Long View | Digital Defence

www.longviewsystems.com

SECURING THE MICROSOFT CLOUD

USER SHIELD

USER SHIELD MANAGED SECURITY SOLUTION

User Shield is a unique offering leveraging **Microsoft's Azure Sentinel SIEM & XDR** technology combined with **Long View's 24x7 Security Operations Center (SOC)** to secure your Microsoft cloud ecosystem (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.

USER 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

User 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.

Shift from individual silos to coordinated cross-domain security

IDENTITY & ACCESS
Entity Behavior, Azure AD Monitoring

ENDPOINT DEVICES
Endpoint Detection (EDR)
Antimalware, ransomware mitigation, risky behaviors

EMAIL & DATA DEVICES
Safe Attachments, Safe Links, Safe Documents, Anti-phishing policies

CLOUD APPS & 3RD PARTY
Discover Shadow IT, App use, monitor user activities for anomalous behaviors, Sensitive Data

Microsoft Gold Partner

Microsoft Partner of the Year 2019 Winner

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 Incidence Response Plan (SIRP) 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.

USER SHIELD OPTIONS, FEATURES & REQUIREMENTS

PRODUCT FEATURES:	ESSENTIAL USER SHIELD	ENABLED USER SHIELD
INCLUDED SECURITY COVERAGE:		

INCLUDES- 24x7 SOC CLOUD SECURITY MONITORING OF;
- Azure Active Directory logs and sign-ins
- Office 365 logging
- Threat Intelligence Indicators

ALSO INCLUDES-
- Microsoft Sentinel Rules & Playbooks
- 24x7 investigation and triage of alerts
- Custom Security Incidence Response Plan (SIRP)
  Note: Does not monitor any Microsoft Defender Products

INCLUDES- Essentials PLUS;
Microsoft Defender Threat Protection monitoring which can include all or any of the below; **(licensing required for each)**
- Defender for Identity (Identity and access)
- Defender for Endpoint (Endpoint device protection)
- Defender for Office 365 P2 (Email protection)*
- Defender for Cloud Apps (formerly MCAS)
- Azure AD Identity Protection (Azure AD P2)
- Defender for Business (Under 300 Users)
- Defender for Cloud (formerly- Azure Security Center & Azure Defender)**

**Priced per Server, (VM, SQL, SaaS, Multi-Cloud using Azure Arc) or Security workload type

MINIMAL LICENCING REQUIREMENTS	
• Office 365 with adding Azure AD P1 • OR M365 E(x) (includes Azure Active Directory P1) • M365 Business Premium includes Azure AD P1) • **An available Azure Subscription is required to deploy Azure Sentinel and Log Analytics workspace**	• Office 365 with adding AD P1 • OR M365 E(x) (includes Azure Active Directory P1) • M365 Business Premium includes Azure AD P1 • ONE or more of the above Microsoft Defender Products • Defender for Office 365 requires Plan 2

PCI DSS COMPLIANT · bsi. ISO/IEC 27001 Information Security Management IS 670324 · AICPA SOC · AICPA SOC

Contact us today. engage@lvs1.com