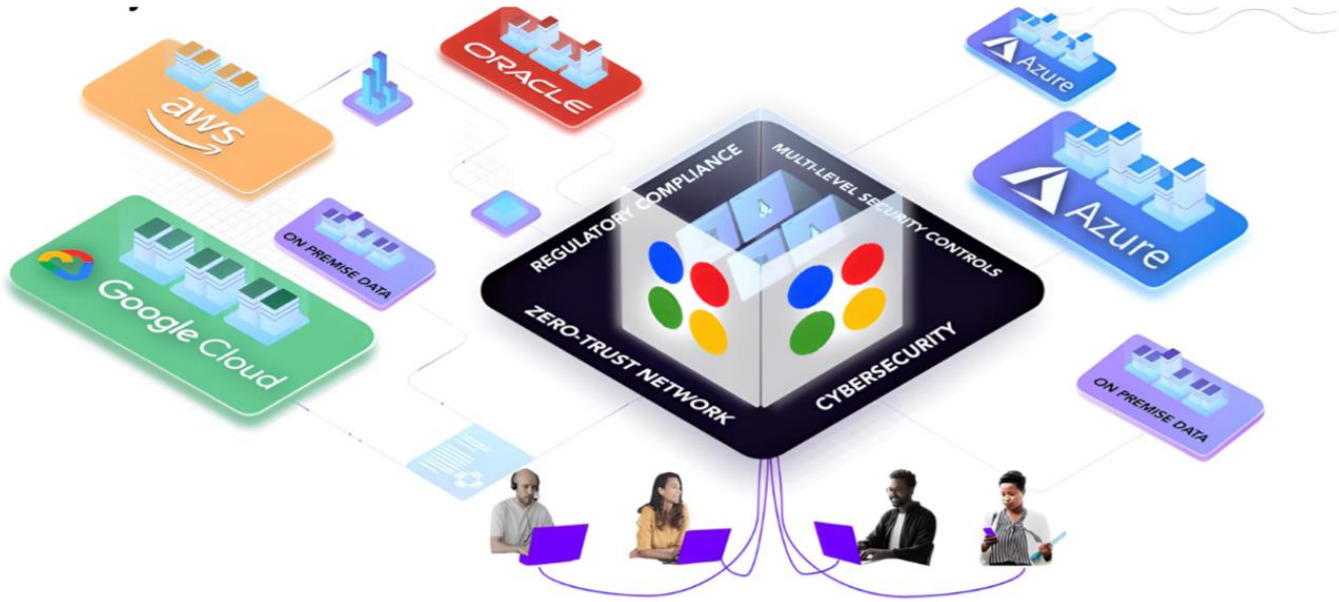


MINDCORE SECURE CLOUD WORKSPACE

MINDCORE SECURE DATA ENCLAVES DESIGNED TO SECURE ACCESS TO DATA AND APPLICATIONS IN ANY CLOUD

MINDCORE TECHNOLOGIES

POWERED BY:

TEHAMA + Microsoft

Executive Summary

In today's rapidly evolving digital landscape, enterprises' ability to safeguard sensitive data across distributed environments has become more complex and challenging than ever. This white paper delves into the critical risks and hurdles organizations encounter, as traditional solutions like virtual desktop infrastructure (VDI) and desktop-as-a-service (DaaS) struggle to keep pace with these changes and will discuss how Mindcore Technologies' innovative data enclaves are revolutionizing data protection.

Our exploration will provide a thorough understanding of Mindcore's data enclave platform, highlighting our innovative strategy and essential features. These include advanced access control, comprehensive data and AI governance, stringent regulatory compliance, and effective attack surface reduction—all meticulously designed to enhance risk profiles and bolster security posture.

The objective of this white paper is to empower organizations with a comprehensive understanding of Mindcore's data enclave platform and the insight needed to navigate the complexities of secure data management in hybrid work environments. Our goal is to enable the implementation of robust attack surface protection strategies while ensuring adherence to the highest standards of security and compliance, without sacrificing agility or performance."

Introduction

In today's complex digital environment, organizations must balance the growing demand for data-driven innovation with the imperatives of securing sensitive information and meet evolving regulatory obligations. As cyber threats increase in sophistication and data privacy regulations become more stringent, traditional approaches to data protection are often not sufficient, too complex or cost
prohibitive.

To address these challenges and more, Mindcore Technologies developed its data enclave architecture—a next-generation solution that overcomes the limitations of legacy technologies like VDI, DaaS and VPN. Mindcore's secure, governed enclaves are purpose-built to support the management, analysis, and collaboration of sensitive data without compromising security or compliance. These controlled environments isolate critical workloads, enforce strict access policies, and give organizations the confidence to operate securely with their most confidential information.

This paper outlines how data enclaves provide centralized management, policy enforcement and mitigate risks associated with unrestricted application and data access, while also supporting secure integration of emerging technologies such as artificial intelligence (AI). By enabling AI adoption within a secure
perimeter, organizations can harness its benefits while maintaining strong governance over data use and movement.

Finally, we examine how data enclaves offer an operational and compliance advantage over traditional strategies such as virtual desktop infrastructure (VDI) and Desktop-as-a-Service (DaaS) models, which often fall short in meeting today's stringent security and regulatory demands.

Table of Contents

The Challenge of Data Security and Governance

Hybrid work presents unique security challenges. Organizations must implement comprehensive strategies that integrate advanced security measures and compliance frameworks to protect sensitive information and navigate the evolving digital landscape. The advancement of artificial intelligence further exacerbates this challenge.

Key challenges of hybrid work models include:

- Increased vulnerabilities
- Regulatory compliance challenges
- Governance and policy enforcement
- Siloed technologies and security gaps
- Prohibitive costs
- Operational complexity and overhead

Increased Vulnerabilities

Unrestricted data access across remote devices and networks significantly increases the risk of data breaches. Employees accessing sensitive information from various locations and devices can expose organizations to cybersecurity threats. Traditional security measures, primarily designed for on-premises environments, often fall short of addressing the dynamic and distributed nature of hybrid work.

Complex Regulatory Landscape

Organizations must navigate a complex and evolving landscape of data privacy regulations, which vary by region and industry. Without robust governance solutions, the risk of non-compliance is heightened, leading to legal repercussions and financial penalties. As regulations become more stringent, real-time policy enforcement and auditability become essential for ensuring compliance.

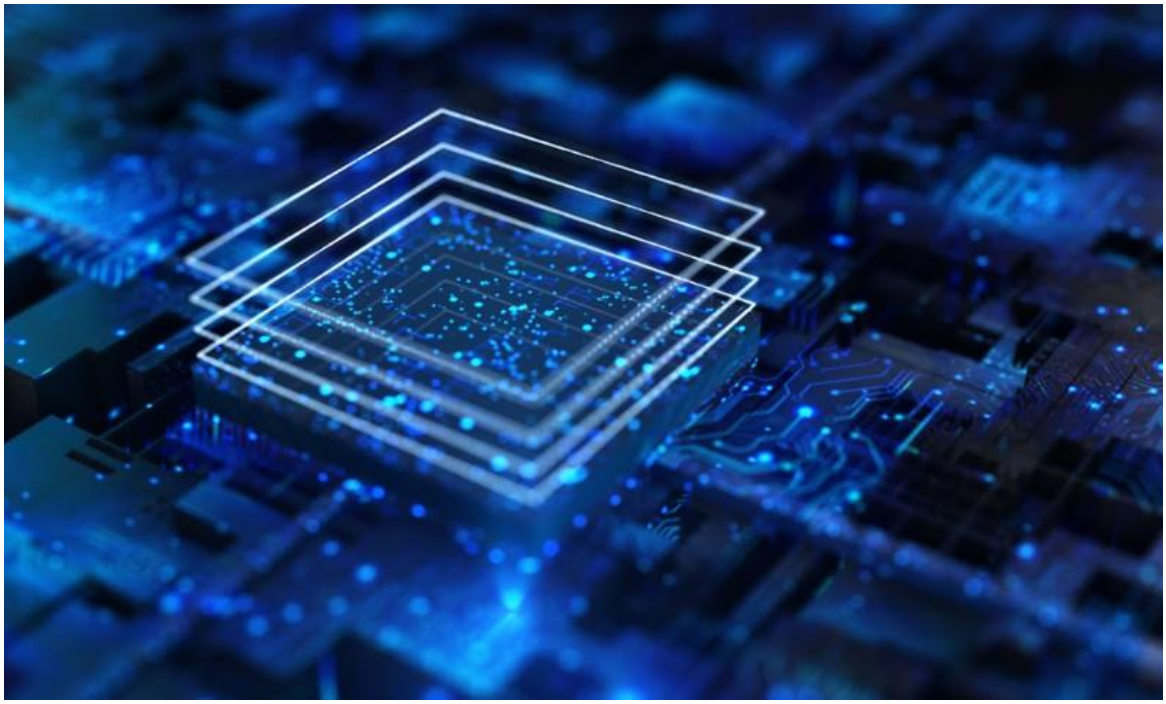
Governance and Policy Enforcement

Effective governance depends on automated, continuous policy enforcement from keyboard to data and applications. Relying on manual processes or integrated, siloed technologies introduces inconsistencies and blind spots that can undermine both security and regulatory compliance. To address this, organizations require systems that are truly ‘end-to-end’ and also offer real-time visibility across workloads, who is accessing data, how it is being used, and when, enabling rapid detection of non-compliance and swift response to potential threats.

Mindcore's Solution: Secure Data Enclaves

Mindcore addresses these challenges with its innovative Data Enclaves—secure, tightly controlled environments designed for safe data management. By establishing a governed ecosystem, organizations can protect sensitive information while facilitating collaboration, advanced analytics, and sustained workforce productivity.

Mindcore's solution incorporates automated governance features that enable real-time compliance enforcement, significantly mitigating risks associated with unrestricted data access and ensuring that organizations meet the highest security and regulatory standards.



The Governance Gap in AI Adoption

Artificial intelligence (AI) is arguably the most disruptive enterprise technology of our generation. Generative AI could add between $2.6 trillion and $4.4 trillion annually to the global economy, translating to a 15–40% productivity gain[1]. Despite its potential to boost productivity, many organizations are slow to adopt AI technologies largely because the landscape of security and governance within these organizations evolved before AI emerged. In other words, their critical systems are often hosted on traditional infrastructures or private clouds, which leads to fragmented data governance and security measures.

This fragmentation is further complicated by overlapping technologies and untagged categories of data, creating an untenable situation where anyone can use any application to access any data they can reach.

Such vulnerabilities prevent enterprises and public sector organizations from fully embracing AI technologies at scale, especially for high-risk, regulated work. Robust governance solutions that facilitate real-time policy enforcement, auditing, and compliance are needed urgently.

In summary, key challenges undermining secure and compliant data management include:

a. Fragmented data governance and security:
   - Disjointed security measures and governance frameworks that involve overlapping technologies.
   - Data is frequently untagged and mixed across various categories of importance, complicating management, and oversight.

a. Unrestricted data access risks:
   - The current state allows anyone within the organization to utilize any application to access any data they can reach, creating untenable security vulnerabilities.
   - No real-time management, oversight, and resolution:
   - Enterprises do not have the necessary tools to enable them to easily and immediately establish highly secure AI-driven data governance enclaves.

[1]. Sources
McKinsey Global Institute, "The Economic Potential of Generative AI: The Next Productivity Frontier," 2023.
PwC, "2024 Global AI Jobs Barometer."
EY, "The Productivity Potential of Generative AI," 2024. Note** The exact percentage can vary depending on industry, application, and implementation quality.

Limitations of Traditional Approaches

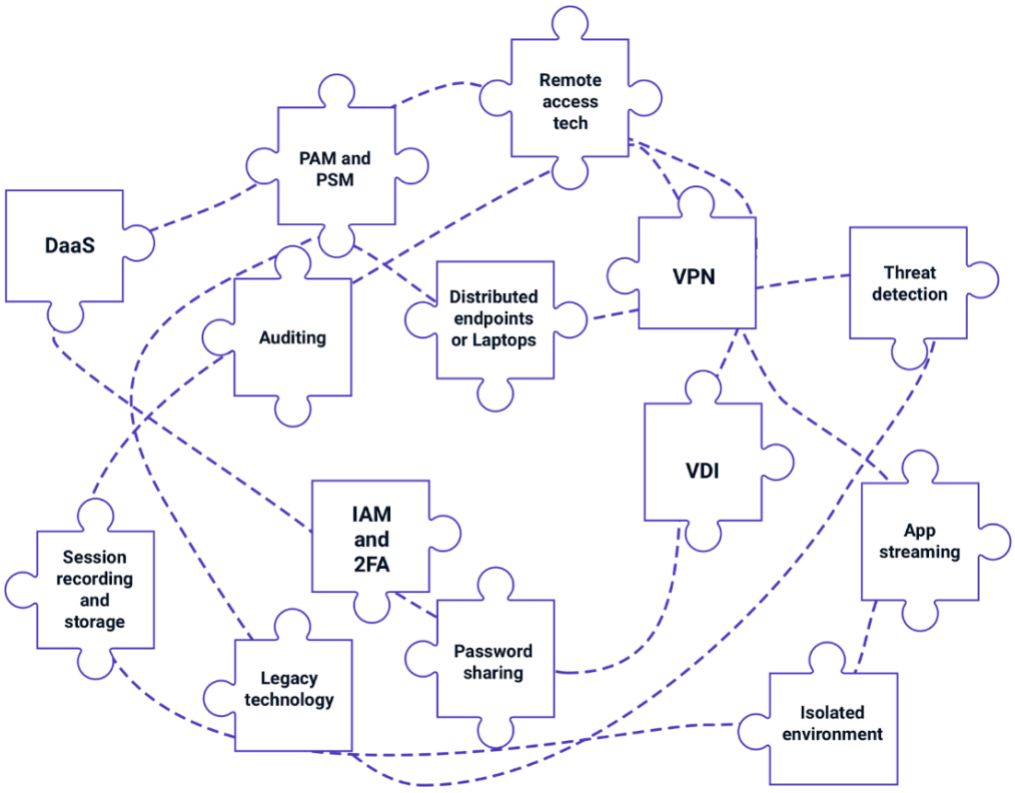
Today, organizations are rapidly reimagining their workplaces, empowering employees to work from anywhere—whether at home, on the go, or in shared spaces. While this shift unlocks unprecedented levels of flexibility, agility, and access to global talent, it also introduces a new set of security and operational risks.

The traditional approach to cybersecurity, centered around perimeter defenses and static infrastructure, is increasingly ill-equipped to meet these challenges. Organizations rely heavily on disparate, siloed solutions such as VPNs, legacy VDI, DaaS and point security tools. These systems require extensive evaluation, procurement, integration, and ongoing management, creating a complex and costly security landscape that is unsustainable at scale. See Figure 1. This fragmented infrastructure often results in delays, security gaps, and increased operational overhead.

Today's approach to delivering cybersecurity and hybrid-work solutions is often too complex, requires significant engineering or integration, or simply lacks native critical security features such as multi-factor authentication (MFA), anti-virus protections, and secure communication channels comparable to VPNs, especially when connecting cloud-based operating systems to enterprise assets. This exposes organizations, particularly those in highly regulated sectors such as banking, health care, insurance, and government, to significant compliance and security risks.

Moreover, environments like VDI and DaaS lack essential IT infrastructure components—including firewalls, routers, patch management, OS image lifecycle management, and compliance enforcement mechanisms—that are vital for enterprise-scale development, operations, and security governance.

Figure 1 – Mindcore delivers a data enclave with built-in access controls, auditability and all relative mechanisms through a unified platform.



The Path Forward

What organizations require is a fundamentally different approach—one that is secure, compliant, rapid to deploy, and adaptable to the complexities of hybrid work and the changing regulatory and compliance landscape. Solutions must provide a true 'out-of-the-box' architecture, eliminating the need for extensive engineering and long deployment timelines while also eliminating security gaps, improving attack surface area, and supporting stringent regulatory standards.

By providing a comprehensive security perimeter around these workspaces and infrastructure, integrating strong access controls, continuous monitoring, and enterprise-grade infrastructure, environments can be transformed into trusted, virtual extensions of the corporate network.

This enables organizations to support a global, distributed workforce with confidence. Simultaneously, all endpoints, whether remote or on-premises, are protected and policed to a consistent policy-based standard of care, ensuring all data and applications are accessed consistent in accordance with all applicable regulatory, compliance and governance requirements.

Mindcore Data Enclaves:
Next Generation Cybersecurity

At the core of Mindcore's innovative platform is a highly secure, proprietary, cloud-native architecture that delivers specialized environments designed for the secure collection, storage, and analysis of confidential data. These environments establish well-governed, controlled ecosystems that protect sensitive information from unauthorized access and breaches, empowering hybrid workforces to access critical data securely, leveraging the scalability and flexibility of the cloud, without compromising security, compliance, or regulatory standards.

The platform's architecture creates virtual data enclaves— secure perimeters or "rooms"—around cloud workspaces, data, applications, and productivity tools. By establishing these secure perimeters, Mindcore's data enclaves address the unique security, operational, and user challenges posed by today's complex and evolving threat environment, see Figure 2 below.

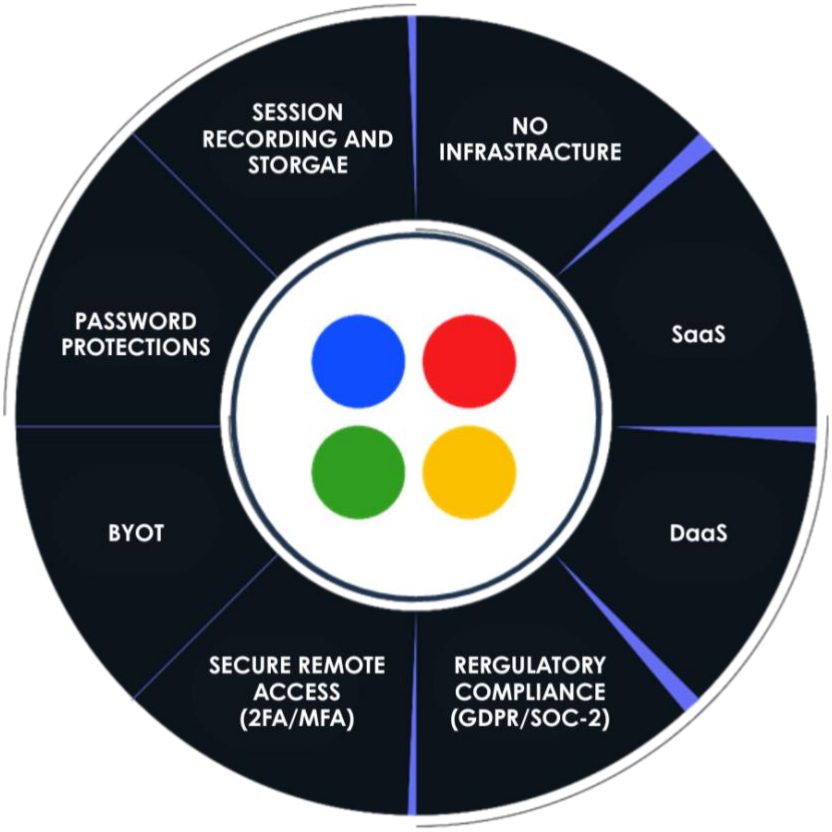


Figure 2 - Mindcore's Platform: Enabling Secure Data Enclaves – Traditional security models rely on fragmented tools that increase complexity and cost and often fail to eliminate technology gaps.

These enclaves are logical groupings of users and resources, enabling organizations to rapidly deploy and provision policies, desktops, services (such as applications), and network infrastructure. This ensures immediate, secure, and scalable work environments across the enterprise.

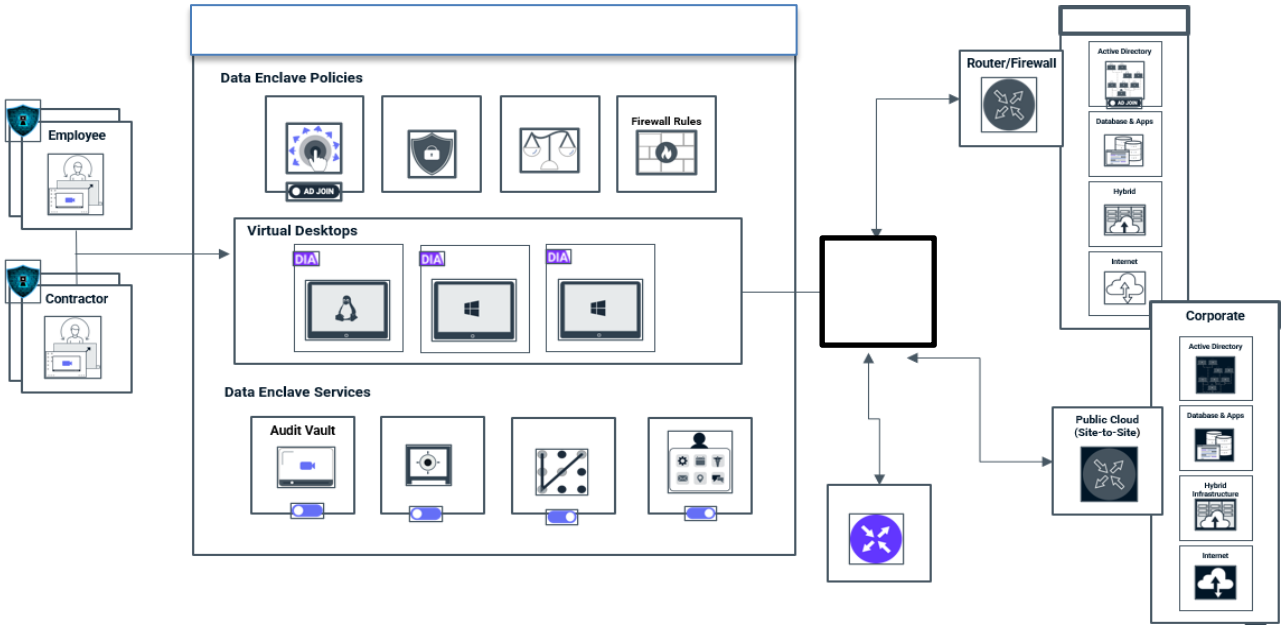
Key Benefits and Business Value

- **Centralized management**, security and cost optimization
- **Eliminate siloed technologies**: with unified, policy-driven security management across all environments.
- **Enhanced attack surface protection:** with advanced tools to identify, mitigate, and manage potential threats proactively.
- **Stringent access controls:** with granular level controls ensuring only authorized personnel can access sensitive data.
- **AI governance:** automated, AI-driven governance, enabling real-time compliance enforcement
- **Regulatory compliance:** supporting organizations in meeting the highest standards of security and compliance, particularly in heavily regulated industries.

Mindcore's data enclaves represent a paradigm shift—building a secure, flexible, and compliant foundation for enterprise data management in an increasingly complex digital world.

A detailed breakdown of Mindcore's security architecture and feature set is available in the appendix at the end of the document.

Figure 3 - Mindcore data enclave delivered as part of an integrated uniform policy-based cybersecurity platform



Secure Controlled Network Infrastructure

Trusted, Secure Channels

To protect sensitive data and systems, it's critical to ensure that user workspaces connect to enterprise resources through secure, controlled communication paths. Traditional methods like VPNs often introduce risk by allowing untrusted devices direct access to the corporate network, potentially enabling the spread of malware and unauthorized access across systems. In addition, VPNs can be costly to maintain, requiring dedicated hardware, ongoing support, and complex management.) To ensure the most rigorous level of compliance and security Mindcore provides an extensive range of built-in mechanisms and controls, including

Per-user MFA, Least-Privilege Role-Based Access Controls

Mindcore enforces multi-factor authentication or SSO and granular role-based access controls (RBAC) at the user level. It also provides seamless integration with the enterprise's preferred choice of identity provider. This ensures only the right individuals have access to the right resources, dramatically reducing the risk of credential misuse or privilege escalation.

Real-time Malware & DLP Scanning of All file Transfers

All file transfers in and out of Mindcore Rooms are scanned in real time for malware and data loss prevention (DLP) violations. This proactive layer of protection helps safeguard sensitive data and ensures compliance during activities like model training or data exchange.

Logical Isolation of Each Room (VPC-to-VPC Segmentation)

Each Mindcore Room operates in a logically isolated virtual environment, ensuring that communication between Rooms and enterprise resources is tightly controlled. This segmentation prevents lateral movement across systems, reducing the risk of unauthorized access and malware propagation.

Zero-Trust Architecture

Mindcore employs a zero-trust model, granting access explicitly on a per-application basis, down to specific IP addresses and ports. This approach minimizes the risk of lateral movement by denying default access and incrementally granting permissions only as needed.

Dynamic User and Endpoint Management

Automated, API -driven synchronization with identity management systems (using protocols such as SAML, OAUTH, SCIM) ensures real-time updates of user access based on role, project, or contractual status. This reduces administrative overhead and enhances security.

Trusted Endpoints and Segregation

To prevent malware and unauthorized access, Mindcore Technologies' innovative platform approach provides comprehensive endpoint management and protection for both physical and virtual devices. It delivers real-time security features, such as anti-malware, exploit defense, and behavioral monitoring—for physical endpoints, while creating protected, governed data enclaves with integrated virtual desktops to enforce strict access controls, automate compliance, and safeguard sensitive data during remote work. This ensures that workflows are secure and compliant across all endpoints.

How Mindcore Data Enclaves Work

Mindcore's data enclaves use presentation-layer protocols (e.g., HTTP, PCoIP) to securely deliver virtual desktops and applications to remote endpoint devices. This approach ensures that the virtual operating system remains isolated within a secure perimeter, protecting it from viruses, malware, or other threats that may reside on the remote endpoint (Figure 3).

Within the secure perimeters, administrators and end users may create collaborative workspaces using either Windows or Linux workspaces. These workspaces can be customized to conform to corporate desktop image policies. End users access their productivity tools and are granted secured, logged, and monitored access to corporate assets through these workspaces, whether such assets are contained on-prem or in the cloud. Mindcore secure perimeters (Data Enclaves) are accessed after successfully negotiating authentication using SSO and multi-factor authentication with the Mindcore platform. End users—including employees, third parties or contractors—establish remote access using their in-field devices. This eliminates the need to provide end users with dedicated hardware or mobile devices. Access is controlled through presentation-layer protocols in a data center or hosted in the cloud.

Access credentials are stored by the enclave administrator, and access to these credentials is logged for traceability. These credentials cannot be removed from the scope of the secure perimeter by end users, only administrators. This prevents the risk of administrative credentials leaking out of the perimeter.

In addition to the collaborative workspaces, the secure perimeter includes other IT-supporting framework components, all provided as SaaS capabilities in a single administrative workflow. To administer, control, and track zero-trust access to the corporate assets, a fully functioning and redundant firewall is contained within the secure perimeter, allowing administrators to explicitly 2specify which application—including the internet—end users can access. The default setting for this firewall is "no access." All accesses are logged, should a review be necessary.

All activity within user workspaces is automatically recorded, providing a complete visual audit trail. These session recordings are readily available to administrators for review when needed, supporting compliance and incident investigation.

Traditional VPNs are no longer required. Instead, secure, encrypted connectivity between the secure perimeter and enterprise systems is enabled through the Mindcore Gateway—a lightweight, dedicated software appliance deployed alongside network assets. The Gateway establishes and maintains a secure, encrypted connection with the secure perimeter's firewall, ensuring safe data transmission. It operates with minimal IT overhead and receives regular updates from the Mindcore platform, ensuring continuous security and performance improvements.

Conclusion

Cyber threats now span careless insiders, organized crime, and nation-state actors—each escalating in frequency and sophistication. For organizations with a distributed or hybrid workforce, the attack surface expands even faster: stolen credentials fuel 38%[2] of breaches, while unmanaged endpoints invite ransomware and data exfiltration. At the same time, legacy infrastructure and patchwork compliance frameworks leave security teams stretched thin. This white paper outlines a practical blueprint for securing a global workforce, meeting regulatory mandates, and reducing cyber-insurance costs—without ripping and replacing your existing IT stack.

To address both gaps and challenges, organizations must adopt a secure perimeter approach around their cloud workspaces—Mindcore Technologies' purpose-built data enclaves delivered as part of a unified cybersecurity platform safeguards data, enforces regulatory compliance, and reduces operational risk, while also eliminating overhead and unnecessary costs.

By implementing the strategies outlined in this paper and leveraging Mindcore Technologies' integrated platform, enterprises can establish a resilient, compliant, and secure environment for remote and hybrid work, protecting their data, operations, and reputation from ever-evolving threats.

[2] The Verizon 2023 Data Breach Investigations Report

APPENDIX

Key Features of Mindcore's Data Enclave Platform

Comprehensive, Multi-Layered Security Architecture

Mindcore's data enclave platform provides a robust security framework that isolates, protects, and governs sensitive data and workflows. By integrating advanced security protocols, zero-trust principles, and flexible deployment options, it enables secure collaboration, confident innovation, and scalable operations, reducing risk while ensuring compliance in complex digital environments.

Isolation and Segmentation

Mindcore's secure data enclaves are logically or physically separated within the cloud, ensuring sensitive data remains protected and isolated from other workloads to prevent unauthorized access and data leakages.

Access Control and Advanced Security

Security is enforced through multi-factor authentication, role-based access controls, identity and risk management, and encryption (at rest and in transit). Enclaves also support intrusion detection, exploit defense, workload protection, network security, client isolation and protection, anomaly monitoring, and audit logging to maintain data confidentiality and integrity.

Governance is delivered through activity monitoring (post multi-factor authentication, role-based permissions, conditional access controls, and identity management) which ensures access control for only authorized users who need to interact with enclave resources.

Advanced Security Measures

Mindcore's enclaves incorporate encryption (at rest and in transit), intrusion detection, anomaly monitoring, and audit logging to safeguard data integrity and confidentiality.

Controlled Data Movement

Data transfers into and out of enclaves are tightly monitored and restricted, with approvals or security checks required to prevent unauthorized exfiltration.

Auditability And Monitoring

The platform continuously logs user activity to support compliance, enable rapid threat detection, and provide full visual and contextual audit trails for governance and reporting.

Regulatory Compliance

Enclaves are ISO 27001 and SOC 2 II compliant, and designed to meet regulations and standards such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Risk and Authorization Management Program (FedRAMP), ensuring lawful, secure data handling across industries.

Granular Permissions And Policy Enforcement

Precise access and policy controls ensure users only access the data, applications, and environments they are explicitly authorized to use—minimizing the attack surface and enforcing the principle of least privilege.

Cloud Ecosystems Integration

Seamless integration with identity and security tools such as Azure Entra ID, SAML, SCIM, and OAuth — supporting centralized access control and workflow automation. The enclave's private network can negotiate secure connections to any enterprise network irrespective of their deployment and configuration models, whether cloud native, on-premise, or hybrid firewalls and connection gateways.

Secure Workflow Enablement

Enclaves support secure operations for high-risk workflows, including:

- AI model training and inference
- Sensitive data analytics
- Confidential development and testing environments

These workflows remain fully auditable and compliant, without compromising performance or slowing down end-user productivity.

Flexible Environments

Enclaves can be rapidly deployed as either temporary or persistent environments. They are also capable of scaling based on the enterprise requirements. This adaptability supports both project-specific use cases and long-term operational needs, accelerating time to value while reducing administrative overhead. Onboarding and offboarding global teams with high standards of care and security in just minutes.