MINDCORE
TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

GCR - LOCAL GOVERNMENT CYBER-INSURANCE

MATT ROSENTHAL
CEO, MINDCORE TECHNOLOGIES
Phone: (561) 404-8411
Website: https://mindcore.com

CYBER-INSURANCE: COMMON AND COSTLY ROAD BLOCKS

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-servicesexposure.

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
POWERED BY:
TEHAMA + Microsoft

SECURE CLOUD WORKSPACE – CYBER INSURANCE

- **MFA on every privileged login.** Secure cloud workspace provides MFA (TOTP, Duo, Okta, Azure AD, etc.) at both the Secure cloud workspace portal and the virtual desktop level; no way to bypass.
- **24×7 EDR/SOC monitoring.** Secure cloud workspace all enclave desktops are instrumented , managed and monitored by Secure cloud workspace Manager 3.0 ; alerts, files and process telemetry are retained for 365+ days.
- **Segmented, immutable backups.** Secure cloud workspace 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 Secure cloud workspace's AWS tenancy
- **Rapid & automated patching.** Base images are patched by Secure cloud workspace 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 INSUERS 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 test and log retention.

MASSACHUSETTS SPECIFIC COMPLIANCE PRESURE

- 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
- PCIDSS fo tax pemitting and parking payments

MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

SECURE CLOUD WORKSPACE – CYBER INSURANCE

- **M.G.L. 93H / 201 CMR 17 encryption.** TLS 1.2-only transport; AES-256 at rest; WISP template mapping delivered by Secure cloud workspace 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 sections5.6, 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.** Secure cloud workspace signs BAAs,is HIPAA/HITECH audited, and logs every PHI access for the required 6-year period.
- **PCI-DSS for payments.** Segments dedicated "Card Services Room" that meets SAQ-A; no PAN ever touches municipal networks, shrinking PCI scope and insurance exposure.

SECURITY CONTROL REQUIREMENTS THAT INSUERS 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 test and log retention.

MASSACHUSETTS SPECIFIC COMPLIANCE PRESURE

- 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
- PCIDSS fo tax pemitting and parking payments

MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

SECURE CLOUD WORKSPACE – CYBER INSURANCE

- **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 <$50k; 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 Secure cloud workspace 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.

SECURITY CONTROL REQUIREMENTS THAT INSUERS 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 test and log retention.

MASSACHUSETTS SPECIFIC COMPLIANCE PRESURE

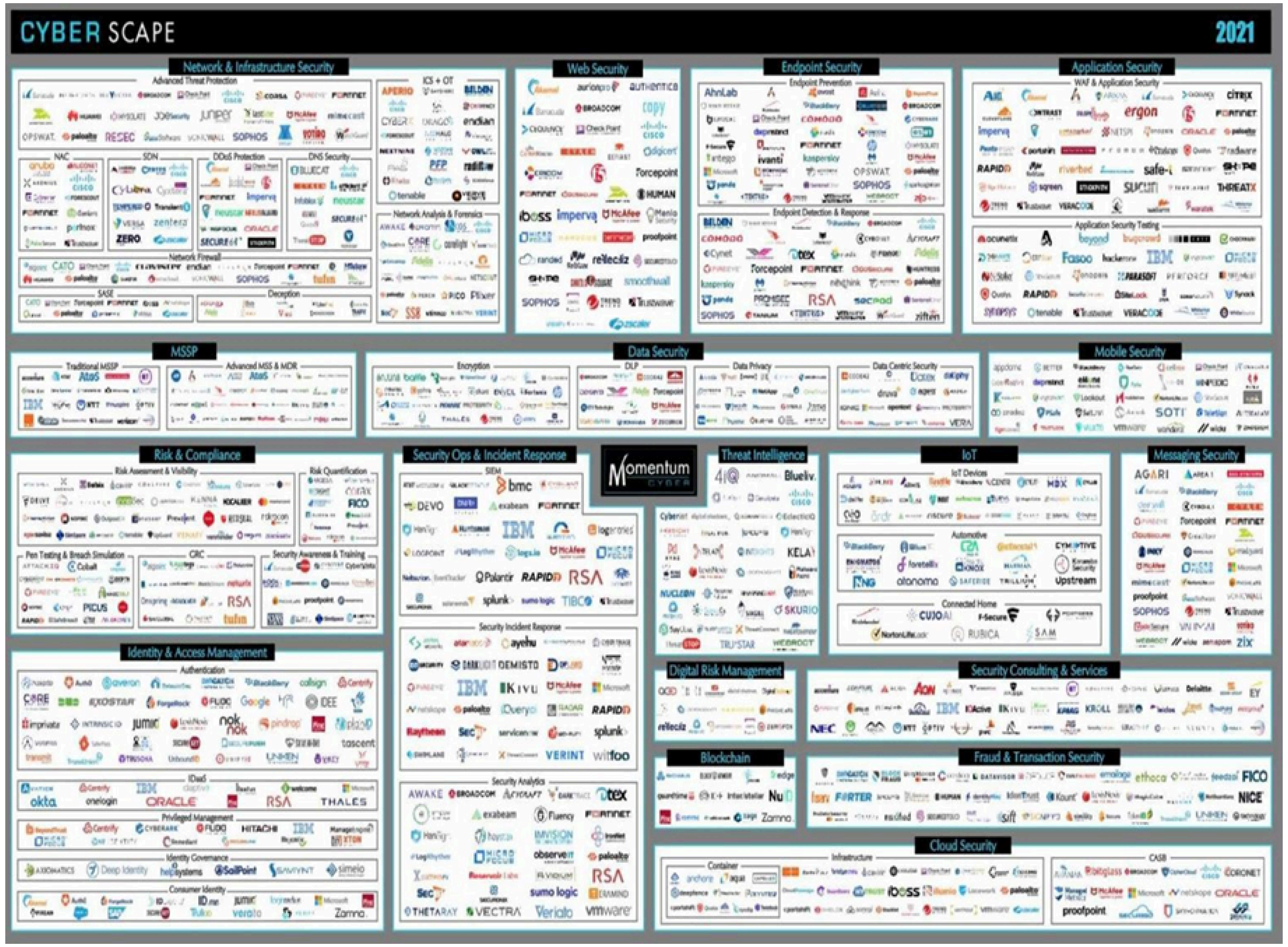
- M.G.L. c. 93H/201 CMR 17 (WISP & encryption rules).
- Massachusetts Public Records Law & Session retention.
- CJIS for municipal police departments.
- FERPA/DESE requirements for school districts.
- HIPAA / EMS & Board of Health
- PCIDSS fo tax pemitting and parking payments

MINDCORE TECHNOLOGIES
POWERED BY: TEHAMA + Microsoft

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

SECURE CLOUD WORKSPACE MANAGER 3.0

VS



WHAT IS THE SECURE CLOUD WORKSPACE

The secure cloud workspace is a secure, scalable platform purpose- built to support Governance, Risk, and Compliance (GRC). By provisioning highly secure data enclaves in the cloud, Secure cloud workspace 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.*

WHAT THE SECURE CLOUD WORKSPACE DOES

The secure cloud workspace uniquely combines secure perimeter data enclaves, cutting-edge cybersecurity services and VDI enabling solution providers to quickly provide comprehensive hybrid work services delivered through fully- managed secure perimeter data enclaves specializing in security, compliance, and data and AI governance

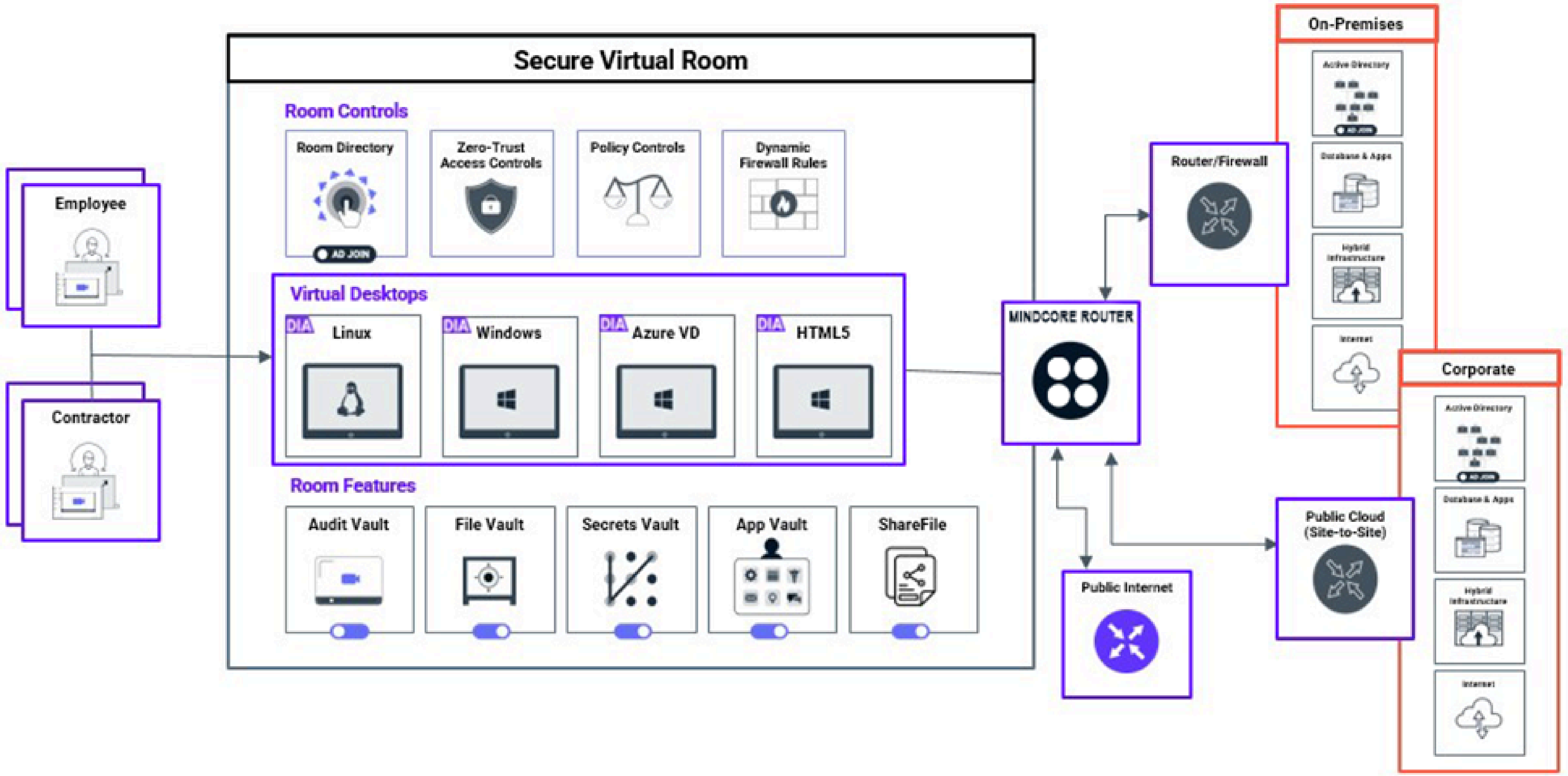
Secure perimeter establishes the following:

The system operates within a tightly governed and secured SOC2-Type 2 and ISO 27001-compliant cloud infrastructure, featuring fully integrated virtual desktops. Access is strictly limited to authorized individuals, who may only interact with permitted data—whether file-based or networked—through approved applications and infrastructure components. This setup ensures a high-integrity audit trail that records all permissions and interactions, thereby enabling comprehensive auditability of all activities conducted within the secure 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.



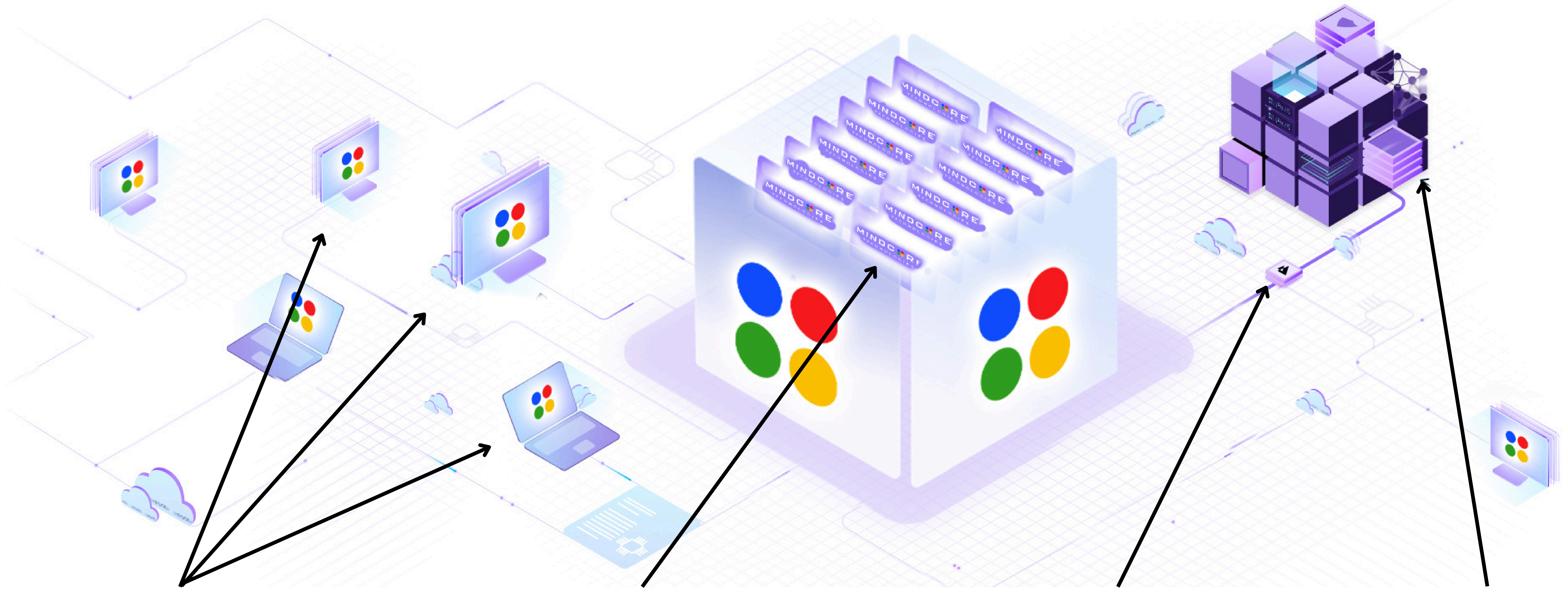
MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

CMMC - ACCELERATION

SIMPLE, SECURE, RELIABLE,AFFORDABLE. PROTECTING DATA, APPS AND WORKFORCE (CMMC, NIST 800-171, GDPR, ISO 27001, SOC2 TYPE II, PCI- DSS, HIPAA, FINRA, OSFI, ETC)



1. TAKE CONTROL OF END POINT

Secure cloud workspace 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 Secure cloud workspace 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 Secure cloud workspace Room operate sas a virtual extension of your secured business infrastructure in the cloud.

MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

EXAMPLE USE CASES

- SECURE HYBRID WORK
- 3RD PARTY ACCESS
- DATA GOVERNANCE
- BUSINESS CONTINUITY AND DISASTER
- ENDPOINT PROTECTION
- M&A
- AI GOVERNANCE
- DDI/DAAS MIGRATION

- CMMC COMPLIANCE
- AUDITOR AND DUE DILIGENCE ENABLEMENT
- REGULATORY COMPLIANCE
- PEN-TESTING AND RED-TEAM ENABLEMENT
- IP PROTECTION
- DEVOPS
- PRIVILEGED ACCESS MANAGEMENT

DATA AND AI GOVERNANCE

WORKSPACE 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 Secure cloud workspace 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 Secure cloud workspace. 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.

MINDCORE
TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

PRIVILEGED ACCESS MANAGEMENT

WORKSPACE 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 to fulfil your various responsibilities (PCI, 23 NYCRR 500, etc).

HERE'S HOW EASY IT IS:

- Create a special-purpose privileged access room on Secure cloud workspace. 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

WORKSPACE SOLUTION

- Provides a fully comprehensive, all-in- one, cloud-based solution that provides safe, reliable remote access to critical systems and data. Secure cloud workspace 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)inany cloud region globally.
- Delegate your rooms to appropriate managers. Teams can then be invited or automatically provisioned using
- Secure .cloud workspace'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.

MINDCORE
TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

AUDITOR AND DUE-DILIGENCE ENABLEMENT

WORKSPACE SOLUTION

- Permit your auditors and invite authorized due-diligence advisors to access your sensitive data and records though a Secure cloud workspace 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 pentesteror auditor.