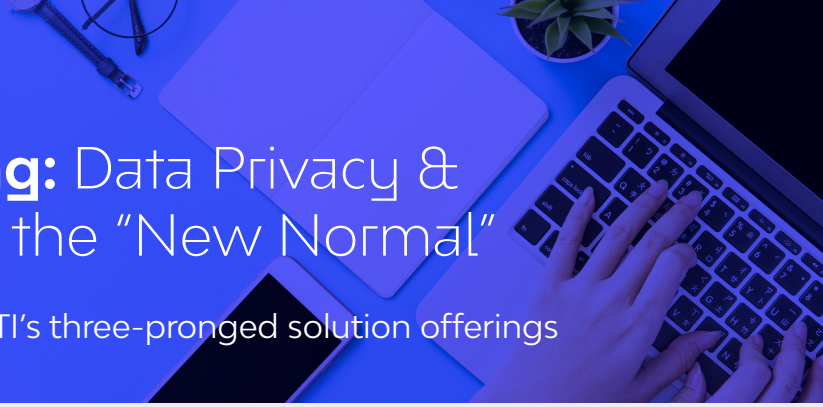
LTI
Let's Solve

Remote Working: Data Privacy & Asset Security in the "New Normal"

Maintain system integrity with LTI's three-pronged solution offerings



Powered by: Microsoft CloudSEK SecurityAdvisor SECURONIX

Global enterprises are adopting secure and effective remote working strategies today, making this a "New Normal." However, there are rising concerns around data privacy and information security as remote working could propel the use of unsecure devices and wireless networks, enabling access to applications from outside the corporate network. Also, due to inconsistent behavioural attributes raising the possibility of exploitation, system integrity could get compromised, resulting in sensitive data leakage.

Threat Advisory and Monitoring

- Secure access and secure devices
- Security management across platforms and applications
- Information protection for control over content sharing
- Threat protection for data residing in apps and cloud

To maintain system integrity and prevent data breach, LTI has created a set of simple yet curated offerings that will provide free advisory service, extra security for collaboration tools and ensure data & asset safety. Here's a quick snapshot of our solutions and their benefits:

Free Advisory Service

Powered by CloudSEK XVigil, this free-of-cost service for the next two months (April-May 2020) provides real-time visibility of actionable threat intelligence to help clients understand their real threat position, with specific focus on exposed vulnerabilities. With the help of this service, you can plan steps to remediate these vulnerabilities and mitigate risk. LTI will provide weekly personalized threat intelligence reports to the customer.

Secure Access & Device Protection

In order to enhance security, LTI recommends Multifactor Authentication **(MFA)** to enterprise resources like applications or virtual desktops even if credential-based access control is enabled. The second step is to protect the devices that connect to the corporate network with Endpoint Detection & Response **(EDR)** and Intrusion Prevention & Firewall (IPS) protection included.

Once the access to a corporate device is secured, information held within the corporate network needs protection as well. Threats from phishing campaigns and spear phishing attacks are real and can vastly compromise corporate networks and data. This is where we suggest the third step of email security with Data Loss Prevention (DLP) enabled to ensure sensitive data is not compromised.

Managing Collaboration Platforms

Collaboration tools like Teams, Zoom, Webex, etc. could be avenues for data compromise. AI-enabled Information Protection through data classification and Information Rights Management **(IRM)** helps plug these gaps. Also, when users need to access applications that are internal, adequate security may not have been enabled, in such instances, **Web App Security** – RAVPN, DDoS & WAF, and CASB become necessary. In addition, sensitive data needs to be secured by techniques such as encryption and tokenization to enable more complete security coverage.

Security Monitoring & Management

In order to enable a more comprehensive view to security, some additional measures should be adopted, such as:

- Monitoring workloads and setting up a comprehensive security monitoring **(SIEM)** program
- Advanced Threat Detection through use of **UEBA** (integrated with EDR), is required to ensure a cyber defense resilient enterprise

User Awareness Training for Remote users

Most security incidents have a human root cause. In most organizations, 20% of users account for 80% of malware detections. The only way to bring down the number of security incidents attributable to humans is through persistent awareness campaigns delivered in an automated and measurable manner. LTI is offering FREE automated remote user security awareness services for 2 months (Apr & May, 2020) that coaches users in real time with bite sized modules to change their behaviour.

Solution Stack

Solution Stack (one time set-up)	**Upto 2500 users**	**Upto 5000 users**	**Upto 10000 users**	**Comments**
Threat Intelligence Advisory from CloudSEK XVigil	2 weeks	4 weeks	6 weeks	-
EDR - Windows Defender ATP				-
MFA - Azure AD				-
Email - O365 EOP+ATP				-
Info Protection - AIP P2				-
VPN - Azure VPN (ExpressRoute)				-
DDoS + WAF - Azure Front Door				-
Encryption - Azure Key Vault				-
SIEM + UEBA - Securonix				Annual subscription required

1 Free Advisory Service is available 7 days after sign up

2 LTI will take 2 days to assess requirements and mobilize resources to begin set up

3 Availability of Microsoft Azure M365 E5 subscription is assumed

4 All non-Microsoft solutions will be provided by LTI as services

5 Any other services required may be separately contracted with LTI

6 Validity of this limited time offer is at the discretion of LTI

7 All services are provided by LTI shared security services

For more information on this offering, please email us on **info@lntinfotech.com**.

LTI (NSE: LTI, BSE: 540005) is a global technology consulting and digital solutions Company helping more than 420 clients succeed in a converging world. With operations in 32 countries, we go the extra mile for our clients and accelerate their digital transformation with LTI's Mosaic platform enabling their mobile, social, analytics, IoT and cloud journeys. Founded in 1997 as a subsidiary of Larsen & Toubro Limited, our unique heritage gives us unrivaled real-world expertise to solve the most complex challenges of enterprises across all industries. Each day, our team of more than 30,000 LTItes enable our clients to improve the effectiveness of their business and technology operations, and deliver value to their customers, employees and shareholders. Find more at www.Lntinfotech.com or follow us at @LTI_Global