Tech Mahindra

ESRM

Enterprise Security & Risk Management

RESPONDING TO UNPRECEDENTED DISRUPTION

For Energy and Utility (E&U) companies that usually have concrete contingency plans in place to offset the impact of natural disasters, the COVID-19 outbreak poses an altogether different challenge. Facing the adverse impact on demand and reduced revenues on one hand, the Sudden Surge in Work-from-Home Users without adequate Security Controls on end points & lack of security awareness has led, enterprise information, and assets vulnerable to Cyber-Attacks such as Email Phishing & Ransomware

The impact of a security breach goes beyond operational concerns, and can have a devastating impact on the financial well-being of a company. Some of the growing concerns of Energy & Utilities organizations continue to be:

- Transformation of The Traditional Network Architecture
- Network Security Vulnerabilities
- Patch Management challenges
- Compliance Management challenges
- Legacy supervisory control and data acquisition (SCADA) systems
- Managing a diverse set of vendor products that generate large amounts of status and threat information
- Incorporating security into service delivery applications that were developed without security as a consideration

The immediate response of most Energy & Utility companies is to ensure the safety of its workforce and continuity of operations for which business leaders must make rapid decisions, and take immediate actions, to protect and support their workers while ensuring that critical business operations continue in a safe and secure fashion.

Tech Mahindra is committed to help Organizations develop a more sustainable and cost-effective approach to adapt risk and security measures and develop resilience to respond to risk and threats. In other word, we help you to become a RISK AWARE Organization.

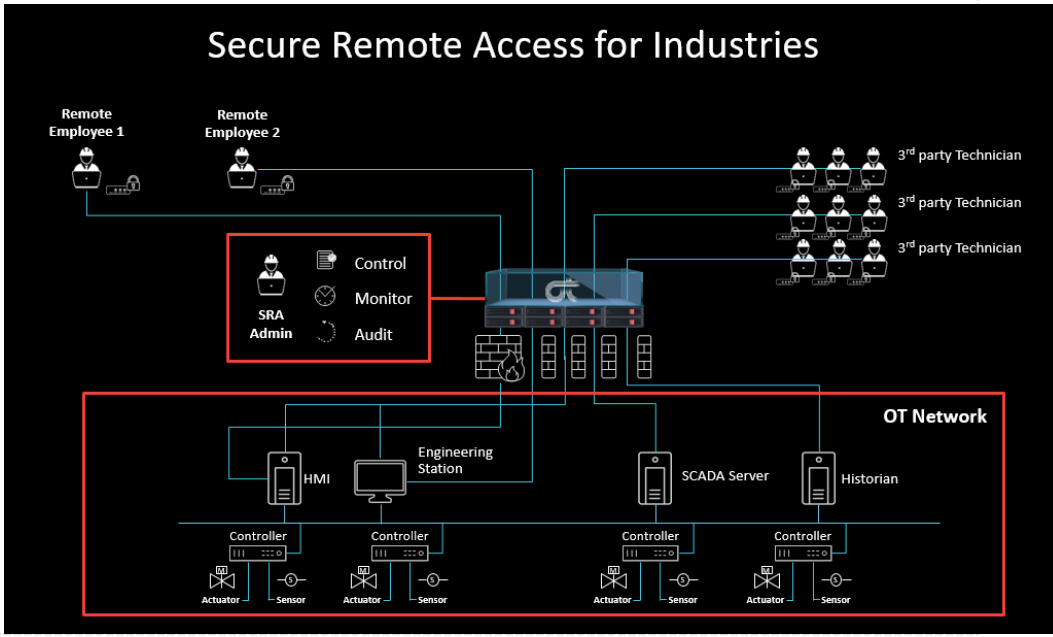
Secure Remote Access For Industries

SCADA (Supervisory control and data acquisition) is widely applied in the generation, transmission & distribution sectors of electricity, Water, Waste Water & Sewerage. SCADA vendors such as Siemens, ABB require to push signatures/patches remotely.

With Covid-19 forcing employees to work from home, even employees of SCADA vendors are mandated to work from home. This is posing serious security threat into the production network of these companies. Hence there is an immediate requirement for these companies to establish a secured remote access into SCADA network

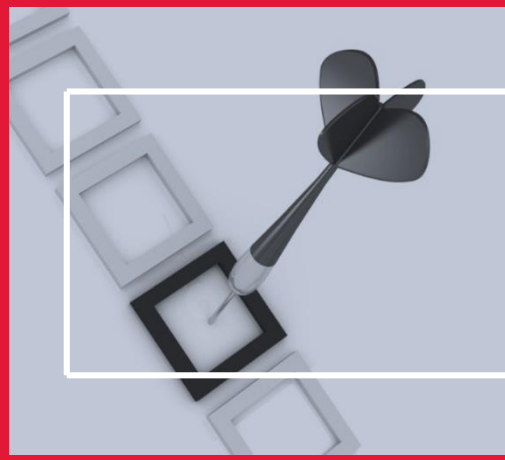
Tech Mahindra's Secure Remote Access can augment safe and secure patches update and also provides control/ monitor and audit capabilities through a remote admin

We can control, monitor and audit critical updates such as daily patches, version upgrade or routine maintenance in a secure manner.



VALUE PROPOSITION

- Choice of solutions – Cisco & US-Dept of Defence approved partner
- Can enhance WaaS to address US-Cert specifications
- Simple and focused solution which addresses access management issues during COVID



Secure Remote Access Solution

Tech Mahindra's Secure Remote Access solution is aimed to help you secure your Business with Remote Work From Home Users by defending the enterprise against Cyber-Attacks, Email Phishing & Cyber Frauds. Ideal for organizations facing sudden surge of remote users with no maximum cap and Looking for pure-play Secure WFH solution & fixed budgets

SOLUTION

Fast & remotely deployable, cost-effective, scalable & trustworthy VPN solution with CISCO Tech/DoD approved available options. Unique cloaking capability against attacks.

SOLUTION KEY TENETS

- Cloud-based & Light-weight solution
- Push deployable within 4-7 days
- Scalable and flexible to handle surge in user volume
- Leverages existing setup
- Trusted partner – Cisco
- Cost-effective @ $xx/user/month
- Compliant with US-CERT released advisories
- https://www/us-cert.gov/ncas/alerts

Email Security-as-a-Service (Anti-Phishing)

Lots of remote workers such as Customer service representatives or call center personnel traditionally working from office, not having enough understanding of cyber security threats and security controls makes enterprise messaging & business applications vulnerable to email, phishing threats and even DDOS considering the scale of remote user access

Almost all industries today use collaboration platforms where email supersedes all available options – conferencing, chat, messaging, sharing of information / assets – need a powerful email security – either on-prem or cloud based or hybrid

Tech Mahindra's Email Security as-a-Service solution provides continuous Monitoring and Detection of Phishing & SPAM attacks, Threat Detection, Reporting, Remediation & forensics - workflow orchestration, Sand-Boxing, AI based Automated detection & Remediation within minutes

VALUE PROPOSITION

- Fully automated Email Phishing Prevention during COVID crisis
- Addresses the surge of phishing emails which traditional systems are unable to handle

SOLUTION KEY TENETS

- Mailbox anomaly detection basis contextual & use behavioral analysis
- Detection of targeted phishing mails and remediation and reporting
- Anti-Malware, Anti-SPAM controls equipped with sand-boxing for non-signature based attacks on mail / exchange servers

SOLUTION KEY TENETS

- Protection of confidential and business critical information from being compromised in the hands of hackers or malicious users (intentionally or due to negligence)
- Zero Minute detection and remediation of polymorphic account compromises
- Cost-effective @ $xx/Mailbox/Month
- Compliant with US-CERT released advisories

https://www/us-cert.gov/ncas/alerts

Pseudonymization & Anonymization as a Service

Data privacy regulators have called for stronger security safeguards on PII (Personally Identifiable Information) processing due to employee WFH. Public health authorities may demand PII or non identifiable data from any company which will have to honoured. However potential lack of resources trained on privacy compliance may end up raising non-compliance risk & risk of penalties and fines

Tech Mahindra's Pseudonymisation & Anonymisation as-a-service solution helps company that may need to provide certain PII to public health authorities (so practically every company that processes PII)

SOLUTION KEY TENETS

Pseudonymisation (temporary conversion of personal data to non-personal data) and anonymization (similar feature, but permanent conversion) help protect PII and comply with data privacy regulations

VALUE PROPOSITION

- Addresses the challenge of PII Privacy Violations in the COVID crisis
- Available Remote managed service when skills manpower onsite is unavailable

SOLUTION KEY TENETS

- This solution can be implemented with large portion of remote work
- Tech Mahindra will provide necessary consultancy from offshore
- Local deployment supported in the US, UK and APAC
- Available in both SaaS and On-Prem or Hybrid delivery model
- Support privacy compliances such as

GDPR
CCPA
HIPAA

Continuous Compliance Assurance-as-a-Service

Almost all industries need a assurance on their security controls & compliance to standards and regulatory guidelines for protection of mission critical application infrastructure supporting business operations and customer delivery channels

Tech Mahindra's Continuous Compliance assurance-as-a-Service solution provides

- Complex & dynamically changing IT and IT GRC controls
- Heavy dependency on SMEs specific to OEM technologies & platforms to retain compliance – leading to uncontrolled configuration of parameters
- % of Cyber Attacks are due to Misconfiguration & Poor Auditing & lack of real-time assessment of IT Recourses

SOLUTION KEY TENETS

Auto Discovery, Continuous Automation, monitoring, validation, Remediation, Single Pane view & Reporting of Misconfigured IT Resources

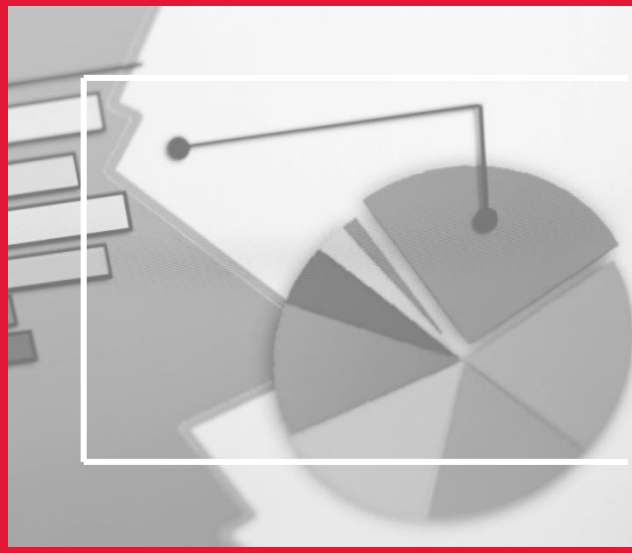
VALUE PROPOSITION

- Short implementation timeline. Can be deployed almost immediately.
- Addresses the immediate needs during COVID to ensure compliance & IT Security controls mis-configurations

SOLUTION FEATURES

- A platform that can be fully customizable & deployed within few days
- Agentless deployment and minimal or almost no onsite involvement
- Available in both SaaS and On-Prem or Hybrid delivery model
- Very broad single pane view of compliances and remediation controls
- Cost-effective @ $xx/Object/Month
- Compliant with US-CERT released advisories

https://www/us-cert.gov/ncas/alerts



AI Based Cyber Defense Platform

Utilities that have extended WFH for remote workers need protection of enterprise mission critical application environment.

Tech Mahindra's Artificial Intelligence based Cyber Defence Platform prevent

- Continuum of attack surface expanded to WFH – Remote Workers
- Inadequate threat monitoring to address the heightened scale of incidents
- New users and partially compliant end points leading to risk exposure

SOLUTION FEATURES

- Cloud-based & Light-weight solution
- Push deployable within 4-7 days
- Scalable and flexible to handle surge in user volume
- Leverages existing setup
- Proven AI Cyber Defence Platform
- Cost-effective @ $xx/EPS/month or $xx/GB/Month or $xx/User/Month
- Compliant with US-CERT released advisories

https://www/us-cert.gov/ncas/alerts

SOLUTION KEY TENETS

- Cloud Based AI-SOC Integration for Remote Security Incident Monitoring & Response
- Integrated and Continuous End-Point Threat Detection & Response

VALUE PROPOSITION

- Automated threat detection and response resulting in minimum human intervention
- Addressing shortage of SOC Analysts during COVID crisis, leveraging AI

Tech Mahindra

www.techmahindra.com
connect@techmahindra.com
www.youtube.com/user/techmahindra09
www.facebook.com/techmahindra
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra

About Tech Mahindra:

Tech Mahindra represents the connected world, offering innovative and customer-centric information technology experiences, enabling Enterprises, Associates and the Society to Rise™. We are a USD 4.9 billion company with 130+K professionals across 90 countries, helping 964 global customers including Fortune 500 companies. Our convergent, digital, design experiences, innovation platforms and reusable assets connect across a number of technologies to deliver tangible business value and experiences to our stakeholders. Tech Mahindra is the highest ranked Non-U.S. company in the Forbes Global Digital 100 list (2018) and in the Forbes Fab 50 companies in Asia (2018).

The Mahindra Group is a USD 21 billion federation of companies that enables people to rise through innovative mobility solutions, driving rural prosperity, enhancing urban living, nurturing new businesses and fostering communities. It enjoys a leadership position in utility vehicles, information technology, financial services and vacation ownership in India and is the world's largest tractor company, by volume. It also enjoys a strong presence in agribusiness, aerospace, commercial vehicles, components, defense, logistics, real estate, renewable energy, speedboats and steel, amongst other businesses. Headquartered in India, Mahindra employs over 2,40,000 people across 100 countries.