SECURE CLOUD WORKSPACE FAQs

Proven IT and Cybersecurity Solutions.
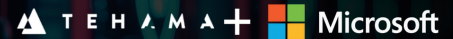
BELOW ARE THE MOST COMMONLY ASKED QUESTIONS WE RECEIVE FROM HEALTHCARE ORGANIZATIONS EXPLORING OUR FULLY MANAGED SECURE CLOUD WORKSPACE, DESIGNED, DEPLOYED, MANAGED BY MINDCORE POWERED BY TEHAMA | MICROSOFT. THESE FAQS ARE DESIGNED TO HELP YOU BETTER UNDERSTAND HOW OUR SOLUTION WORKS, HOW IT FITS INTO YOUR ENVIRONMENT, AND WHY IT MAY BE THE RIGHT FIT FOR YOUR COMPLIANCE, SECURITY, AND OPERATIONAL NEEDS.

1. HOW IS THIS DIFFERENT FROM A VPN OR VDI?

UNLIKE VPNS OR VDI, OUR SOLUTION PROVIDES ZERO-TRUST, AIR-GAPPED ACCESS WHERE DATA NEVER TOUCHES THE ENDPOINT. IT'S FULLY MANAGED, FASTER TO DEPLOY, AND INCLUDES BUILT-IN COMPLIANCE TOOLS THAT VPNS AND VDIS TYPICALLY LACK.

2. IS THIS SOLUTION HIPAA COMPLIANT?

YES. THE PLATFORM MEETS HIPAA, SOC 2, AND HITRUST REQUIREMENTS WITH AUDIT-READY LOGS, ROLE-BASED ACCESS CONTROL, DATA ENCRYPTION, AND SESSION RECORDING—ALL BUILT IN AND CONTINUOUSLY UPDATED.

3. IS THIS SOLUTION EXPENSIVE?

NOT AT ALL. IT'S OFTEN MORE COST-EFFECTIVE THAN THE COMBINED EXPENSES OF ENDPOINT TOOLS, VPN LICENSES, AUDIT PREP, AND BREACH RECOVERY. MOST ORGANIZATIONS SEE A NET REDUCTION IN IT/SECURITY COSTS BY 20–35%.

4. WE USE MICROSOFT OR CITRIX—WHY WOULD WE SWITCH?

OUR PLATFORM IS PURPOSE-BUILT FOR HEALTHCARE COMPLIANCE AND ZERO-TRUST SECURITY, WITH EASIER ONBOARDING, NO ENDPOINT RISK, AND NO INFRASTRUCTURE FOR YOU TO MANAGE.

5. CAN OUR IT TEAM MANAGE THIS INTERNALLY?

YOU DON'T HAVE TO. IT'S FULLY MANAGED BY OUR TEAM—WE HANDLE EVERYTHING FROM PROVISIONING TO COMPLIANCE OPERATIONS, FREEING YOUR IT STAFF TO FOCUS ON HIGHER-VALUE WORK.

6. HOW QUICKLY CAN WE GET STARTED?

MOST CUSTOMERS GO LIVE IN DAYS, NOT WEEKS. SECURE WORKSPACES CAN BE PROVISIONED ALMOST INSTANTLY AFTER ONBOARDING AND ACCOUNT SETUP.

DESIGNED, DEPLOYED, MANAGED BY MINDCORE

7. WHAT IF A DEVICE ACCESSING THE WORKSPACE GETS COMPROMISED?

NO DATA IS EVER STORED ON THE DEVICE. THE SECURE WORKSPACE ISOLATES ALL ACTIVITY IN THE CLOUD, SO EVEN IF A DEVICE IS LOST OR INFECTED, YOUR SYSTEMS AND PHI ARE FULLY PROTECTED.

8. WILL THIS INTEGRATE WITH OUR CURRENT SYSTEMS OR EHR PLATFORM?

YES. USERS ACCESS YOUR EXISTING SYSTEMS INSIDE THE SECURE WORKSPACE WITH NO NEED TO CHANGE HOW YOUR APPS OR EHR SYSTEMS ARE CONFIGURED.

9. IS THE INFRASTRUCTURE U.S.-BASED?

YES. MINDCORE'S INFRASTRUCTURE IS HOSTED IN TAMPA, FLORIDA, AND WE CAN CONFIGURE U.S.-ONLY DATA RESIDENCY TO MEET YOUR REGULATORY REQUIREMENTS.

10. IS THIS A STABLE LONG-TERM SOLUTION?

ABSOLUTELY. MINDCORE IS TRUSTED BY HEALTHCARE PROVIDERS, GOVERNMENT AGENCIES, AND LARGE ENTERPRISES. OUR PLATFORM IS DESIGNED FOR LONG-TERM COMPLIANCE AND SECURITY AT SCALE.

ADDITIONAL FAQS: THE VALUE OF A SECURE DATA ENCLAVE

---

11. WHAT EXACTLY IS A SECURE DATA ENCLAVE?

A SECURE DATA ENCLAVE IS A CONTROLLED, ISOLATED ENVIRONMENT WHERE USERS CAN ACCESS SENSITIVE APPLICATIONS AND DATA WITHOUT THAT DATA EVER LEAVING THE SECURE PERIMETER. IT ELIMINATES ENDPOINT RISK AND ENSURES FULL VISIBILITY INTO ALL USER ACTIVITY.

12. WHY IS A SECURE DATA ENCLAVE BETTER THAN TRADITIONAL DESKTOP ACCESS?

TRADITIONAL ACCESS OFTEN LEAVES DATA EXPOSED ON USER DEVICES OR VULNERABLE TO MISCONFIGURATION. A SECURE DATA ENCLAVE ENSURES ZERO DATA LEAKAGE BY ISOLATING ACCESS IN THE CLOUD AND ENFORCING POLICY CONTROLS AT EVERY LAYER.

13. HOW DOES A SECURE ENCLAVE REDUCE BREACH RISK?

BECAUSE NO DATA EVER TOUCHES THE USER'S PHYSICAL DEVICE AND ALL ACTIVITY IS RECORDED AND MONITORED, THE ATTACK SURFACE IS DRASTICALLY REDUCED. EVEN IF A DEVICE IS COMPROMISED, THE ENCLAVE PROTECTS THE DATA AND DENIES EXTERNAL THREATS.

14. CAN A SECURE DATA ENCLAVE HELP WITH VENDOR ACCESS AND COMPLIANCE?

ABSOLUTELY. IT ALLOWS THIRD-PARTY VENDORS TO SECURELY ACCESS ONLY WHAT THEY NEED, WITH FULL SESSION VISIBILITY, TEMPORARY ACCESS, AND BUILT-IN AUDIT LOGS—MAKING HIPAA AND SOC 2 COMPLIANCE MUCH EASIER TO MAINTAIN.

DESIGNED, DEPLOYED, MANAGED BY MINDCORE