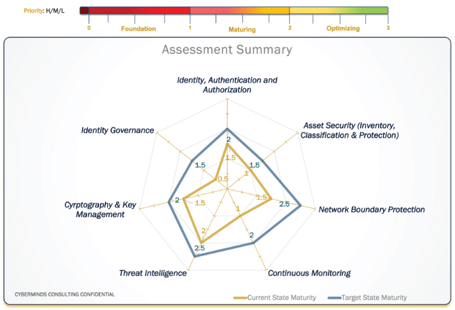
Zero Trust Readiness Assessment Services Brief

Hybrid work model touches all aspects of business; from HR policies & procedures to office layouts to technology needs including Cybersecurity. As organizations ramp up their goals to adopt Hybrid Work Models, it has become increasingly apparent that traditional approaches to security are no longer sustainable.



1. Adversaries have found ways to exploit a greater number of weakly protected back doors into corporate systems. This includes the undetected loopholes in existing remote work technologies.
2. Not all workloads today reside within guarded corporate data centers. Cloud adoption has moved critical applications & data outside corporate boundaries.
3. The stress and distraction that come with homebound work can make employees more vulnerable to sophisticated "social engineering" cyberattacks. The volume of successful attacks that result from human error is only expected to rise.

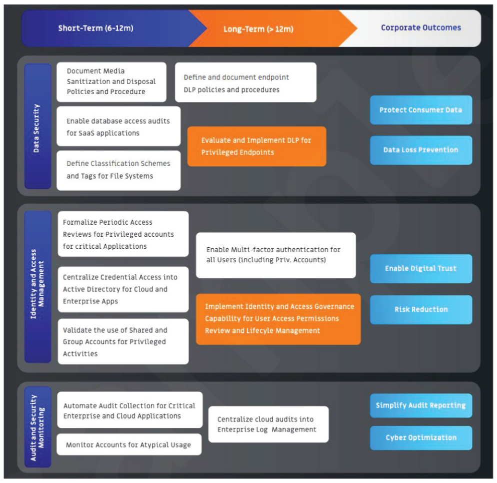
To take on the new cybersecurity challenges of virtual working environment, companies must understand the changes in their cyber risk profile and revamp their strategies to adopt emerging concepts centered around **Zero-Trust**. Otherwise, the current better-than-expected outcome of the rapid shift to "work from home" may not find success in the longer term.

Least privileged access, limits to user access with just-in-time/just-enough-access, and risk-based adaptive polices, are becoming crucial defenses in enabling virtual work environments. Companies must verify explicitly, always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

The journey to securing Hybrid Workplace requires a progressive approach. CyberMinds Consulting's Zero-Trust Security Readiness Assessment is a No-Fee, virtual, half-day technical workshop to enable companies assess their current maturity and readiness to adopt Zero/No-Trust concepts and principles that are foundational to securing Hybrid Work Environments.

Our assessment includes

1. Cyber Risk Analysis across seven domains: Identity, Authentication and Authorization - Network Boundary Protection - Asset Security - Cryptography - Identity governance - Continuous monitoring - Threat Detection and Response (No Fee) .
2. Risk Assessment Report (No Fee).
3. Detailed Cyber Roadmap with technology insights & recommendations (Fixed fee add-on) .



Short-Term (6-12m)
Long-Term (> 12m)
Corporate Outcomes

Data Security
Document Media Sanitization and Disposal Policies and Procedure
Enable database access audits for SaaS applications
Define Classification Schemes and Tags for File Systems
Define and document endpoint DLP policies and procedures
Evaluate and Implement DLP for Privileged Endpoints
Protect Consumer Data
Data Loss Prevention

Identity and Access Management
Formalize Periodic Access Reviews for Privileged accounts for critical Applications
Centralize Credential Access into Active Directory for Cloud and Enterprise Apps
Validate the use of Shared and Group Accounts for Privileged Activities
Enable Multi-factor authentication for all Users (including Priv. Accounts)
Implement Identity and Access Governance Capability for User Access Permissions Review and Lifecyle Management
Enable Digital Trust
Risk Reduction

Audit and Security Monitoring
Automate Audit Collection for Critical Enterprise and Cloud Applications
Monitor Accounts for Atypical Usage
Centralize cloud audits into Enterprise Log Management
Simplify Audit Reporting
Cyber Optimization

Benefits of our approach

1. Provides visibility into the current state capabilities and potential improvement areas.
2. Streamlines the conversation for Cyber Investments around prioritized domains.
3. Enables a time-based progressive approach to implementation of Zero-Trust initiatives keeping the organizational requirements & constraints in mind.

✉ contact@cybermindssolutions.com

☎ (855) 945-1970

https://www.cybermindssolutions.com/