Reference Card for Manufacturing

SOPHOS

Manufacturing organizations are witnessing the Industry 4.0 era. Smart factories equipped with industrial IoT devices, robotics, and advanced analytics are revolutionizing manufacturing operations, leading to cost savings, improved efficiencies, and operational ease. However, legacy manufacturing technologies, rapid digitization, IT/OT convergence, and the sector's vast and complex supply chain network are increasing the sector's attack surface.

Sophos dramatically reduces the threat response time of manufacturing organizations with its next-gen services and products, allowing organizations to consolidate their security management with a single vendor. This document provides a general reference on how Sophos solutions help manufacturing organizations meet their cybersecurity requirements for uninterrupted operations.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing access to critical industrial control systems	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
Protecting intellectual property (IP) from theft	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Intercept X	Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across your endpoint devices. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.
	Sophos Firewall	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across the extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection safeguards your users and devices from malicious content and apps.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Email	Allows the creation of multi-rule DLP policies for users to ensure the protection of sensitive information with the discovery of confidential contents in all emails and attachments. It also seamlessly encrypts your sensitive data to stop breaches.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Insider Threat Protection	Sophos Firewall	Protects your sensitive data from accidental or malicious disclosure with complete policy control over web categories, applications, removable media, and mobile devices used in your network. Offers insights into your riskiest users and applications to ensure that your policies are enforced before your security is compromised with actionable intelligence from Sophos User Threat Quotient (UTQ). Offers the most extensive set of user authentication options available on any firewall, including Active Directory integration, and even our unique and easy-to-use Synchronized User ID solution that facilitates seamless user authentication across the firewall and endpoints to offer tighter, granular user access, blocking an external attacker as well as a malicious insider from gaining access to sensitive systems or data.
	Sophos Cloud Optix	Connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real-time that can help you identify credential misuse or theft. An IAM visualization tool that provides a complete map of IAM relationships allows your IT teams to identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks quickly and easily.
Minimizing attack surface to ensure uninterrupted manufacturing operations	Sophos Firewall	Comes with built-in web, email and zero-day protection to keep advanced malware threats at bay, preventing breach attempts from zero-day malware, APT or a ransomware attack.
	Sophos XDR	Pulls in rich network, email, and other data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence, and human expertise to identify impact and response.
Protecting against phishing attacks	Sophos Email	Scans all inbound messages for key phishing indicators such as brand spoofing and impersonation attempts in real-time using SPF, DKIM, and DMARC authentication techniques and email header anomaly analysis. This helps to spot and block phishing emails before they reach your users.
	Sophos Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
	Sophos Intercept X	Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – multiple layers of protection technologies including credential theft protection, exploit protection, anti-ransomware protection, and tamper protection, that optimize your defenses.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Preventing advanced malware and threats	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
Reducing third-party vendor risks	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
	Sophos Intercept X Advanced with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing the distributed manufacturing enterprise	Sophos Secure Access portfolio	Includes Sophos ZTNA to support secure access to applications, Sophos SD-RED remote Ethernet devices to safely extend your network to branch offices and remote devices, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch for secure access on the LAN. Everything is managed through a single cloud-based security platform – Sophos Central.
	Sophos Cloud Optix	Sophos's cloud security posture management solution, Sophos Cloud Optix, enables teams to proactively improve security posture, detecting insecure configurations and vulnerabilities. By automatically mapping security and compliance standards to your environments, Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
Securing resources in the cloud	Sophos Cloud Native Security	Provides complete multi-cloud security coverage across environments, workloads, and identities. It protects your cloud infrastructure and data with flexible host and container workload security for Windows and Linux. Multi-layered technologies protect against ransomware and other advanced attacks including cloud-native behavioral and exploit runtime detections that identify threats such as container escapes, kernel exploits, and privilege-escalation attempts.
Securing legacy manufacturing systems	Sophos Firewall Sophos SD-RED	Put Sophos SD-RED in front of an exposed device, and it will tunnel traffic to a protective Sophos Firewall for scanning. If your network is flat, you will likely need to make changes to IP address schemes and possible switch topology – our technical specialists can discuss your situation and show you how to do this.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK