetts-specific compliance pressures

- M.G.L. c. 93H / 201 CMR 17 (WISP & encryption rules)
- Massachusetts Public Records Law & Session Retention
- CJIS for municipal police departments
- FERPA / DESE requirements for school districts
- HIPAA / EMS & Board of Health
- PCI-DSS for tax, permitting and parking payments

Mindcore Technologies – Cyber Insurance

Structural and budgetary challenges unique to local government

- **MFA on every privileged login**

Mindcore provides MFA (TOTP, Duo, Okta, Azure AD, etc.) at both the Mindcore portal and the virtual desktop level; no way to bypass

- **24×7 EDR/SOC monitoring**

Mindcore all enclave desktops are instrumented , managed and monitored by Mindcore Manager 3.0 ; alerts, files and process telemetry are retained for 365+ days

- **Segmented, immutable backups**

Mindcore VDI provisioned inside secure data enclave; copy/paste, USB and print are policy-controlled. Snapshots and customer data are backed up to immutable storage inside Mindcore's AWS tenancy

- **Rapid & automated patching**

Base images are patched by Mindcore within 24 h of a critical CVE and rebooted automatically during maintenance windows—no local IT effort.

- **Privileged-access management**

Role-based access, JIT session launch, keystroke + screen recording, and automatic log-off after inactivity all meet insurer PAM language.

- **Formal IR evidence**

Session recordings, audit logs, file-vault transfers and SOC alerts export directly to Splunk or S3, providing the "artifacts" underwriters want for tabletop tests.

Security-control requirements that insurers now treat as non-negotiable

- Multifactor authentication (MFA) everywhere
- Endpoint detection & response (EDR) and 24×7 monitoring
- Segmented, immutable, offline backups
- Privileged-access management & patching cadence
- Formal incident-response (IR) plan, tabletop tests and log retention

Massachusetts-specific compliance pressures

- M.G.L. c. 93H / 201 CMR 17 (WISP & encryption rules)
- Massachusetts Public Records Law & Session Retention
- CJIS for municipal police departments
- FERPA / DESE requirements for school districts
- HIPAA / EMS & Board of Health
- PCI-DSS for tax, permitting and parking payments

Mindcore Technologies – Cyber Insurance

Security-control requirements that insurers now treat as non-negotiable

- Multifactor authentication (MFA) everywhere
- Endpoint detection & response (EDR) and 24×7 monitoring
- Segmented, immutable, offline backups
- Privileged-access management & patching cadence
- Formal incident-response (IR) plan, tabletop tests and log retention

Security-control requirements that insurers now treat as non-negotiable

- **M.G.L. 93H / 201 CMR 17 encryption**

  TLS 1.2-only transport; AES-256 at rest; WISP template mapping delivered by Mindcore for easy inclusion in the town's master WISP
- **Public Records retention**

  Immutable screen & file logs give record custodians verifiable evidence while still allowing "right-to-delete" policies on the customer side
- **FBI-CJIS for police**

  Rooms can be locked to GovCloud regions that are CJIS-compliant; two-factor auth + full disk encryption + audit trail meet sections 5.6, 5.9 & 5.10
- **FERPA for schools**

  No data stored on Chromebooks or teacher laptops; access only through the Room VDI, satisfying "reasonable methods to protect" requirements.
- **HIPAA for EMS/health**

  Mindcore signs BAAs, is HIPAA/HITECH audited, and logs every PHI access for the required 6-year period.
- **PCI-DSS for payments**

  Segment a dedicated "Card Services Room" that meets SAQ-A; no PAN ever touches municipal networks, shrinking PCI scope and insurance exposure.

Massachusetts-specific compliance pressures

- M.G.L. c. 93H / 201 CMR 17 (WISP & encryption rules)
- Massachusetts Public Records Law & Session Retention
- CJIS for municipal police departments
- FERPA / DESE requirements for school districts
- HIPAA / EMS & Board of Health
- PCI-DSS for tax, permitting and parking payments

Mindcore Technologies – Cyber Insurance

Security-control requirements that insurers now treat as non-negotiable

- Multifactor authentication (MFA) everywhere
- Endpoint detection & response (EDR) and 24×7 monitoring
- Segmented, immutable, offline backups
- Privileged-access management & patching cadence
- Formal incident-response (IR) plan, tabletop tests and log retention

Security-control requirements that insurers now treat as non-negotiable

- Multifactor authentication (MFA) everywhere
- Endpoint detection & response (EDR) and 24×7 monitoring
- Segmented, immutable, offline backups
- Privileged-access management & patching cadence
- Formal incident-response (IR) plan, tabletop tests and log retention

Massachusetts-specific compliance pressures

- **Fragmented IT ownership**

Create separate Rooms for police, fire, DPW, school, library, etc., each with its own policies but under one console and one insurance application.

- **Procurement & 30B delays**

SaaS / Opex model qualifies as a “software subscription,” often exempt from formal bid if <$50 k; deploy in days instead of fiscal-year cycles.

- **Legacy infrastructure, Aging PC/Windows**

End-user device becomes a thin client; security posture is dictated by the Room image, not by whatever hardware the user happens to own.

- **Rising premiums / deductibles**

Demonstrable MFA, EDR, audit trail and immutable backups allow brokers to argue for lower retentions or to avoid ransomware exclusions.

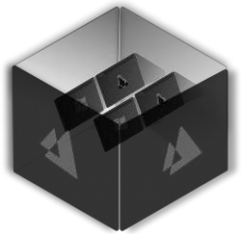
- **Misrepresentation risk on apps**

Instead of guessing, the town can truthfully check “Yes” to MFA, EDR, PAM, encryption, logging, segmentation—because Mindcore enforces them.

- **Shared-services exposure**

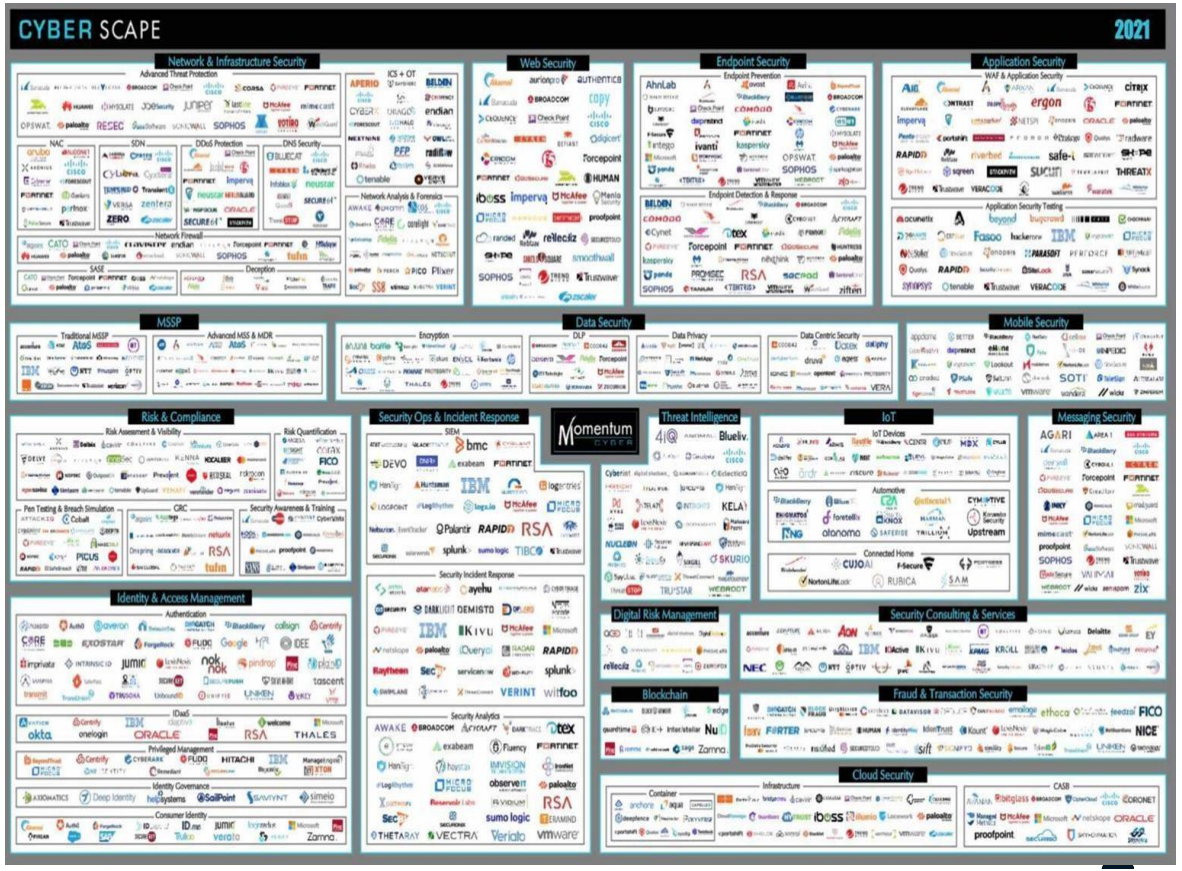
Invite county dispatchers, state agencies, external auditors or vendors into a Room with time-boxed, read-only access; no VPNs or network “trust” needed.

Establishing, securing, and managing a compliant GRC platform is often fragmented and high-risk—introducing complexity, gaps in oversight, and compliance exposure. It doesn't have to be this way



Mindcore Manager 3.0

Vs



What is Mindcore

Mindcore is a secure, scalable platform purpose- built to support Governance, Risk, and Compliance (GRC). By provisioning highly secure data enclaves in the cloud, Mindcore helps organizations meet ATO, RMF, and CSF requirements with ease through:

- **Centralized policy and identity enforcement**
- **Integrated endpoint, data, and cloud protection**
- **Real-time audit trails and role-based access**
- **Automated compliance evidence collection**
- **Seamless integration across security tools and workflows**

What Mindcore does

All-in-one platform uniquely combines proprietary **secure perimeter data enclaves, advanced cybersecurity, and endpoint protection**, with VDI.

Provides **highly secure work environments, delivered through managed data enclaves,** ensuring organizations can quickly and efficiently meet their security control requirements and ensure sensitive data and workflows are secure, auditable and fully compliant.

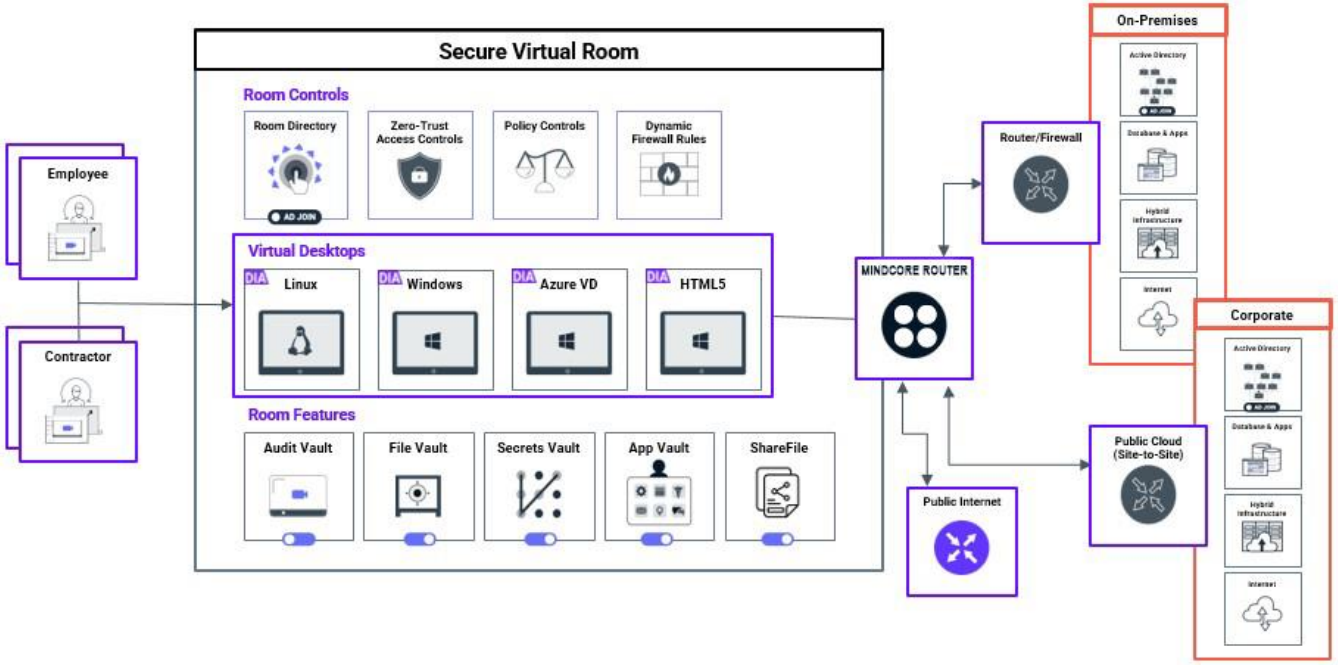
Mindcore Data enclaves simultaneously provide:

Tightly	**governed, secured** SOC2-Type 2/ISO 27001 cloud infrastructure
with	**virtual desktops** fully integrated,
that	**only the people** permitted,
may access	**only the data** permitted, both file and networked,
leveraging	**only the apps** permitted and only the infrastructure permitted, with
a high-integrity	**audit trail** of all of those permissions, and
establishing	**full auditability for activities** within the enclave.

Data Enclave: Highly-Restricted Zones in the cloud

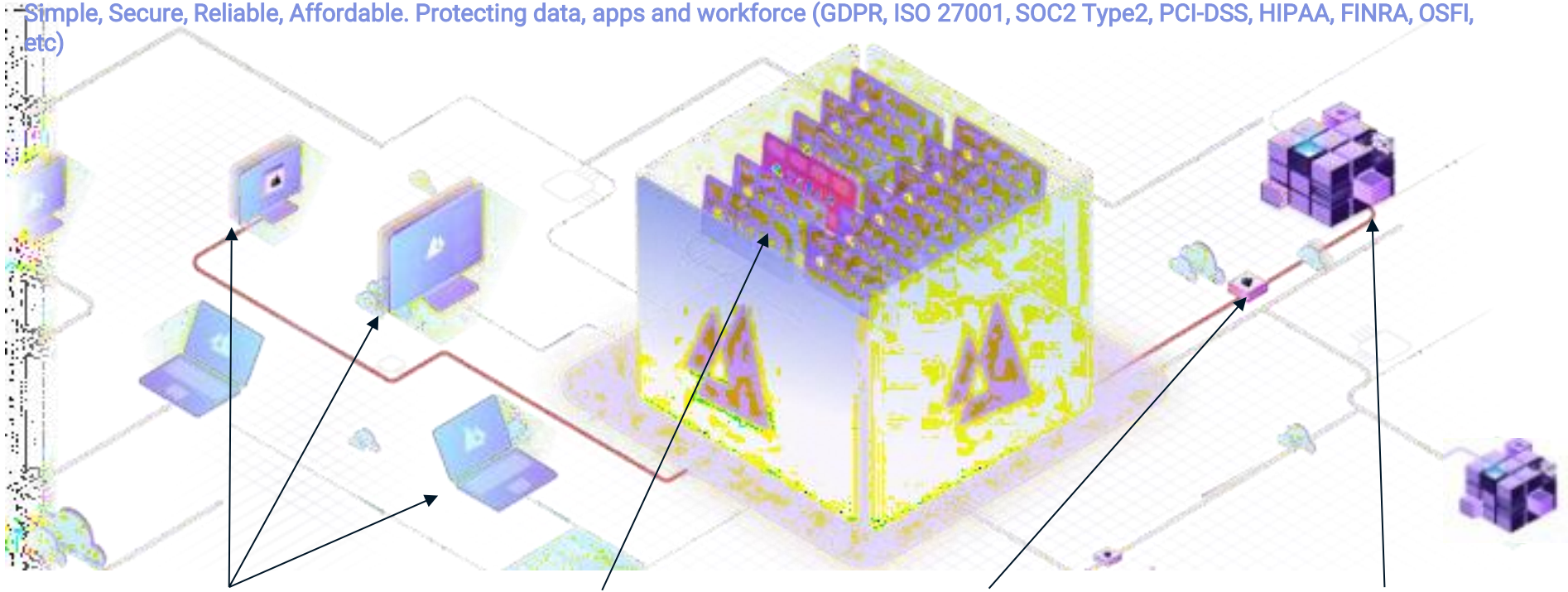
Highly-Restricted Zones (HRZ) to secure and govern access to sensitive data, apps and networks (ISO 27001, SOC 2 Type 2, GDPR, PCI-DSS, HIPAA, FINRA, OSFI, 23 NYCRR 500, SEC, SOX, NIST 2.0)

- Secure data enclaves
- Comprehensive suite of security and cyber services
- Auditing and Monitoring
- Strict Access Control
- Centralized management, provisioning and cost optimization
- Integrated infrastructure and virtual desktop



Simple: Click, Connect, Go

Simple, Secure, Reliable, Affordable. Protecting data, apps and workforce (GDPR, ISO 27001, SOC2 Type2, PCI-DSS, HIPAA, FINRA, OSFI, etc)



1. Take control of end point

Mindcore takes custody of the work where the fingers hit the keyboard, from any physical device: no data ever reaches the end user device.

2. Provision secure perimeter(s)

Protect, control, manage and audit all work performed on the fully managed and governed virtual desktops

3. Zero Trust connect to corp data and application(s)

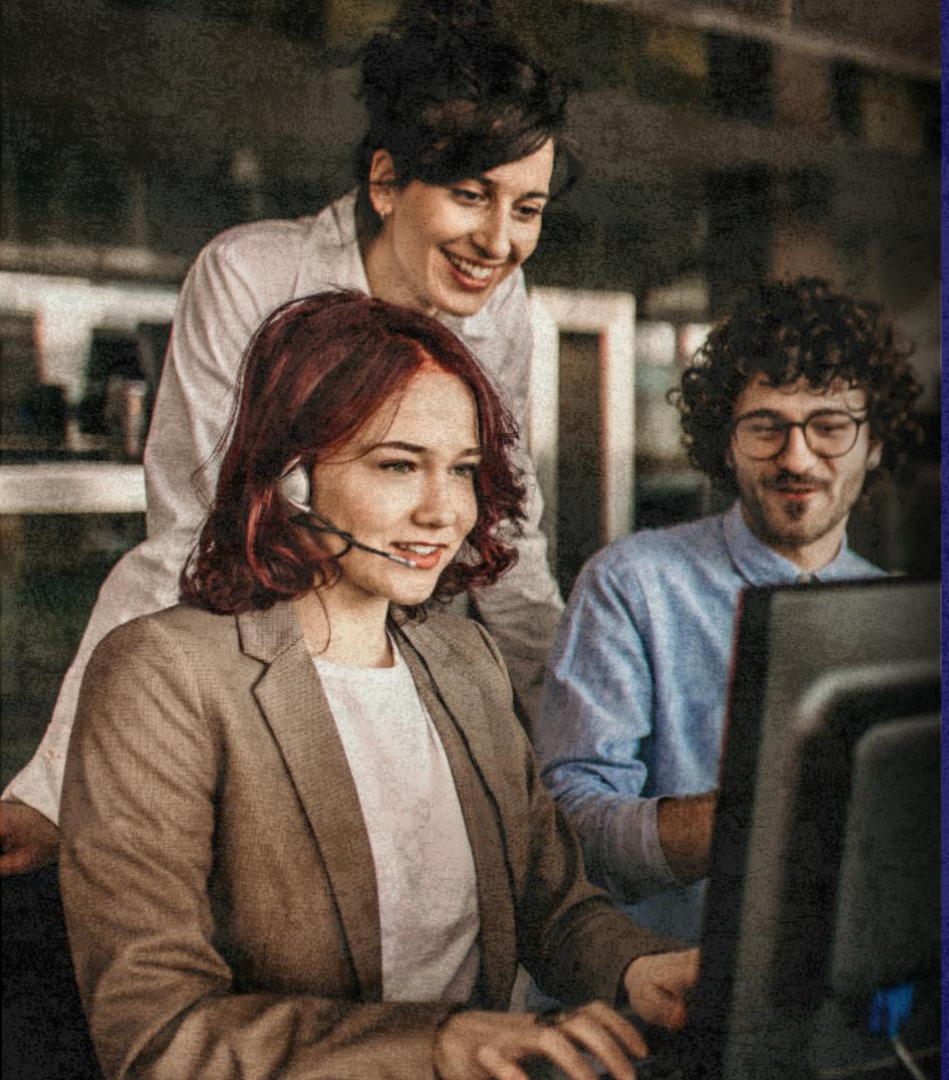
The Mindcore Gateway technology connects the work products to as many enterprise data footprints as necessary, no matter how mission-critical and data-sensitive they are.

4. Enterprise secure perimeter business Service(s)

The Mindcore Room operates as a virtual extension of your secured business infrastructure in the cloud.

Example Use Cases

- Secure hybrid work
- 3rd Party access
- Data governance
- Business continuity and disaster
- Endpoint protection
- M&A
- AI Governance
- VDI/DaaS Migration
- Cybersecurity and zero-trust transformation
- Auditor and due diligence enablement
- Regulatory compliance
- Pen-testing and red-team enablement
- IP Protection
- DevOps
- Privileged access management



MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

SECURING YOUR DIGITAL TOMORROW, TODAY!

Your Trusted Partner in Managed IT & Cybersecurity

MATT ROSENTHAL

CEO, MINDCORE TECHNOLOGIES

Phone: (973) 903-1102

Website: https://mind-core.com

Data and AI Governance

Mindcore Solution

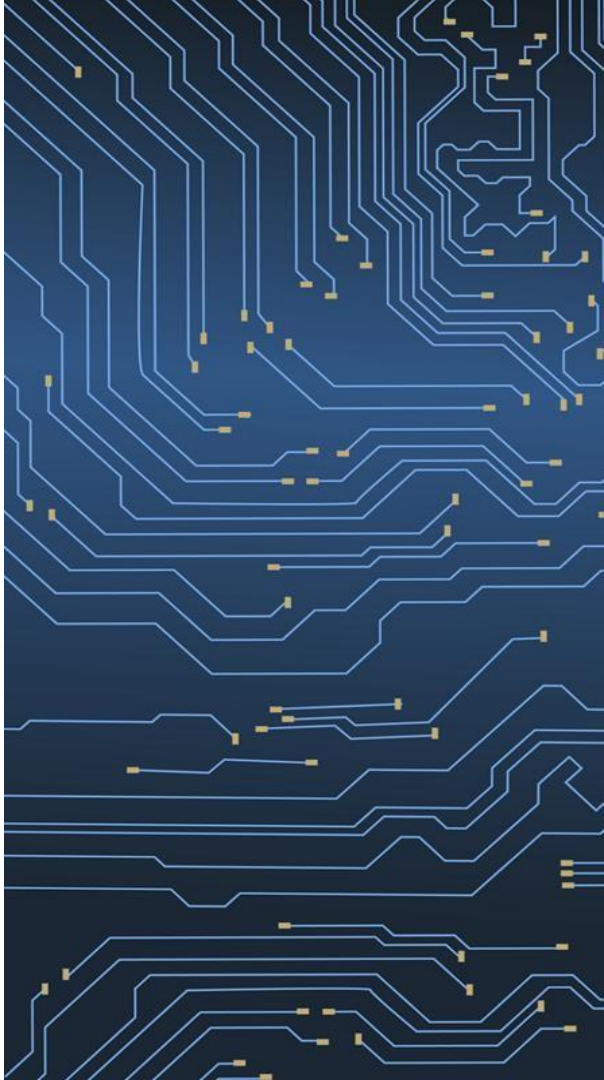
- Accelerate the adoption of AI without compromising security or compliance.
- Maximize the economic and productivity benefits of a workforce amplified with market-leading AI tools

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.



Privileged Access Management

Mindcore Solution

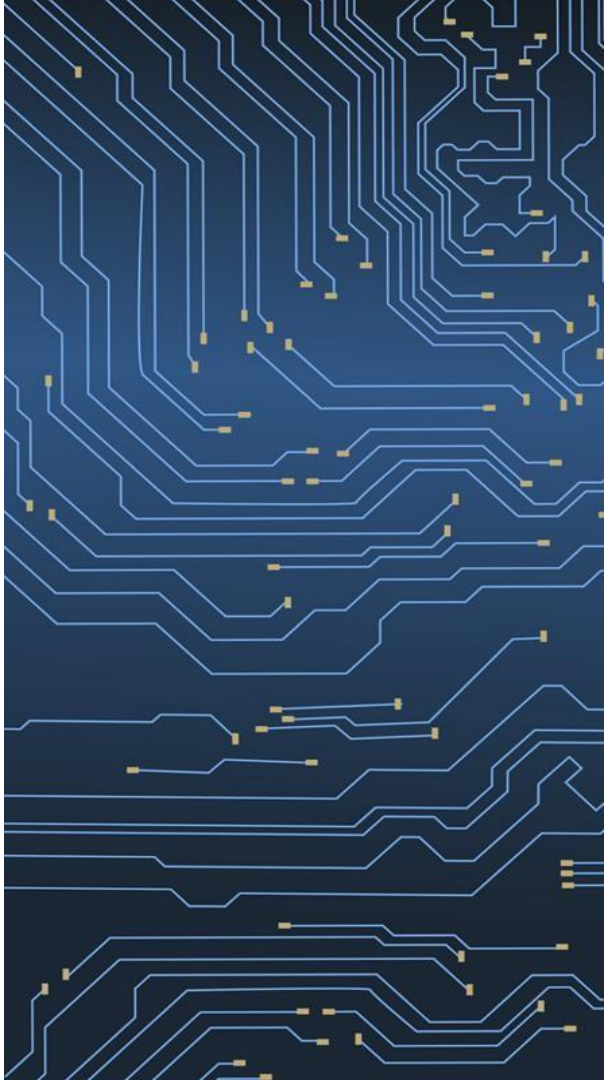
- Permit insiders to safely and responsibly administer highly-sensitive systems such as credit-card databases, financial transaction and trading systems, messaging and invoice approval systems.

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.



Secure Hybrid Work

Mindcore Solution

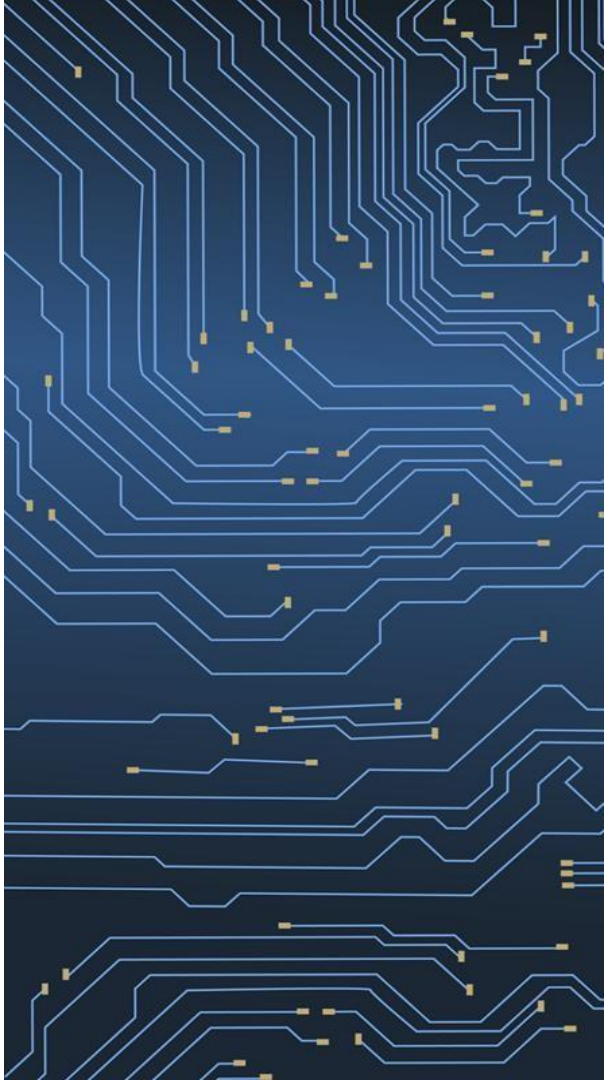
- Provides a fully comprehensive, all-in-one, cloud-based solution that provides safe, reliable remote access to critical systems and data. Mindcore also addresses security, compliance and productivity concerns.

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

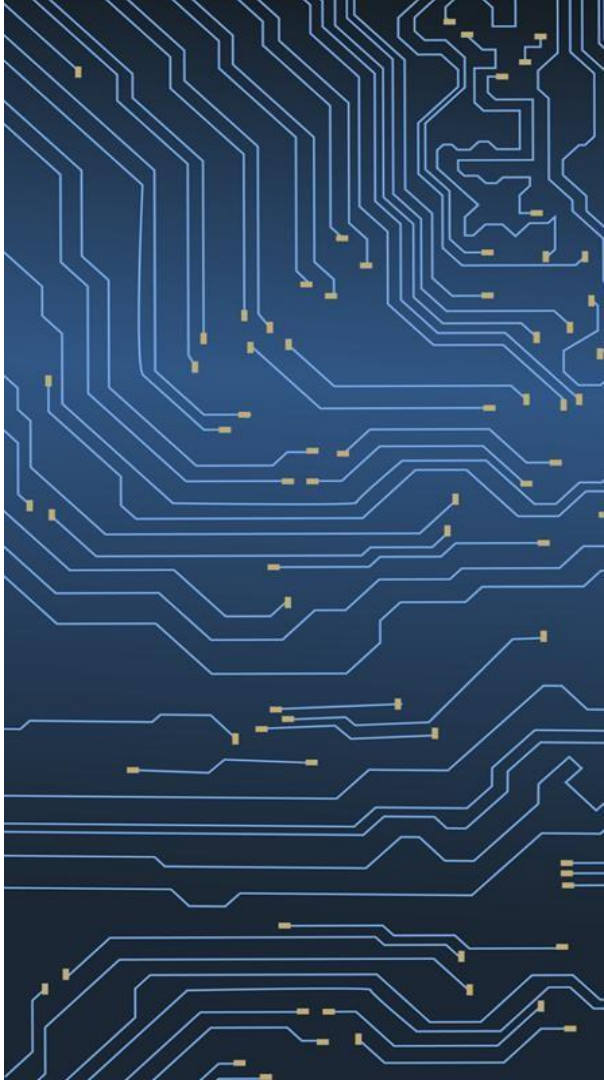
- Permit your auditors and invite authorized due-diligence advisors to access your sensitive data and records though a Mindcore enclave, instead of directly or through a data room that permits downloading files locally (which most do, to the horror of many).

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.



Key Notes:

Mass. cities, towns, school districts and other municipal entities run into most often when they try to buy or renew a cyber-insurance policy. They fall into three broad buckets—(1) technical security controls required by underwriters, (2) statutory / regulatory compliance obligations that are specific (or especially relevant) to Massachusetts public-sector entities, and (3) structural or budgetary realities of local government that make the first two harder to satisfy. When one or more of these items is missing or only partially implemented, carriers either (a) refuse to quote, (b) add large exclusions, or (c) impose steep premiums and deductibles.

In short, the hurdle for a Massachusetts municipality to obtain reasonably priced cyber-insurance is no longer simply "fill out a form." Carriers are demanding hard, auditable evidence of MFA, EDR, segmented backups, and a living WISP—all on top of a patchwork of Mass. and federal regulations. The gap between those expectations and the fiscal / governance realities of local governments is the primary challenge.

Quick wins the carrier's loss-control engineer will like ——————————

- Export a one-click "Evidence Package" (MFA config, EDR status, backup reports, IR run-book) and attach it to the policy application.
- Spin up a "Table-Top Room" so police, fire and school leaders can run an IR exercise with actual Mindcore logs—produces the board-approved minutes insurers demand.
- Use ARPA or MIIA grant money to fund the Mindcore subscription; tell the underwriter the town already has funded controls for the whole policy term.