SOPHOS

Cybersecurity Guide for the Manufacturing Industry

Sophos' expert threat analysts and world-leading threat intelligence help you to identify and respond to advanced threats faster, 24/7.

Industry 4.0 and "smart factories" are transforming the manufacturing industry. Industrial Control Systems (ICS) like SCADA, Industrial IoT (IIoT) devices, robotics, and advanced analytics are revolutionizing the way factories operate today. But extensive digital transformation, IT/OT convergence, and the sector's extremely low tolerance for operational downtime are expanding the attack surface, increasing manufacturers' risks of vulnerability exploitation, data spillage, production sabotage, etc.

Sophos secures manufacturing organizations against a wide range of cyberattacks, including human-led threats that technology alone cannot prevent. From managed detection and response (MDR) to endpoint and network security, Sophos enables manufacturers to optimize their defenses and frees IT teams to focus on the business.

A Sophos Whitepaper. April 2023

Cybersecurity Challenges in Manufacturing

The cybersecurity challenges for the manufacturing sector continue to grow because of rapid digitalization and lack of equally sophisticated cybersecurity standards, which has left IT and OT leaders unprepared to respond to new cyber threats. Besides this, cyber threats in this sector continue to grow in both volume and complexity.

A 2022 Sophos survey of 419 IT professionals working in the manufacturing and production sector revealed that 55% of organizations were hit by ransomware in 2021 – a 52% increase in the rate of ransomware attacks over the previous year.

The average cost to remediate a ransomware attack was US$1.23M for manufacturers. Furthermore, a significant 77% of respondents said the attack impacted their ability to operate, while 71% said it caused them to lose business/ revenue.

It's not just ransomware. The overall IT environment in manufacturing has become even more challenging: over the year, 61% of organizations reported an increase in attack volume, 66% reported an increase in attack complexity, and 51% reported an increase in the impact of attacks.

55%
of manufacturing organizations hit with ransomware in 2021

$1.23M
average cost to remediate following an attack

>1 Month
10% of manufacturing organizations took over a month to recover following an attack

77%
of manufacturing organizations hit by ransomware said it impacted their ability to operate

66%
of IT pros in manufacturing sector observed an increase in the complexity of attacks

59%
data recovered by manufacturing organizations after paying the ransom

57%
of attacks on manufacturing resulted in data being encrypted

7%
of manufacturing organizations recovered ALL data after paying the ransom

Source: Sophos' global survey on The State of Ransomware 2022

Behind these statistics are several changes in the threat landscape:

The professionalization of cybercrime

One of the most significant developments over the last year has been the development and professionalization of the cyber threat economy. Criminal groups increasingly specialize in a particular component of an attack, for example, initial access, ransomware, information-stealing malware, and more, and offer it as a service to other criminals. These 'as-a-service' models lower the skill threshold required to conduct an attack, increasing the volume of adversaries and threats.

These specialist services provide execution guidance and resources for their criminal customers, enhancing the effectiveness of the attacks. Illustrating this point, in March 2022, an associate of the Conti ransomware-as-a-service group published an archive that included a rich trove of documentation and guidance designed to instruct an "affiliate" attacker in the steps required to conduct a ransomware attack.

Attackers are also adopting many of the behaviors of legitimate IT service providers, including asking ransomware victims to 'rate their service' once they have decrypted the files post-payment.

The evolution of attacker tactics, techniques, and procedures

Adversaries frequently exploit weaknesses in organizations' security posture in an attempt to avoid being stopped by security solutions. These include:

- **Exploiting unpatched vulnerabilities** – This was the number one method adversaries used to penetrate organizations in attacks that Sophos' incident responders were brought in to remediate last year, used in 47% of incidents.
- **Exploiting legitimate IT tools** – Many of the top tools used by IT professionals are also abused by adversaries, including PowerShell, PsExec, and PowerShell, to exploit stolen access data and credentials. By posing as legitimate users, attackers hope to trick their way into an environment.

The cybersecurity challenges for this sector don't end here. Manufacturing organizations also need to contend with insider threats (both malicious and accidental), strict regulatory compliance requirements, and third-party vendor risks, amongst other challenges.

Sophos Security for the Manufacturing Sector

Sophos delivers advanced cybersecurity solutions that enable manufacturing organizations to manage and reduce cyber risk. Our adaptive cybersecurity ecosystem provides a full portfolio of market-leading services and products that elevate our customers' defenses against even the most advanced threats, all powered by the unparalleled threat, AI, and security operations expertise of Sophos X-Ops.

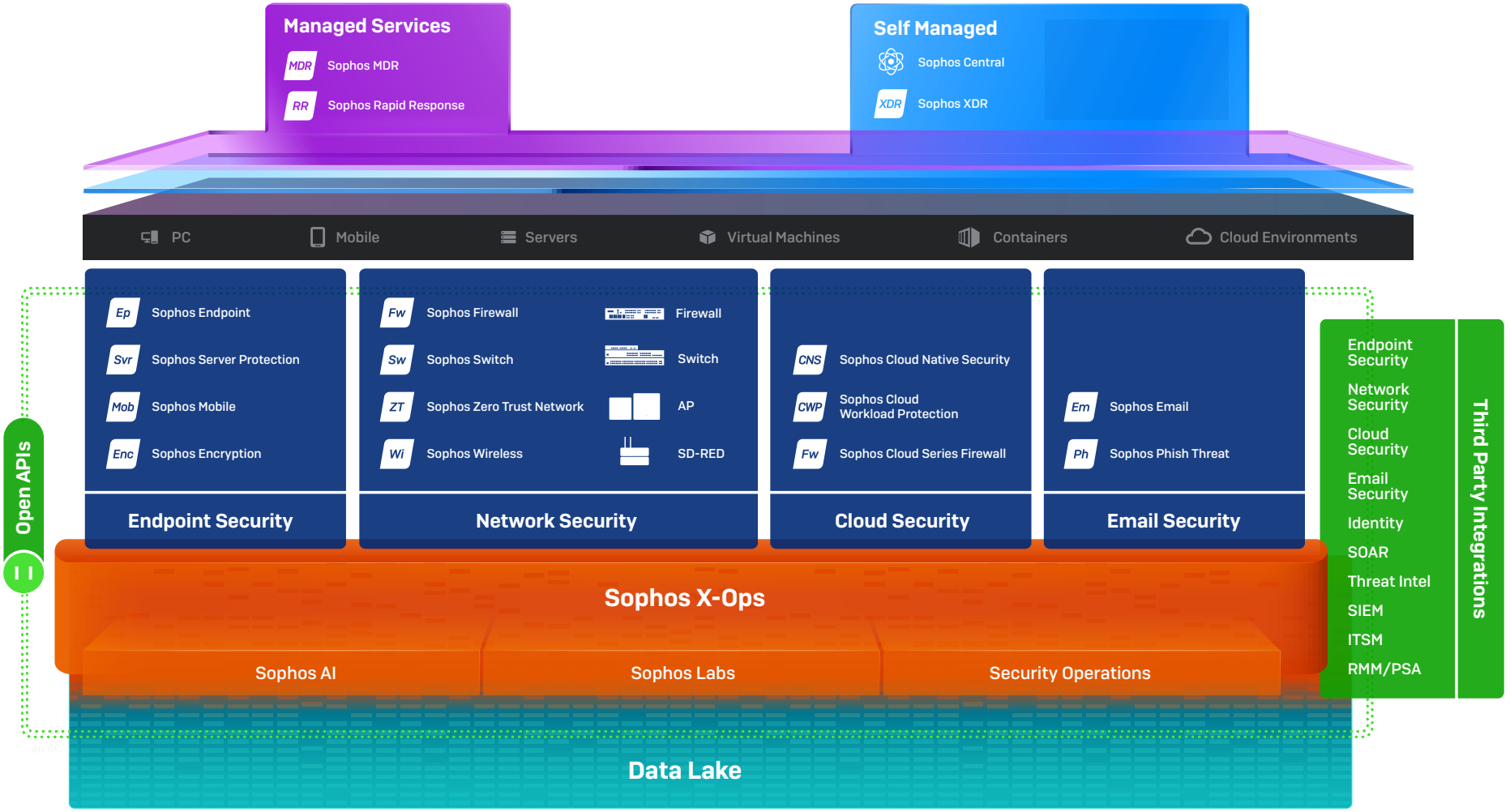
Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally.

No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos.

The **highest rated** and **most reviewed** MDR Service, Endpoint and Firewall on Gartner Peer Insights.

As of August 1, 2022

Sophos Adaptive Cybersecurity Ecosystem



Use Cases

Sophos can help address the most common cybersecurity challenges facing manufacturing organizations.

Stopping Advanced Human-led Attacks, Including Ransomware

Sophos MDR is a fully-managed, 24/7 service delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.

"With Sophos MDR we have reduced our threat response time dramatically."

Tata BlueScope Steel

"Sophos MDR's ability to remediate or remove threats in a swift manner and bring them to our attention frees us up to focus on high-value tasks."

Tomago Aluminium

"Sophos releases the IT teams to undertake more proactive tasks instead of being drawn into managing security challenges."

AG Barr

With Sophos MDR our expert analysts detect and respond to threats in minutes – using your preferred technology – whether you need a full-scale incident response or assistance making more accurate decisions.

We use:

- Sophos' award-winning solutions, including our endpoint, firewall, cloud, and email protection
- Products from other vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others
- Any combination of our technology and other vendors' technology

Sophos MDR protects your organization from advanced attacks that technology solutions alone cannot prevent while increasing the return on your existing investments. As the world's most trusted MDR provider, we have unparalleled depth and breadth of expertise in threats facing the manufacturing sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one manufacturing sector customer to all other customers in the industry, elevating everyone's defenses.

MOST TRUSTED	TOP RATED	BEST PROTECTION
#1 Provider	**4.8/5** Gartner Peer Insights	**38 mins** to detect, investigate, respond
More organizations trust Sophos for MDR than any other vendor	Highest-rated and most reviewed MDR solution as of August 1, 2022	Our analysts are over 5X faster than the fastest in-house SOC teams

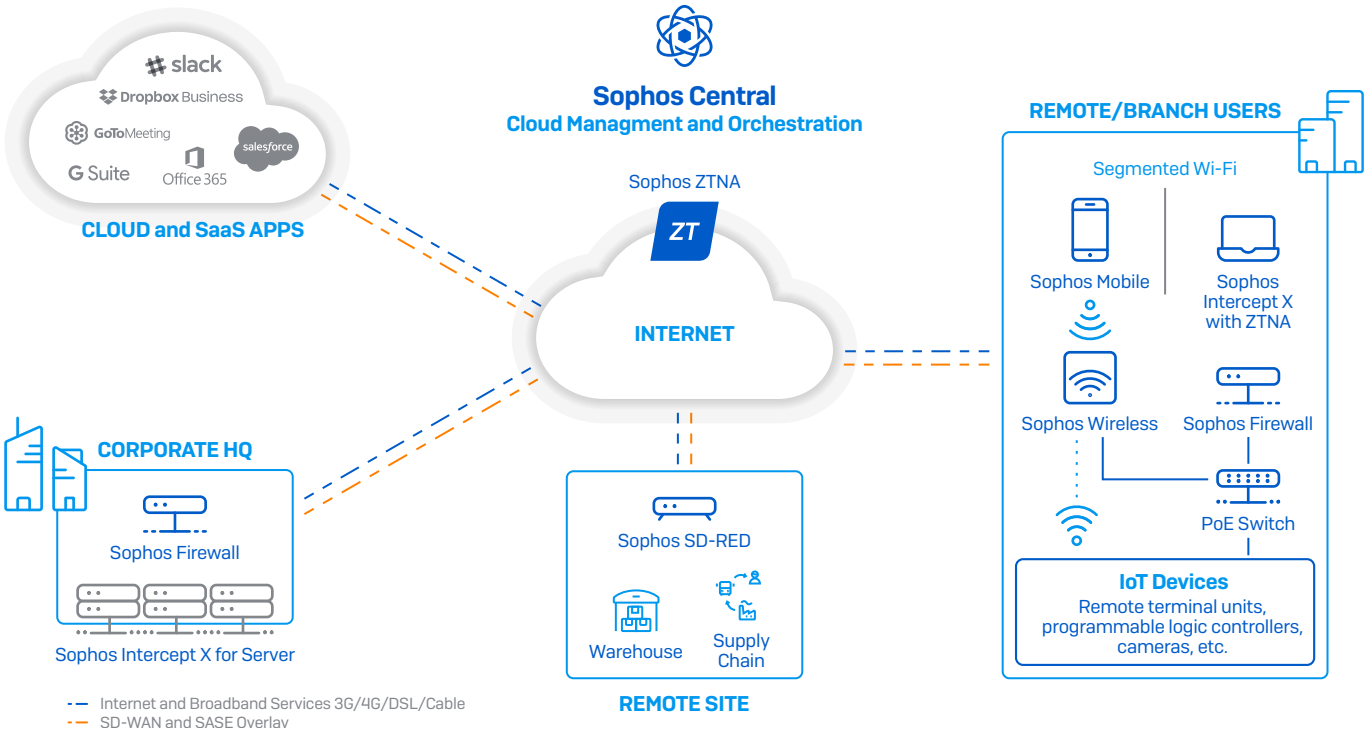
As of September 2022

Securing Access to Critical Industrial Control Systems and Data

Manufacturers need to adopt a zero-trust approach of "trust nothing, verify everything" to secure access to their critical infrastructure and proprietary information. Sophos Zero Trust Network Access solution continuously validates user identity, device health, and compliance before granting access to your applications and data.

Sophos ZTNA shields your Remote Desktop Protocol (RDP) systems – a common tool for remote workers and administrators, but also one of the most common vectors of attack by bad actors – from attacks and provides secure access only to authorized users and devices, including new passwordless options with Microsoft Windows Hello for Business that further helps secure important credentials from possible compromise.

Manufacturers can securely connect remote devices and branch sites from anywhere, deliver critical cloud and SaaS applications, and securely share data with Sophos Secure Access Portfolio. Utilize Sophos ZTNA to secure access to your applications, Sophos SD-RED remote Ethernet devices to safely extend your network to your remote devices and branch sites, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch network access layer switches for secure access on the LAN. Everything is managed through Sophos Central, our all-in-one cloud-based security platform.



Securing Your Network

Sophos Firewall offers powerful protection from the latest threats while accelerating your important SaaS, SD-WAN, and cloud application traffic. Recognized as a Gartner Customers' Choice for Network Firewalls 2022, Sophos Firewall tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain.

Network segmentation is an effective way by which manufacturing organizations can reduce their cyber-risk exposure and return to business as usual faster after a security breach. For example, the IT network of a manufacturing organization can be segmented from the OT network to prevent lateral movement and lateral infection. Sophos Firewall offers flexible and powerful segmentation options via zones and VLANs. This provides ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.

You can also segregate your traffic at the switch level with Sophos Switch, which allows you to configure VLANs to segment your internal traffic and reduce the attack surface in case of a security breach or infection.

Securing Against Phishing Attacks

Phishing scams, more specifically spear-phishing attacks, are one of the easiest ways for attackers to gain access to your system and valuable data.

One of the best ways to stop phishing attacks is to train your employees on how to recognize a phishing scam. Sophos Phish Threat offers a collection of more than 30 security awareness training modules to educate and test your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics.

Allow only trusted senders into your employees' inboxes with Sophos Email that 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. You can further prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with discovery of proprietary information and other confidential contents in all emails and attachments.

Most phishing attacks infect the access points to your network by luring recipients to click on a malicious link that leads to downloading malware on the device or giving access to sensitive data to hackers. To strengthen your network against phishing attacks you must strengthen your endpoint security. Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution.

To optimize your defenses, you need layered protection: multiple sophisticated security capabilities with each playing its part in defending against advanced attacks. Sophos Endpoint is packed with these layers of protection, including:

- Credential theft protection that prevents unauthorized system access.
- Exploit protection to stop the techniques adversaries use.
- Anti-ransomware protection which identifies and blocks malicious encryption attempts.
- Tamper protection that prevents adversaries from turning off defenses so they can deploy their payloads.

Combining multiple layers of protection technologies enables us to optimize our customers' defenses. Testament to the quality of our defenses – and the power of layered protection – we stop 99.98% of threats up-front (AV-TEST average score), and recently earned perfect scores in SE Labs endpoint protection report.

Securing Your Intellectual Property (IP) from Theft

Intellectual property (IP) is crucial information held by manufacturers that helps them stay competitive. Confidential information like product designs, formulas, process patents, and other unique know-how of a manufacturing organization are an attractive target for cybercriminals, competitors, and ex-employees as this gives them immediate access to critical information without investing time and money in R&D. For manufacturers, IP theft can spell huge business loss, and sometimes closure.

Protect your intellectual property data by training your employees to look out for potential threats and creating a positive security awareness culture in your organization with automated attack simulations and security awareness training with Sophos Phish Threat.

Get absolute control over who can access data on your network with Sophos ZTNA. You can establish granular controls to block lateral movement and make sure that only authorized parties can access your sensitive data.

Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across your endpoint devices with Sophos Intercept X endpoint protection. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.

Prevent data breaches with Sophos Email, which allows you to create 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.

Protection Against Insider Attacks

The risk of insiders with authorized access to proprietary data or controls to critical manufacturing operations misusing their privileges or breaching the manufacturer's trust is a critical threat that the manufacturing industry must deal with. Stealing trade secrets, sabotaging manufacturing processes, or damaging equipment via remote access are some of the threats that insiders pose.

Get 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). Take your protection a step further with Sophos Firewall, which 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. It offers user awareness across all areas of the firewall with user-based access policies for traffic shaping (QoS), and other network resources, regardless of the IP address, location, network, or device.

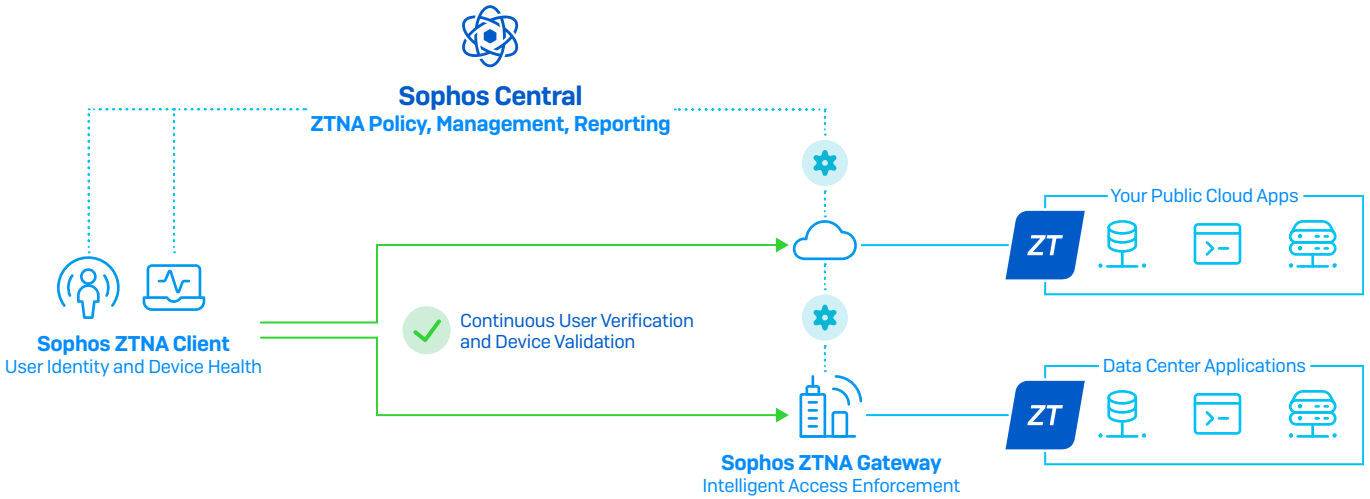
Reducing Supply Chain Risks

Manufacturing supply chains are vast and complex. A vulnerability in any of a supplier's networks can rapidly propagate to infect multiple suppliers and businesses.

Use AI, exploit prevention, behavioral protection, and other advanced technologies to defend against threats that infiltrate manufacturers via third-party suppliers with Sophos Intercept X. Plus, our powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.

Get 24/7 expert support with over 500 specialists working around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf with Sophos MDR.

Protect against supply chain attacks that rely on supplier access to your systems via very granular access controls with Sophos ZTNA, which authenticates requests from trusted partners, irrespective of their location. The unique integration of Sophos Endpoint and Sophos ZTNA automatically prevents compromised hosts from connecting to networked resources, preventing threats from moving laterally and getting a foothold on your network.



Securing Legacy Systems

Manufacturers must protect their legacy or unpatched manufacturing control systems and processes from known vulnerabilities. These devices often run out-of-date operating systems or browsers that cannot be updated because they are no longer supported – yet they need to be connected to the network.

Sophos Firewall and Sophos SD-RED can help. 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 – and our technical specialists can discuss your situation and show you how to do this.

Securing Data Across Multi-Cloud Manufacturing Environments

The cloud is powering up smart factories. Cloud adoption is enabling modern manufacturers to collect real-time machine data from shop floors and convert large volumes of data into business intelligence that helps with process optimization, uncovering inefficiencies, and highlighting ways to operate more sustainably. But the cloud is also a major target for cybercriminals looking to exploit less established cybersecurity practices than in traditional on-premises environments.

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. Plus, it also makes it easy to keep on top of your cloud spend. You can quickly identify if your account is being abused and eject the adversaries before they rack up a big bill.

Conclusion:

Cyberattacks like ransomware, exploits, and phishing can have a severe business and reputational consequences for manufacturers. Protecting your IT environments and sensitive data requires an integrated security approach.

Sophos protects your systems and data wherever they exist with our next-gen services and technologies while enabling you to consolidate your security management with a single vendor. All Sophos solutions are controlled through a unified cloud-based management console, Sophos Central, which allows real-time information sharing between products, centralized management, automated incident response, and deeper insights – all of which, working together, further elevates your protection while enhancing the efficiency of your IT team.

To learn more about how Sophos secures manufacturing organizations and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-04-05 EN-WP (NP)

SOPHOS