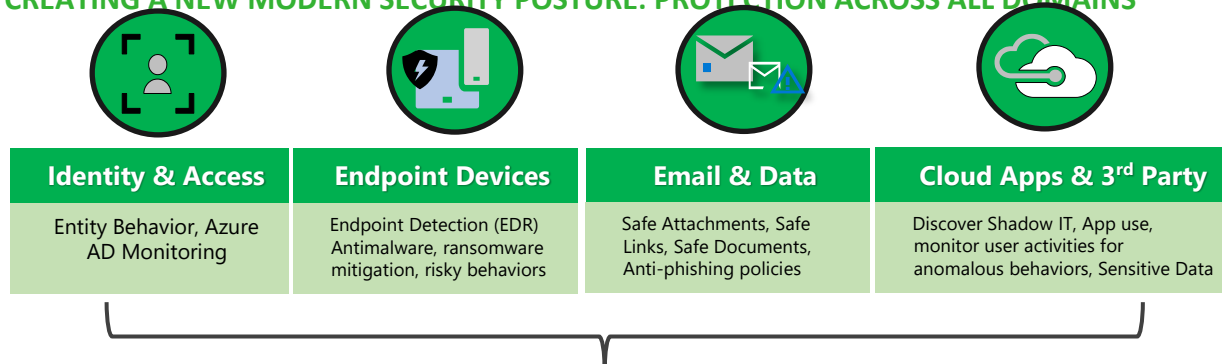## MXDR SHIELD SECURITY SOLUTION

MXDR Shield is a unique offering leveraging **Microsoft's Sentinel SIEM & XDR** technology combined with **Long View's 24x7 Security Operations Center (SOC)** to secure your Microsoft cloud ecosystem (Microsoft Office365, OneDrive, Teams, Azure, Microsoft 365 Defender, Dynamics 365). Our unique configuration provides end-to-end threat visibility across all your resources; correlated, prioritized alerts based on the deep understanding Microsoft has of specific resources and AI that stitches that signal together altogether with coordinated alert action across the organization. We enable quick deployment without costly infrastructure setup and maintenance, along with limitless scale to meet your security needs and ongoing business growth.

MXDR SHIELD DEPLOYMENT

Expert Sentinel configuration and 24x7 monitoring. Our SOC experts will professionally setup Sentinel into your Azure workspace including deployment of our proven expert rulesets and automated playbooks that will automatically respond to threats and other suspicious activities including workstation or user quarantine in near real-time. Your company's system administrators will be notified while our 24x7 SOC triages to provide you the best course of action for remediation, so you're never surprised or off-guard. Automation can be leveraged to trigger playbooks developed by Long View to quarantine workstations (endpoints) or suspend user access during malicious behavior. Other threats may require triage by Long View's skilled SOC team. This is all achieved with a second instance of Sentinel located in Long View's SOC which is linked and synchronized to the client's workspace to investigate and respond as required.

CREATING A NEW MODERN SECURITY POSTURE: PROTECTION ACROSS ALL DOMAINS

Identity & Access	Endpoint Devices	Email & Data	Cloud Apps & 3rd Party
Entity Behavior, Azure AD Monitoring	Endpoint Detection (EDR) Antimalware, ransomware mitigation, risky behaviors	Safe Attachments, Safe Links, Safe Documents, Anti-phishing policies	Discover Shadow IT, App use, monitor user activities for anomalous behaviors, Sensitive Data

Shift from individual silos to coordinated cross-domain security

MXDR Shield is designed to protect your modern workplace, the real power comes behind a fully integrated solution that coordinates **detection, prevention, investigation, and response, across identities, endpoints, email, Cloud applications, and 3rd-party connectors** including security appliances & firewalls such as Cisco Umbrella & Meraki, Palo Alto Panorama to provide integrated protection against sophisticated attacks thought the entire kill chain. With the ability to utilize threat intelligence feeds from various sources, the machine learning and intelligence provided by Sentinel can help to reduce the false positives and the ability to respond quickly to attacks.

FAST RETURN ON BUSINESS VALUE

Cloud Protection – Protection against know threats and Zero-day attacks, targeted phishing, ransomware & Viruses, utilizing Microsoft Sentinel platform with advanced AI & Machine learning to eliminate false positives.

Monitoring – Fully integrated 24x7 SOC with eyes on glass watching for anomalies, ready to triage or consult as necessary.

Detection- Sentinel detects threats faster and allows for deep investigation from its integrated approach - allows us to gain access to the kill chain in the event of a breach occurring, who has been breached, what data has been compromised.

Response – Response support from an attack through Long View's Security Escalation Document (SED) is setup with the client- a documented procedure for what to do when something is going terribly wrong, who should be notified and what are next steps.

For more information on **MXDR Shield** or our **Digital Defence portfolio**, please contact your account manager or directly at
engage@lvs1.com

longviewsystems.com