MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

COMMON & COSTLY CHALLENGES

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

CMMC: COMMON AND COSTLY CHALLENGES

FRAGMENTED ACCESS CONTROLS

- Inconsistent identity providers and RBAC models. across users and contractors.
- Difficulty enforcing MFA and least-privilege access policies.

WEAK EVIDENCE COLLECTION

- Manual or incomplete control mapping to CMMC practices.
- Delays and gaps during audits or assessments.

DISJOINTED TOOLING ENVIRONMENTS

- Conflicting security tools create complexity.
- Redundant spending and inconsistent enforcement.

LACK OF CONTINUOUS MONITORING

- Inadequate logging and endpoint visibility.
- Gaps in incident detection and audit readiness.

CLOUD SPRAWL & SHADOW IT

- Untracked SaaS use creates unmonitored data flows.
- Increased risk of exfiltration and noncompliance.

POOR DATA HANDLING PRACTICES

- CUI stored or transferred through unapproved channels.
- High risk of data leakage or non-compliance.

NO DATA RESIDENCY CONTROL

- CUI may be processed or stored outside U.S. borders.
- DFARS and FedRAMP compliance put at risk.

REMOTE WORKFORCE RISKS

- Unmanaged devices used for sensitive work.
- No safeguards against local storage or unauthorized printing.

UNSECURED THIRD PARTY ACCESS

- Vendors and subs access CUI with no consistent controls.
- Activity logging is often absentor siloed.

DELAYED INCIDENTRESPONSE

- No unified forensic or response tooling.
- Breach notification timelines(72h) at risk.

MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

CMMC: ACHIEVEDWITH SECURE CLOUD WORKSPACE AND WURSTA

FRAGMENTED ACCESS CONTROLS

- Secure cloud workspace Rooms enforce role-based access and MFA automatically.
- Wursta integrates Workspace identity and access policies for context-aware control.

LACK OF CONTINUOUS MONITORING

- Secure cloud workspace records every session and logs all access
- Workspace audit trails centrally managed and reviewable.

POOR DATA HANDLING PRACTICES

- Secure cloud workspace disables file transfer, copy/paste, USB by default.
- Google Drive classification and DLP enforce CUI handling.

REMOTE WORKFORCE RISKS

- Zero Trust desktops in Secure cloud workspace prevent data from reaching unmanaged devices
- Wursta configures secure Workspace access via verified devices or Chromebook

WEAK EVIDENCE COLLECTION

- Secure cloud workspace provides CMMC-ready evidence artifacts automatically.
- Google Workspace logs and file activity.

UNSECURED THIRD PARTY ACCESS

- Secure cloud workspace Rooms isolate and time-box third-party activity
- Google Shared diverse strict CUI access by role and time.

DISJOINTED TOOLING ENVIRONMENTS

- Secure cloud workspace delivers a fixed, certified stack that maps directly to CMMC controls.
- Wursta consolidates Workspace security controls for easier policy alignment.

CLOUD SPRAWL & SHADOW IT

- Secure cloud workspace session and file logs reveal risky behavior or tools.
- Wursta enables API-level SaaS discovery and enforcement.

NO DATA RESIDENCY CONTROL

- Secure cloud workspace Rooms can be deployed in U.S. regions with geo-locking.
- Google Workspace U.S.-only data regions enforced by Wursta.

DELAYED INCIDENTRESPONSE

- Secure cloud workspace's kill switch and instant evidence export accelerate response.
- Google Workspace alert in hand IR workflows managed by Wursta reduce delay.

MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

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

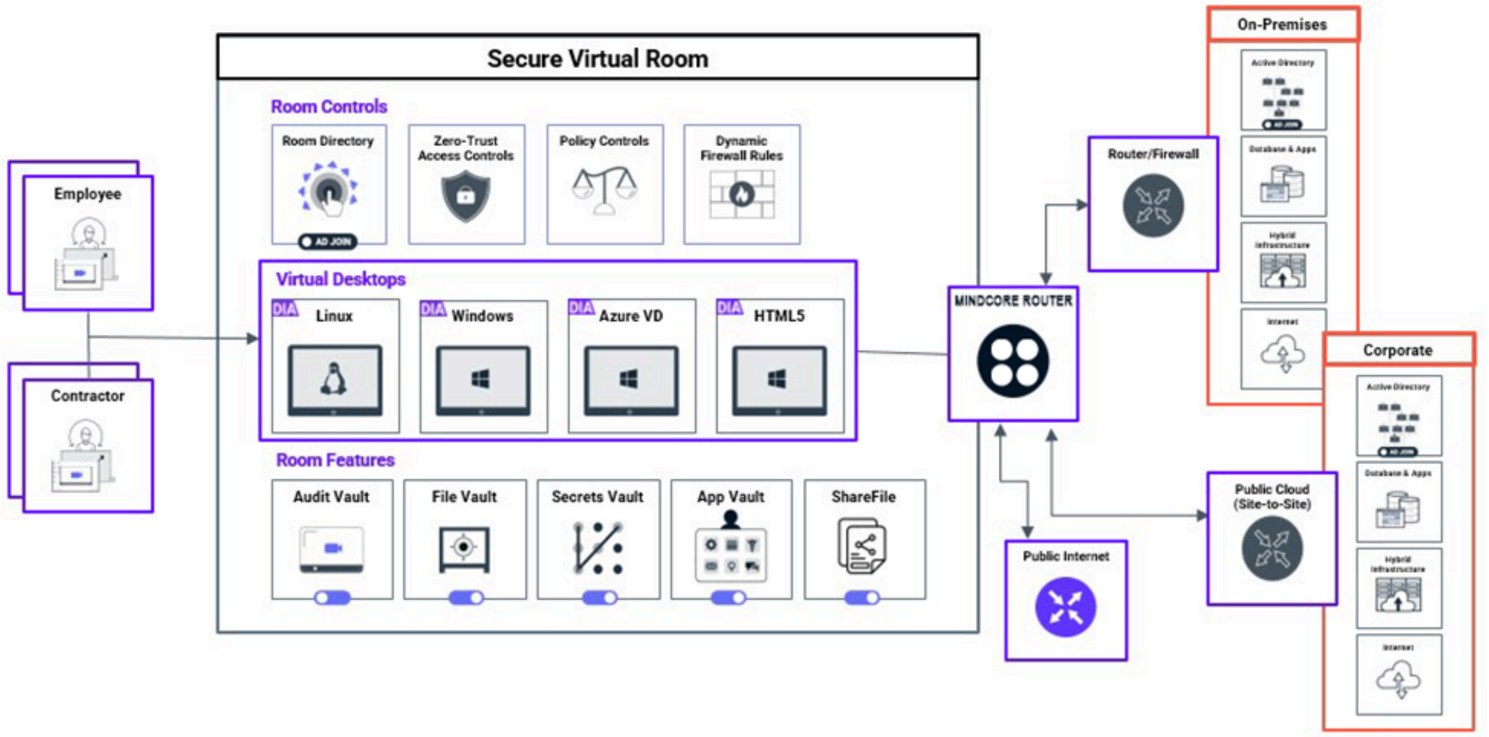
Secure perimeter establishes the following:

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)

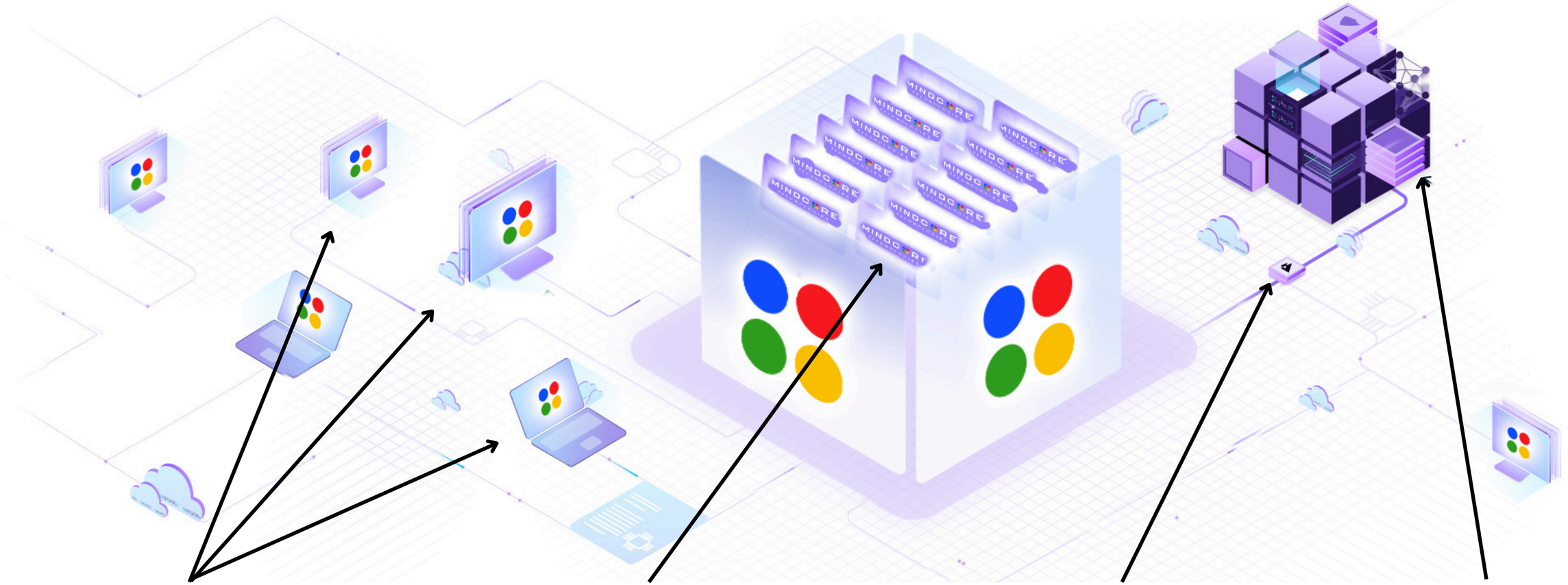
- Secure data enclaves.
- Comprehensive suite of security and cyber services.
- Auditing and Monitoring.
- Strict Access Control.
- Centralized management, provisioning and cost optimization.
- Integrated infrastructure and virtual desktop.



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.

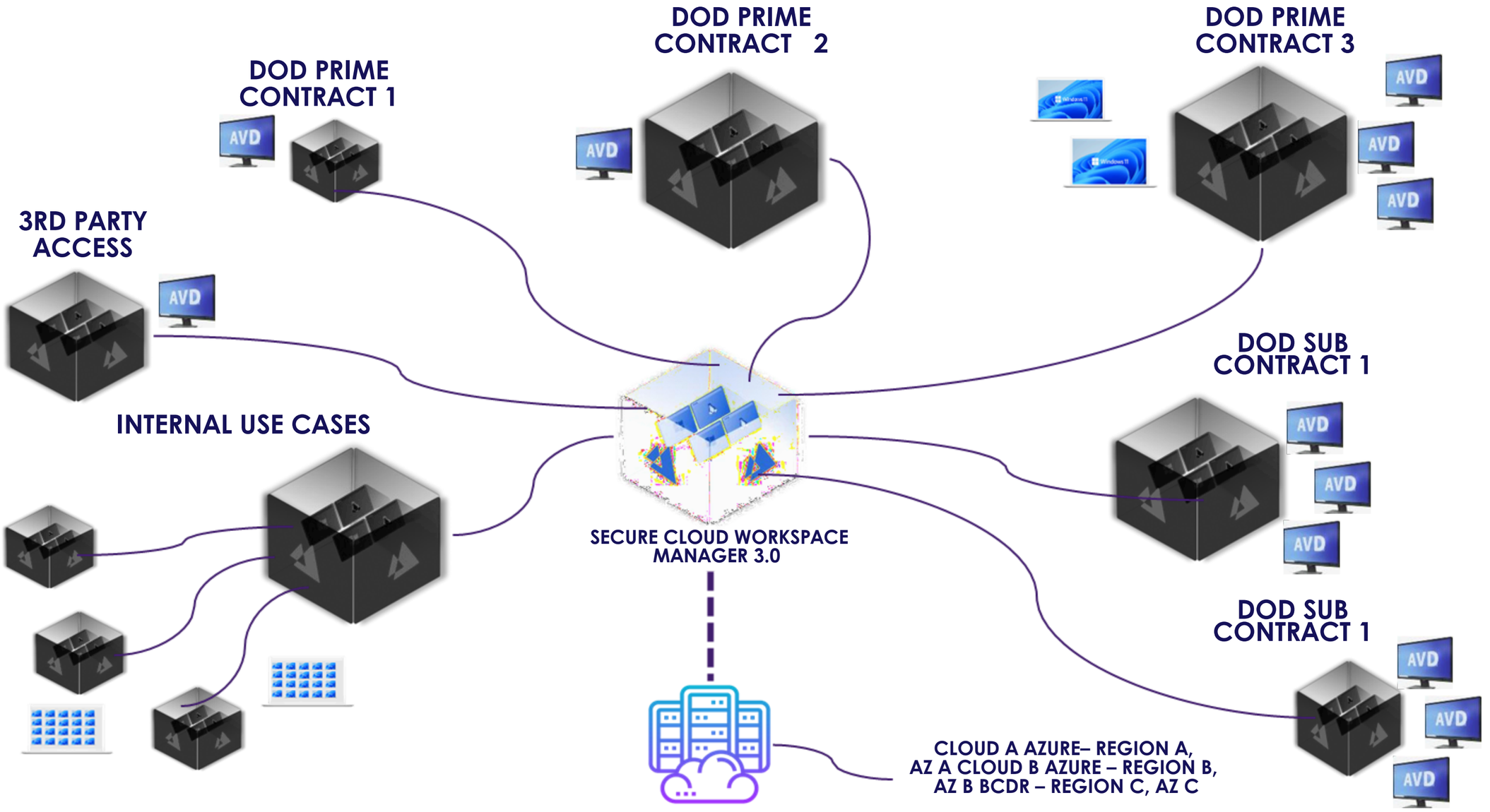
4. ENTERPRISE SECURE PERIMETER BUSINESS SERVICE(S)

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

MINDCORE TECHNOLOGIES

POWERED BY:

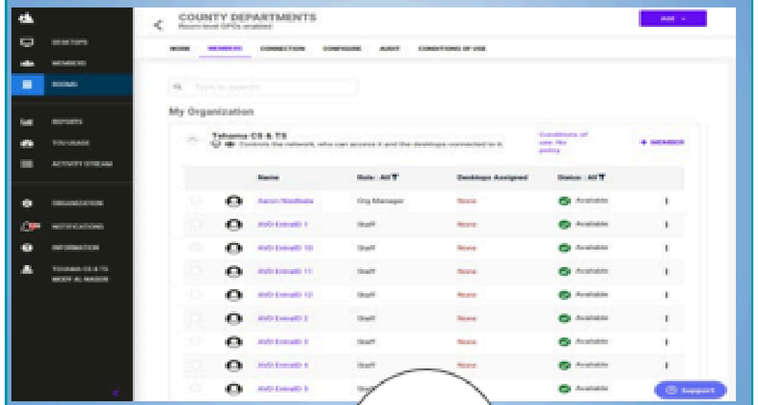
TEHAMA + Microsoft



MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

SECURE, SCALABLE WORKSPACES FOR ANY USE CASE

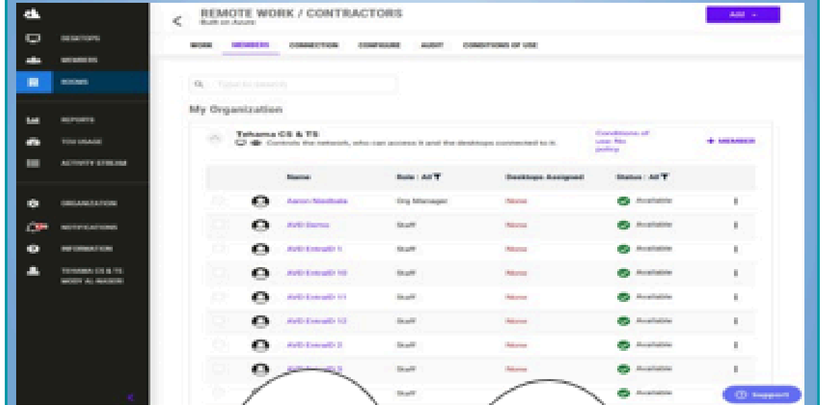
DoD Prime Contracts



Staff located ANYWHERE

- Prime Contract #1
- Prime Contract #2
- Prime Contract #2

DoD Subcontracts

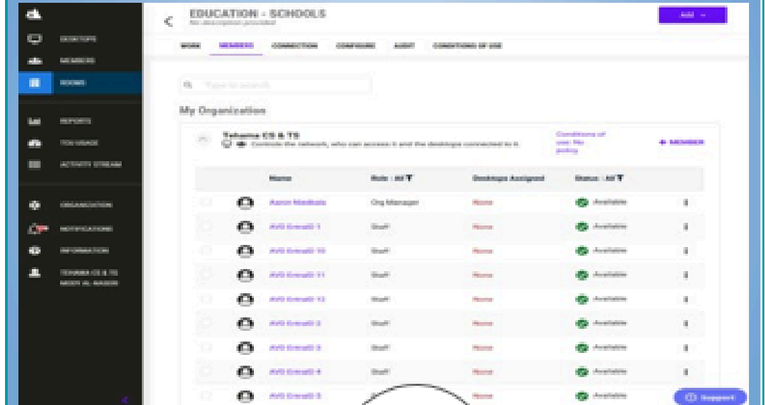


Staff

3rd Party Contractors

- Subcontract #1
- Subcontract #2

Internal Use Cases



Staff located ANYWHERE

- HR
  Location #1
- Information Technology
  Location #1
- Finance
  Location #2

MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

CMMC: CUSTOMER “X”

DOD FACILITY DESIGNING CONTRACT

- CMMCII compliance.
- Data residency, protection& security.
- CUI Governance.
- Role-based privileged access controls.
- Key management.

RESULTS

- Increased TAM, achieved by the ability to win CMMC-based DoD contracts.
- Accelerated CMMC II Compliance with assertion - ready solution.
- Achieved Certified Third Party Audit Organization (C3PAO) CMMC compliance verification.
- Reduced IT burden by eliminating physical endpoint compliance checks & policy enforcements.

SECURE CLOUD WORKSPACE & WURSTA SOLUTION

- Cohesive CMMC cloud-native compliant enclave.

- DoD Facility Designing Contract
- CMMCII compliance
- Data residency, protection& security
- CUI Governance
- Role-based privileged access controls.
- Key management

- CMMC-controlled Virtual Desktop Infrastructure for governed CUI workloads.
- Restrictive access to integrated Google Services for data availability and classification.
- CUI Loss Prevention.
- Integrated context aware access.
- Advanced encryption services.

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.

MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

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.

MINDCORE TECHNOLOGIES
POWERED BY:
TEHAMA + Microsoft

MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

SECURING YOUR DIGITAL TOMORROW, TODAY!

Your Trusted Partner in Managed IT, Cloud, & Cybersecurity

MATT ROSENTHAL

CEO, MINDCORE TECHNOLOGIES

Phone: (561) 404-8411

Website: https://mindcore.com