Vulnerability pentration testing

Hybrid cloud security involves Network (physical, virtual and WAN), Server and Endpoint (Physical, Virtual or container), and application support at all layers of the service mesh across multiple data centers and hardware devices. Companies increasingly seek “single pane of glass” administration for hybrid cloud networking that includes all of the features of traditional network administration and data center management software with improved real-time data packet analytics. Hybrid cloud security must operate at all levels of the distributed network and include support for new, innovative software platform. Hybrid cloud security poses unique problems for administrators that are best addressed through tools and utilities

Endpoint Protection

Endpoint Detection and Response (EDR): Automatically detect and prioritize potential threats and quickly see where to focus attention and know which machines may be impacted

> XDR integrates powerful endpoint detection and response (EDR) with the industry’s top-rated endpoint protection. Built for both IT security operations and threat hunting, Intercept X detects and investigates suspicious activity with AI-driven analysis. Unlike other EDR tools, it adds expertise, not headcount by replicating the skills of hard-to-find analysts.

Extended Detection and Response (XDR): Go beyond the endpoint by incorporating cross-product data sources for even more visibility

> Sophos Intercept X Advanced with XDR is the industry’s only XDR solution that synchronizes native endpoint, server, firewall, email, cloud and O365 security. Get a holistic view of your organization’s environment with the richest data set and deep analysis for threat detection, investigation and response for both dedicated SOC teams and IT admins.

Anti-Ransomware: Ransomware file protection, automatic file recovery, and behavioural analysis to stop ransomware and boot record attacks

> Today’s ransomware attacks often combine multiple advanced techniques with real-time hacking. To minimize your risk of falling victim you need advanced protection that monitors and secures the whole attack chain. Sophos Intercept X gives you advanced protection technologies that disrupt the whole attack chain including deep learning that predictively prevents attacks and System Guard which rolls back the unauthorized encryption of files in seconds.

Deep Learning Technology: Artificial intelligence built into Intercept X that detects both known and unknown malware without relying on signatures

> By integrating deep learning, an advanced form of machine learning, Intercept X is changing endpoint security from a reactive to a predictive approach to protect against both known and never-seen-before threats. While many products claim to use machine learning, not all machine learning is created equally. Deep learning has consistently outperformed other machine learning models for malware detection.

Exploit Prevention: Deny attackers by blocking the exploits and techniques used to distribute malware, steal credentials, and escape detection

> Exploit prevention stops the techniques used in file-less, malware-less, and exploit-based attacks. While there are millions of pieces of malware in existence, and thousands of software vulnerabilities waiting to be exploited, there are only handful of exploit techniques attackers rely on as part of the attack chain – and by taking away the key tools hackers love to use, Intercept X stops zero-day attacks before they can get started.

Managed Threat Response: Elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats

> Managed Threat Response (MTR) provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully managed service. MTR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision. Unlike other services, the MTR team goes beyond simply notifying you of attacks or suspicious behaviours, and takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats.

Active Adversary Mitigations: Active adversary mitigation prevents persistence on machines, credential theft protection, and malicious traffic detection

> Intercept X utilizes a range of techniques, including credential theft prevention, code cave utilization detection, and APC protection that attackers use to gain a presence and remain undetected on victim networks. As attackers have increasingly focused on techniques beyond malware in order to move around systems and networks as a legitimate user, Intercept X detects and prevents this behaviour in order to prevent attackers from completing their mission.

Central Management: Manage your endpoint protection, EDR, XDR and other Sophos solutions from a unified console

> Central is the cloud-based management platform for all Sophos solutions. You can investigate potential threats, create and deploy policies, manage your estate, see what is installed where and more, all from the same unified console.

Network Protection Firewall & Wireless

Deep Packet Inspection: (DPI) engine provides high-performance traffic scanning for IPS, AV, Web Protection, and App Control in a single streaming engine.

Encrypted Traffic: TLS Inspection with industry-leading performance, visibility, policy tools, and built-in intelligence removes an enormous blind spot in your protection.

Zero-Day and ML Protection: Firewall leverages industry-leading machine learning technology to instantly identify the latest ransomware and unknown threats before they get on your network.

Cloud Sandbox: Zero-day Dynamic File Analysis uses next-gen cloud-sandbox technology powered by deep-learning to provide your organization with the best protection against zero-day threats like the latest ransomware and targeted attacks coming in through phishing, spam, or web downloads

Web Protection: Protection engine includes innovative technologies required to identify and block the latest web threats.

Synchronized Security: Our Security Heartbeat links your managed endpoint with your firewall to share health and other valuable information enabling an automated and coordinated response to isolate threats and prevent lateral movement.

Advanced Threat Protection: Delivers advanced threat protection to instantly identify bots and other advanced threats while defending your network from today's sophisticated attacks.

User Identity: User identity-based policies and unique user risk analysis give you the knowledge and power to regain control of your users before they become a serious threat to your network.

Application Control: Complete application visibility and control over all applications on your network with deep-packet scanning technology and Synchronized App Control that can identify all the applications that are currently going unidentified on your network.

Web Control: Full visibility and control over all your web traffic with flexible enforcement tools that work the way you need, with options for user and group enforcement of activity, quotas, schedules, and traffic shaping

Content Control: Flexible, user-based monitoring and control of keyword content and downloadable content, including file types via FTP, HTTP, or HTTPS.

Business Applications: Combine next-gen firewall capabilities with our enterprise-class web application firewall to protect your critical business applications from hacks and attacks while still enabling authorized access.

Email and Data: Protect your email from spam, phishing, and data loss with our unique all-in-one protection that combines policy-based email encryption with DLP and anti-spam

SD-WAN: Firewall integrates all the features you need to enable your SD-WAN connectivity, quality, security, and continuity goals.

Site-to-Site VPN: Sophos Firewall supports all standards-based VPN technologies as well as our own light-weight extremely robust layer 2 tunnels.

Wireless Controller: Every Sophos Firewall includes an integrated wireless controller to enable easy secure wireless deployments for our APX wireless access points, all managed from a single console.

ZTNA: Firewall integrates with Sophos Zero Trust Network Access (ZTNA) to offer a secure and simple way for users to securely connect to important applications and data.

Segmentation: Flexible and powerful segmentation options via zones and VLANs provide ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.

Managed Threat Response

Threat Notification Isn't a Solution – It's only the Starting Point. Managed detection and response (MDR) services simply notify you of attacks or suspicious events. Then it's up to you to manage things from there whereas with our MTR, your organization is backed by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats.

Complete Control and Transparency

We do the work, but you own the decisions. This means you control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications. Weekly and monthly reports let you know what is happening in your environment and what steps have been taken to keep you safe.

- **Notify:** We notify you about the detection and provide details to help you with prioritization and response.
- **Collaborate:** We work with your internal team or external point(s) of contact to respond to the detection.
- **Authorize:** We handle containment and neutralization actions and inform you of the action(s) taken.

Machine Learning High-Fidelity Detection: We combine deterministic and machine learning models to spot suspicious behaviors and the tactics, techniques, and procedures used by the most advanced adversaries.

Proactive Defense: Combining threat intelligence with newly-discovered indicators of compromise identified through threat hunts, Intercept X proactively protects your environment.

Elite Expertise: Our highly-trained team of threat hunters, engineers, and ethical hackers has your back 24/7, investigating anomalous behavior and taking action against threats.

Outcome-based focused Security: Every hunt, investigation, and response action results in decision-driving data that is to enhance configurations and automated detection capabilities.

Cloud protection

Hybrid Cloud Security: Trusted to provide powerful and effective cybersecurity solutions specifically designed to be accessible and manageable for any organization. Available in a single, unified

management console. Threat protection, monitoring, and response solutions provide protection of on-premises and cloud environments from the latest advanced threats and vulnerabilities.

Cloud Native: Accelerate your business and protect cloud investments with cloud native protection covering Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure, Kubernetes clusters, container registries, and Infrastructure-as-Code environments from the latest threats and vulnerabilities, while optimizing cloud resource spend.

Cloud Edge Firewall: Protect environments from network threats, maintain web application availability, and extend your secure network with flexible SD-WAN, Zero Trust Network Access, and VPN connectivity.

SaaS Email Security: Stop phishing, business email compromise attacks, and ransomware with advanced protection, data loss prevention, and encryption for SaaS email services.

Cloud Security Posture Management: Monitor infrastructure and integrate with CI/CD pipelines to proactively reduce business risk from unsanctioned activity, vulnerabilities, misconfigurations, and insecure identities.

Cloud Workload Protection: Stop ransomware and advanced threats with award-winning protection for cloud server instances that includes XDR and cloud security posture management.

Serverless Protection: Maintain serverless infrastructure and protect shared storage assets from malicious content by integrating Labs global threat intelligence APIs.

24/7 Threat Protection, Monitoring, and Response: Take the weight of 24/7 threat monitoring and response off your shoulders with a proactive managed services team monitoring your environments 24/7 to respond the latest threats.