

SOPHOS Cyber Security as a Service

Walter Narisoni

Director Sales Engineer South EMEA

SOPHOS

The Hard Truth

66%

of organisations hit by
ransomware

46%

of organisations paid the ransom

65%

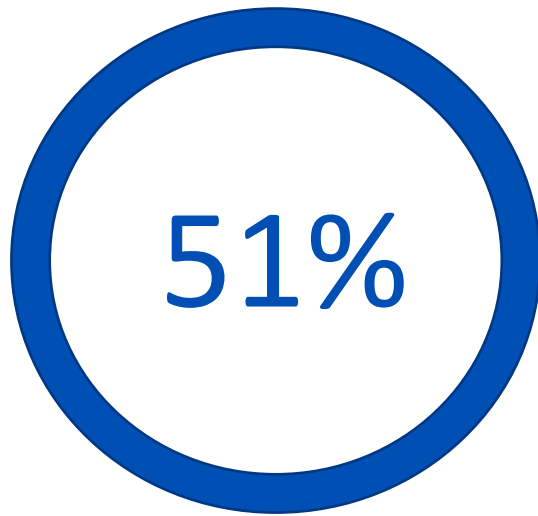
of attacks successfully
encrypted data

£1.4m

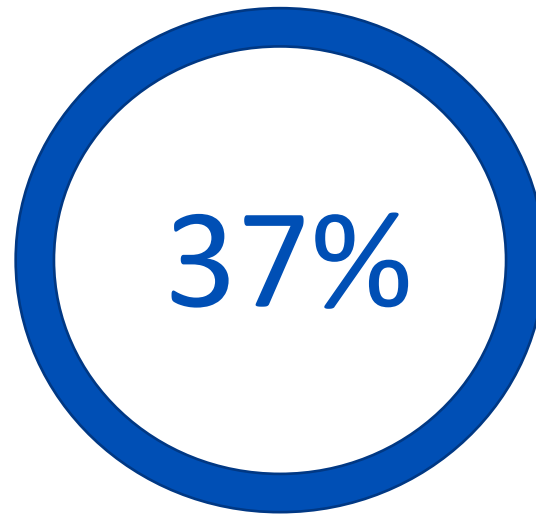
average ransomware recovery cost

Ransomware is Back on the Rise

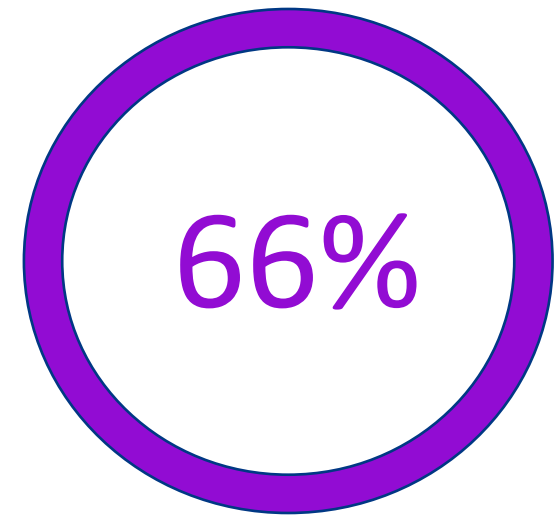
2019



2020



2021



Ransomware Recovery Is A Complex Process

1 MONTH
Average recovery time

SLOWEST

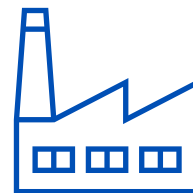
FASTEST



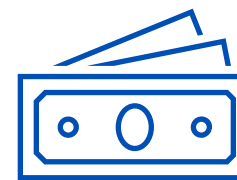
Higher
Education



Central/Federal
Government



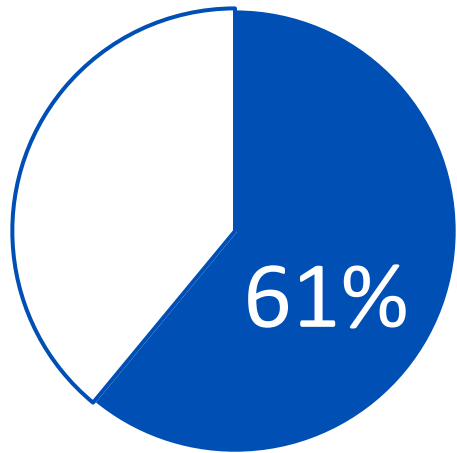
Manufacturing/
Production



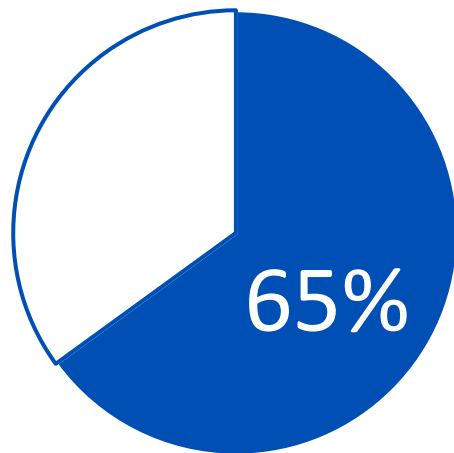
Financial
Services

Less Data Is Recovered After Paying the Ransom

Percentage of data restored after paying the ransom

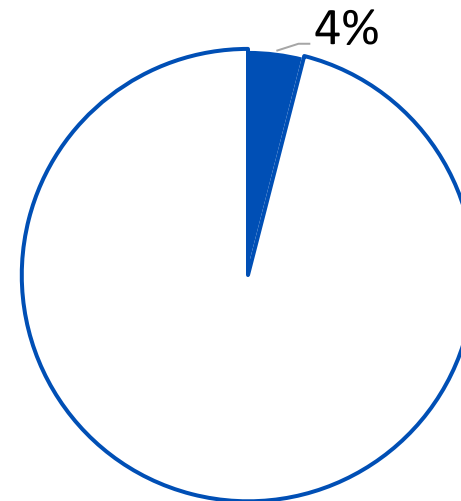


2021

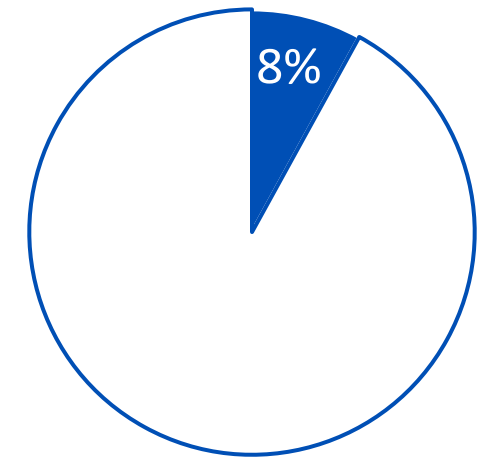


2020

Percentage that got ALL their data back after paying the ransom



2021



2020

The Outlook is Bleak

89% Hit by ransomware have insurance that covers ransomware



Category	Percentage
Hit by ransomware have insurance that covers ransomware	89%
Not hit have insurance that covers ransomware	70%

70% Not hit have insurance that covers ransomware



Cyber Insurance is Harder to Secure

94%

The process for securing cover changed over the last year

54%

Higher level of cybersecurity needed

47%

Policies are more complex

40%

Fewer companies now offer cyber insurance

37%

The process takes longer

34%

It's more expensive

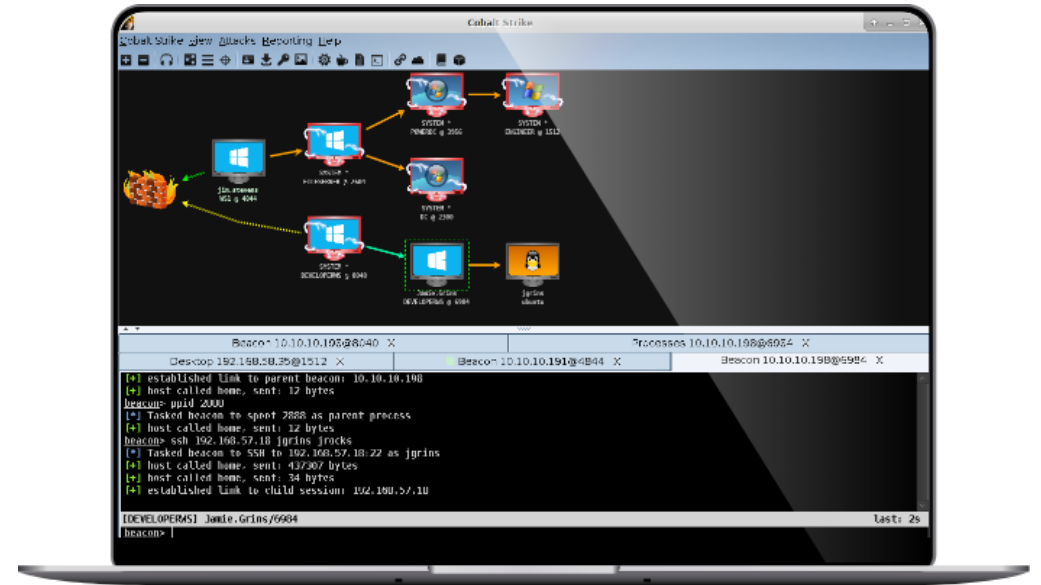
Ransomware Will Become More Modular, Uniform and Influential

- Specialists will offer different elements of an attack “as-a-service”
- The developers create sophisticated code
- Playbooks will enable different adversary groups to implement very similar attacks
- Initial Access Brokers (IABs) and malware delivery platforms will find and target victims



The Abuse Of Attack Simulation Tools Will Continue

- Commercial attack simulation tools are designed to test defenses
- Adversaries are abusing these tools
- Most of the ransomware cases Sophos investigated in 2021 involved the abuse of Cobalt Strike Beacons
- Every alert relating to such tools or combination of tools could indicate the presence of an intruder



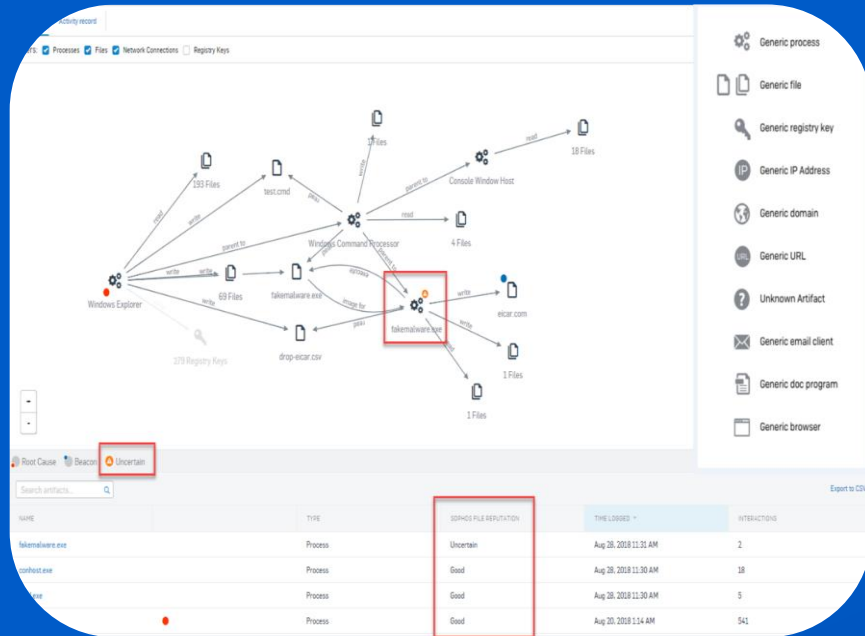
More Attacks Will Mass-Abuse IT Administration Tools and Vulnerable Internet Facing Services

In 2021, attackers targeted software bugs in...

- SolarWinds' Orion remote management tool
- Microsoft Exchange (ProxyLogon, ProxyShell)
- Kaseya's remote IT management tool (REvil ransomware)



Human Threat Hunting



DIY with XDR

or



Outsource with MDR



Cybersecurity is so complex and moves so fast that most organizations simply can't manage it effectively on their own.



Complex



Expertise

Challenges to deliver IT security

81%

Their ability to find and retain skilled IT security professionals is a **major challenge** to their ability to deliver IT security

54%

“A significant challenge”

27%

“Our single biggest challenge”

Managed Detection and Response (MDR)

A fully-managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent



Gartner®

By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities

Cybersecurity as a Service



Less Risk



Greater Efficiency



Lower Costs

Cybersecurity as a Service



**OPTIMIZE
PREVENTION**

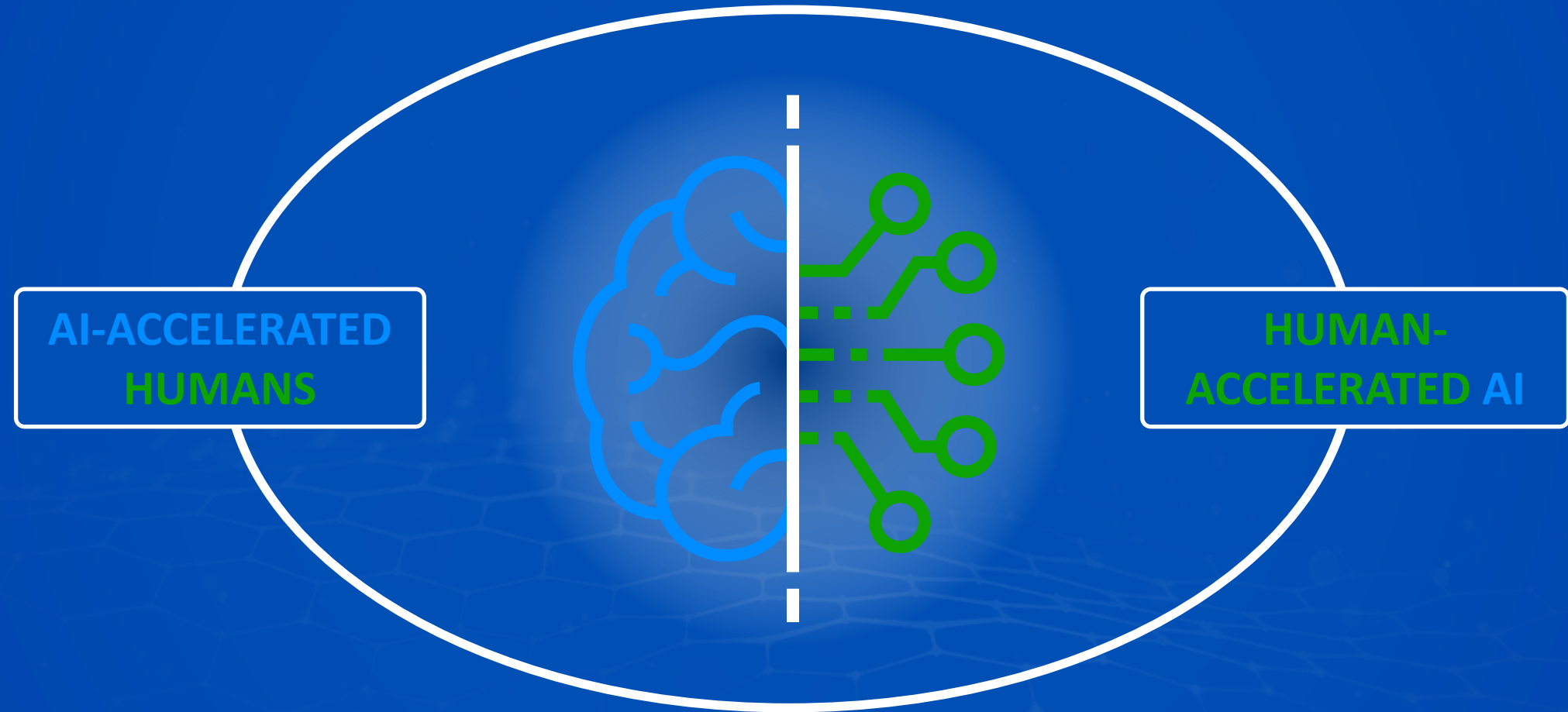


**MINIMIZE TIME
TO DETECT AND
RESPOND**



**AUTOMATE WITH
HUMAN-MACHINE
COLLABORATION**

Automate With Human-Machine Collaboration





Sophos MDR

Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own

Threat Detection

Enabled by extended detection and response (XDR) capabilities that detect known threats and potentially malicious behaviors wherever your data reside

Incident Response

Our analysts respond to threats in minutes whether you need full-scale incident response or assistance making more accurate decisions

12,000+ MDR Customers

99.98% of threats automatically blocked*

Average Sophos MDR Threat Response Times

Time to Detect

Less than 1 Minute

Time to Investigate

Less than 25 Minutes

Time to Respond

Less than 12 Minutes

Response Actions

Actions	Description
Change Configurations	Adjust configurations to manage an active threat. Can include adjusting threat policies, enabling EDR/MTR on unprotected devices, adjusting exclusions, etc.
Isolate Hosts	Leverage Sophos Central's isolate host functionality to limit the exposure a compromised asset could have
Block Files	Block files by SHA256 within an environment to prohibit malicious content from running
Run Scan	Initiate system scan
Block websites/IPs/CIDR	Block a specific website or IP address through web control
Block Application	Block a specific application through application control
Use Live Terminal	If other response actions are not effective, the use of Live Terminal can give us direct access to the host. <i>*Requires team lead approval.</i>



Sophos MDR

Compatible with your environment

We can use our tools, someone else's tools or any combination of the two

Compatible with your needs

Whether you need full-scale incident response or assistance making more accurate decisions

Compatible with your business

Our team has deep experience hunting threats targeting organizations in every industry

Sophos



Endpoint



Firewall



Cloud SaaS



Email



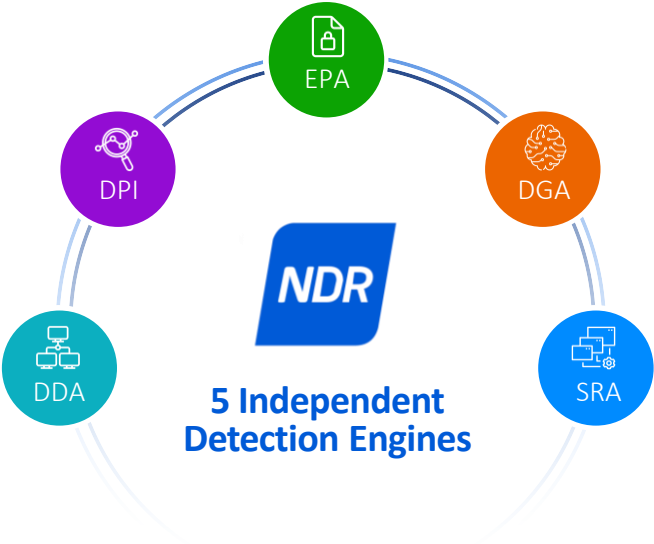
Identity



Network



Detects Network Threats and Generates Cases for Investigation and Correlation within Sophos MDR



DDA **Device Detection Analytics**

Identifies systems communicating on your network that are not managed by Sophos, including unauthorized, potentially malicious devices

DGA **Domain Generation Algorithms**

Powered by a deep learning Long Short-Term Memory (LSTM) prediction model to detect domain names generated by algorithms

DPI **Deep Packet Inspection**

Detects known IOCs amongst encrypted and plain text traffic to rapidly identify threat actors and TTPs

SRA **Session Risk Analytics**

Powerful logic engine that utilizes rules that alert on session-based risk factors (e.g., self-assigned TLS Certificates, binary application transfer, etc.)

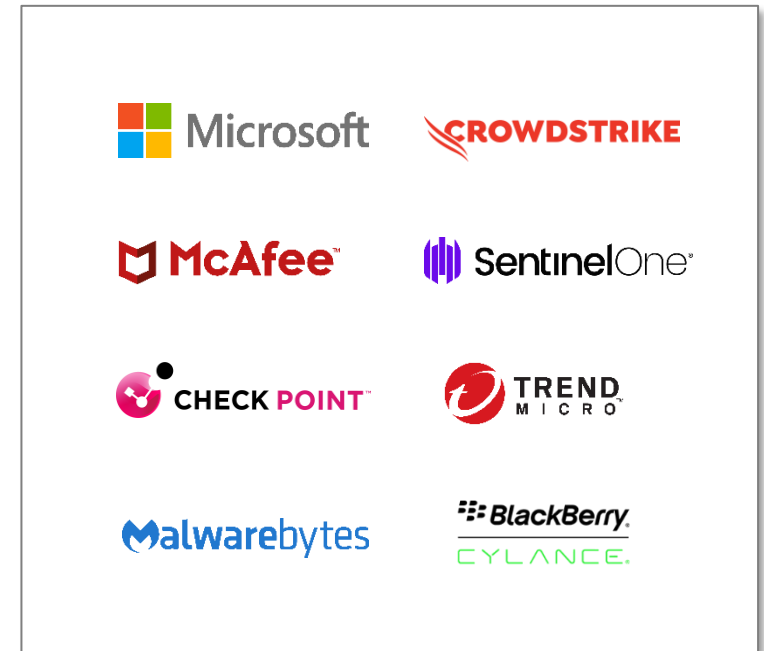
EPA **Encrypted Payload Analytics**

Detects zero-day C2 servers and new variants of malware families based on patterns found in the session packets size, direction, and interarrival times

XDR Sensor

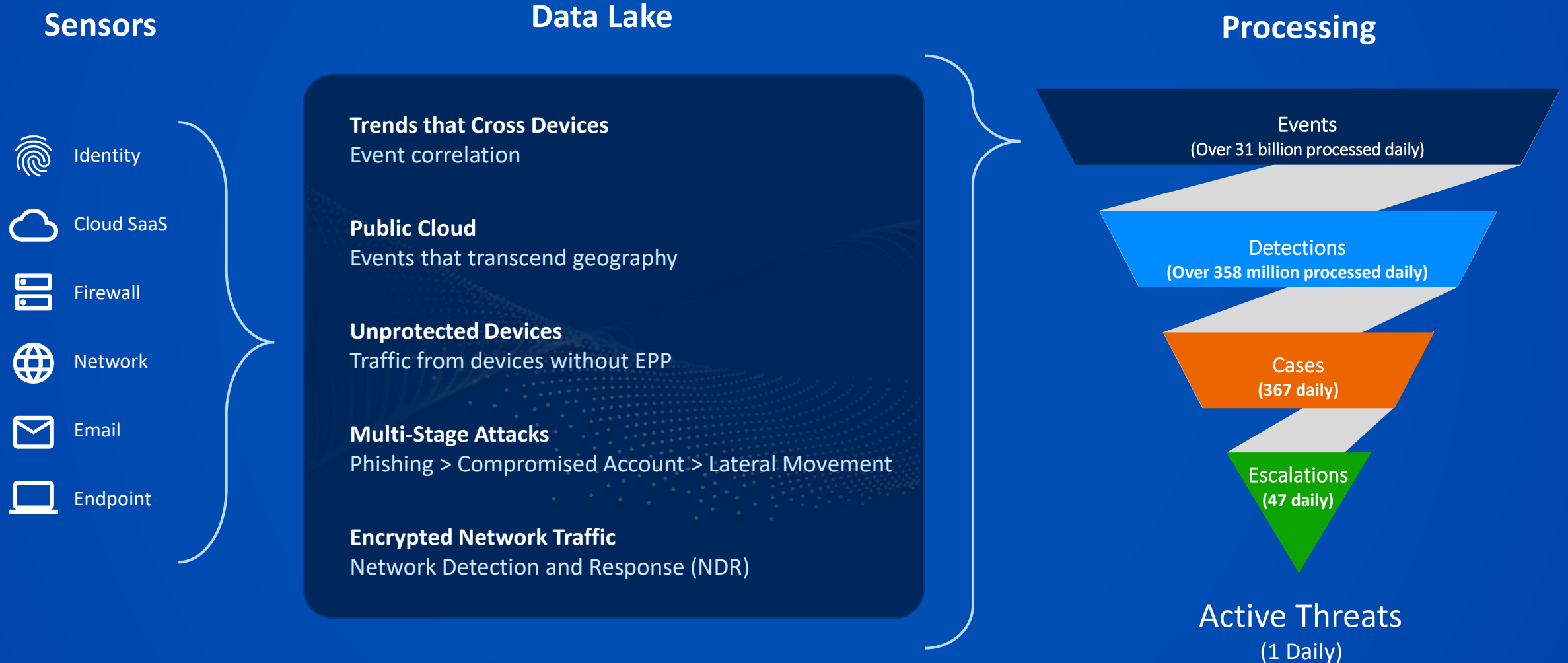
Gives organizations using non-Sophos endpoint protection an immediate path to Sophos XDR and Sophos MDR

- **Runs alongside non-Sophos endpoint products**
 - No Sophos protection. AV provided by third-party endpoint
- **Cross-platform support**
 - Windows, macOS, Linux
 - **No reboot required!** ~80MB footprint
- **Sophos-generated XDR detections**
 - **Note:** Additional detections generated by third-party endpoint products require SOC.OS connectors, available for MDR only at launch
- **Sophos XDR investigation and response capabilities**
 - Live Discover - manual and scheduled data lake queries
 - Live Response - connect to devices to investigate and remediate issues



- ✓ Behavioural Detections
- ✓ Local/Global Reputation
- ✓ Event Journals
- ✓ Live Discover
- ✓ Live Response
- ✓ Response Actions

Broad, Advanced Telemetry Allows Sophos to See More



Sophos MDR Is the Best of Both Worlds

BRING-YOUR-OWN-TECHNOLOGY MDR

Provides MDR services using the customer's existing cybersecurity tools

- ✔ Can collect security data from multiple sources
- ⚠ Limited ability to perform manual response actions
- ⚠ Typically provide "guidance" only, leaving customer to implement

Representative vendors



SINGLE VENDOR MDR

Provides MDR services as an overlay on top of vendor's own cybersecurity tools

- ✔ Cybersecurity tools and MDR services are integrated
- ⚠ Requires customer to rip and replace existing cybersecurity tools
- ⚠ Limited to actions that can be taken by the one set of cybersecurity tools

Representative vendors



Sophos MDR

The only service that combines the strengths of both delivery models

- No need to replace existing cybersecurity tools
- Delivered using our integrated tools, third-party tools, or any combination of the two
- Customized service levels from detailed notification to full-scale incident response

Sophos Service Tiers

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓	✓
Compatible with non-Sophos security products	✓	✓	✓
Weekly and monthly reporting	✓	✓	✓
Monthly intelligence briefing: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Account Health Check		✓	✓
Expert-led threat hunting		✓	✓
Threat Containment: attacks are interrupted, preventing spread <small>Uses full Sophos XDR agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)</small>		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale Incident Response: threats are fully eliminated <small>Requires full Sophos XDR agent (protection, detection and response)</small>			✓
Root Cause Analysis: performed to prevent future recurrence			✓
Dedicated Incident Response Lead			✓

Included Integrations – No Additional Charge

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations

Included in Sophos MDR and Sophos MDR Complete Pricing

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; integrated at no additional charge

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection

Sophos Endpoint Protection

Block advanced threats and detect malicious behaviors—including attackers mimicking legitimate users

Included in Sophos MDR and Sophos MDR Complete Pricing

Sophos Email

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

Product sold separately; integrated at no additional charge

Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events from Office 365 and Azure Active Directory activity logs

Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform

Product sold separately; integrated at no additional charge

90-Days Data Retention

Retains data from all Sophos products and any third-party (non-Sophos) products in the Sophos Data Lake

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Add-On Integrations



Sophos Network Detection and Response

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

Compatible with any network via SPAN port mirroring



Firewall

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall



Identity

- Okta
- Duo



Public Cloud

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud



Email

- Proofpoint
- Mimecast



Network

- Darktrace
- Forcepoint
- McAfee (web gateway)



1-Year Data Retention

All Integration Packs are available for Sophos MDR, Sophos MDR Complete, and Sophos Threat Advisor
All Integration Packs need to be purchased based on the number of Sophos MDR seats for that customer

MDR That Meets You Where You Are

People

I need an expert team to...

Completely manage threat response

Co-manage threat response with my team

Alert my team to threats that require action

Process

Confirmed threats require...

Full-scale incident response: threat is eliminated

Containment so my team can eliminate them

A detailed alert with remediation guidance

Technology

I want to use...

Sophos: best protection, detection, and response

A combination of Sophos and non-Sophos tools

Non-Sophos tools only

Visibility

Detect threats using data from...

Endpoint

Firewall

Email

Identity

Public Cloud

Network

Free integrations with Sophos solutions, including:

XDR Sophos XDR

Fw Sophos Firewall


Em Sophos Email

Mob Sophos Mobile


Cld Sophos Cloud

NDR Sophos NDR

Non-Sophos Integrations included with the service:

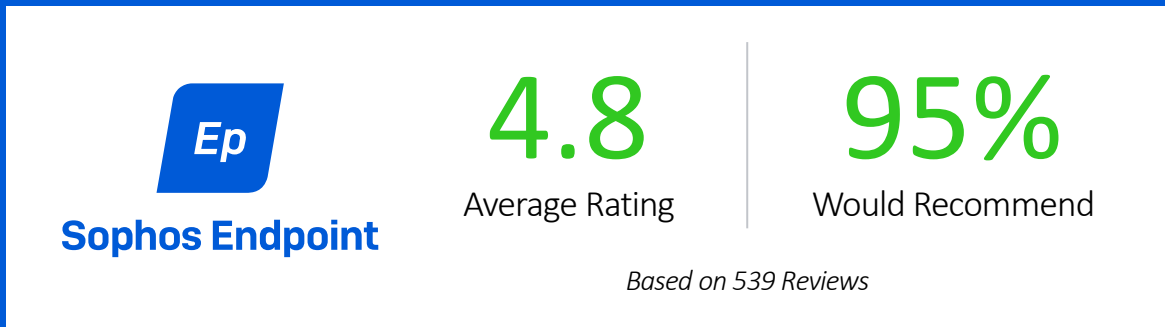
 Any endpoint protection platform, including Windows Defender

Add-on integrations available for purchase:

 Virtually any security tool that generates threat detection data

Gartner Peer Insights™

The **highest rated** and **most reviewed** solutions across MDR, Endpoint, and Firewall



Reviews from last 12 months as of August 1, 2022
*Vendors with fewer than 50 customer reviews

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

**24/7 threat hunting,
investigation, and
response delivered by
an expert team as a
fully-managed service**



Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside



Proactive threat hunts performed by highly-trained analysts uncover more malicious behavior than security products can detect on their own



Analysts respond to threats in minutes whether you need full-scale incident response or assistance making more accurate decisions



Identifies the root cause of threats and provides recommendations to prevent future incidents and reduce risk to your business

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

Emergency incident response to rapidly eliminate active threats and monitor for reoccurrence



Delivered by a 24/7 team of remote incident response experts, threat intelligence analysts, and threat hunters



Rapid deployment enables threat responders to take immediate action to triage, contain, and eliminate active threats



45 days of ongoing threat monitoring and response from the Sophos MTR team ensures any recurrence of the threat is handled immediately



Fixed-fee pricing determined by the number of users and servers in your environment keeps remediation costs predictable

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

The fastest, most effective means of identifying ongoing or past attacker activity in your environment.



Delivered by an expert team of threat hunters and response specialists who confirm if an attacker is operating undetected in your environment



Identifies the scope of the threat and quantifies the potential risk of a widespread security incident



Receive a written report with technical documentation and a non-technical executive summary detailing evidence of attacker activity



Immediately shift from threat assessment to threat neutralization with Sophos Rapid Response

Zero Trust Network Access

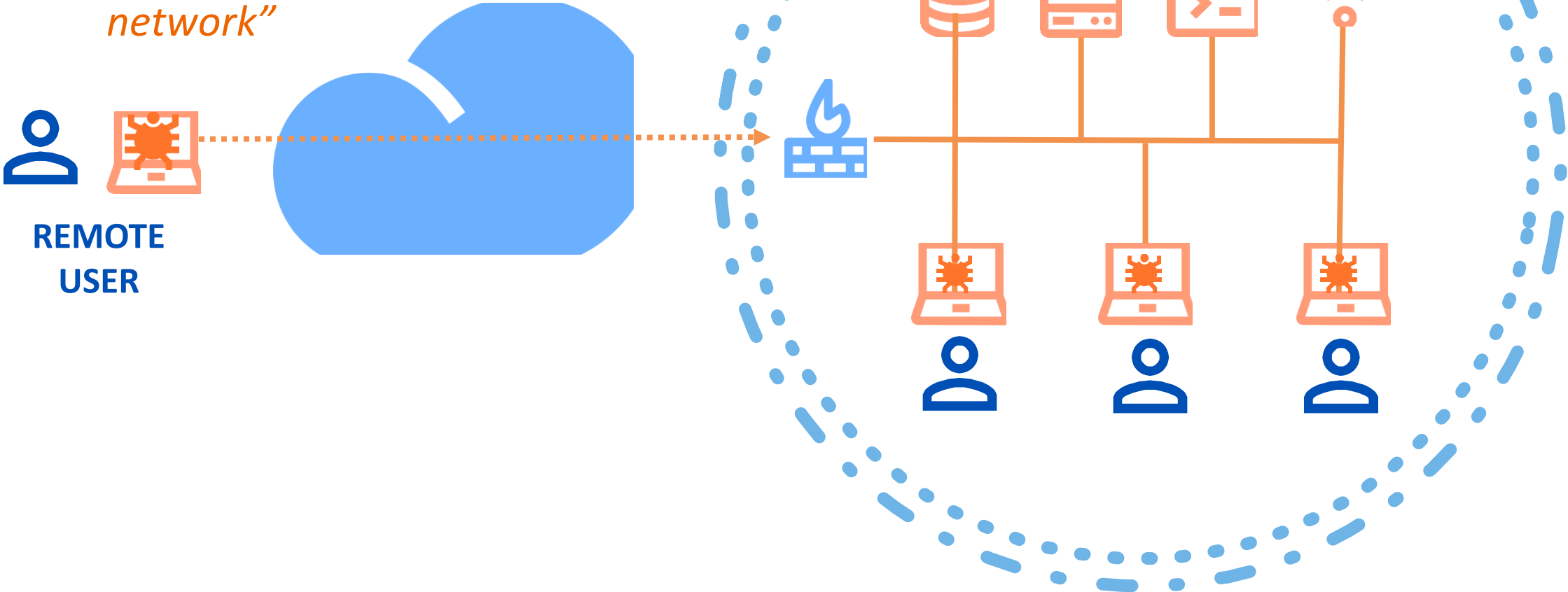


Times have changed with Remote Access



Classic Scenario

*Remote Access VPN:
users are "on the network"*



Micro Segmentation



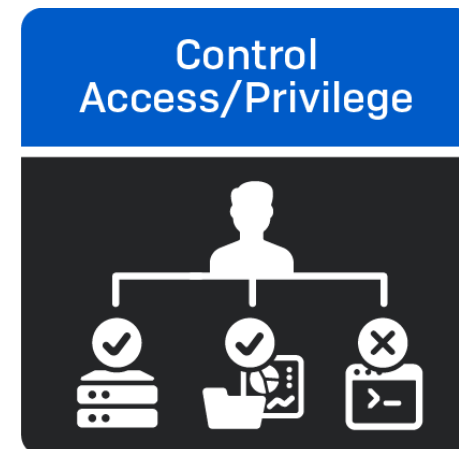
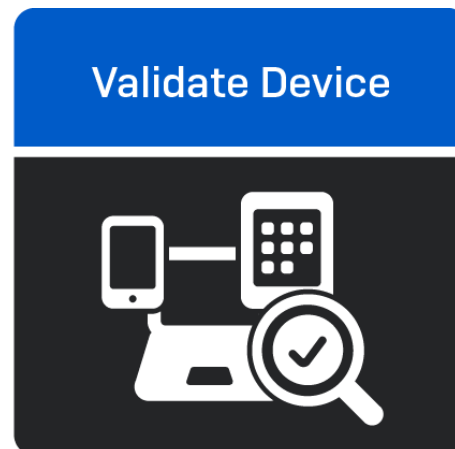
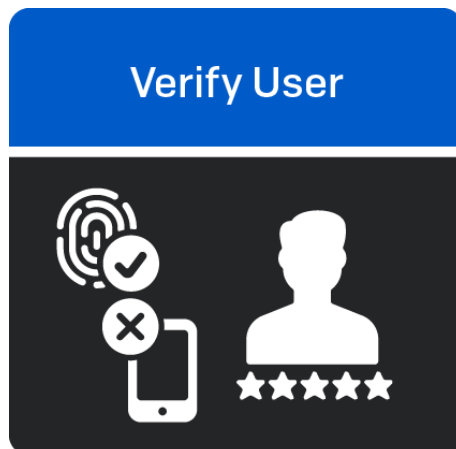
Airport Security vs Zero Trust

As same as Airport Security, Zero Trust requires to check everything and trust nothing:

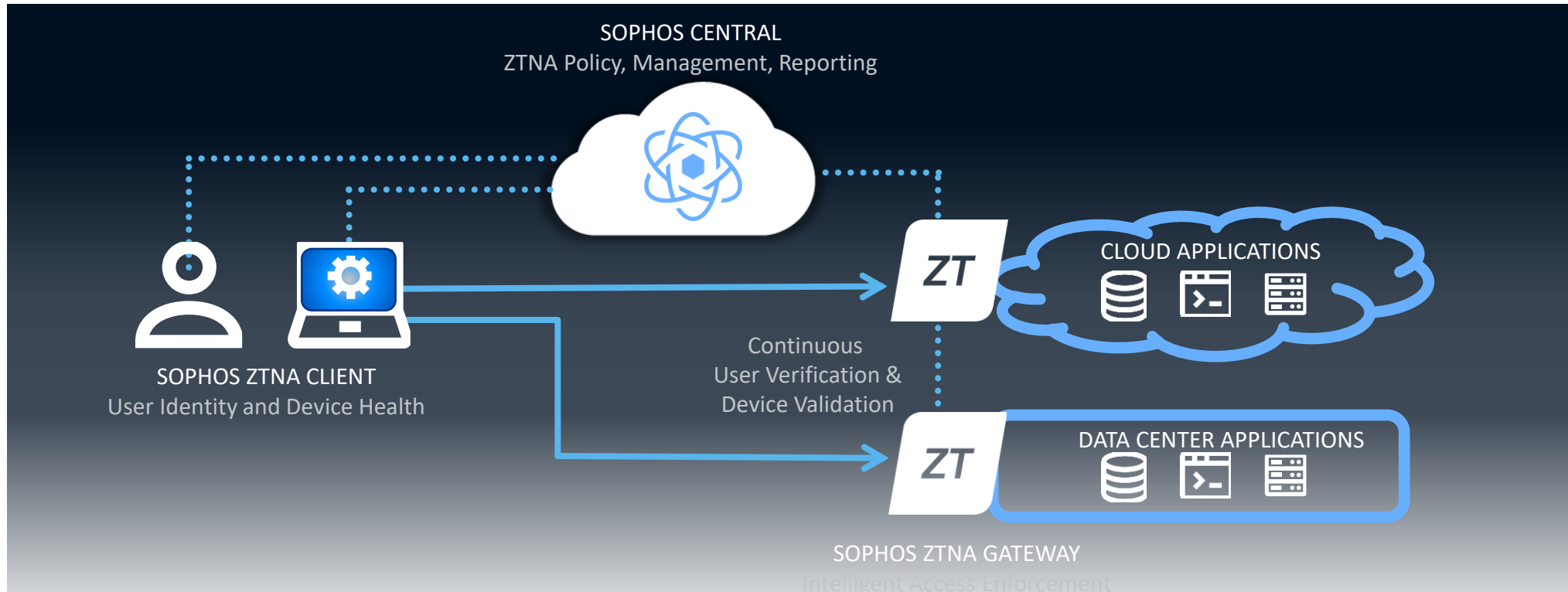
AIRPORT



ZTNA



Sophos ZTNA Components



ZTNA CLIENT

- Integrates identity and device health continuously
- Synchronized Security Heartbeat or Windows Security Center*
- Easy to deploy from Sophos Central
- Windows, Mac*, Mobile*

**Roadmap item*

SOPHOS CENTRAL

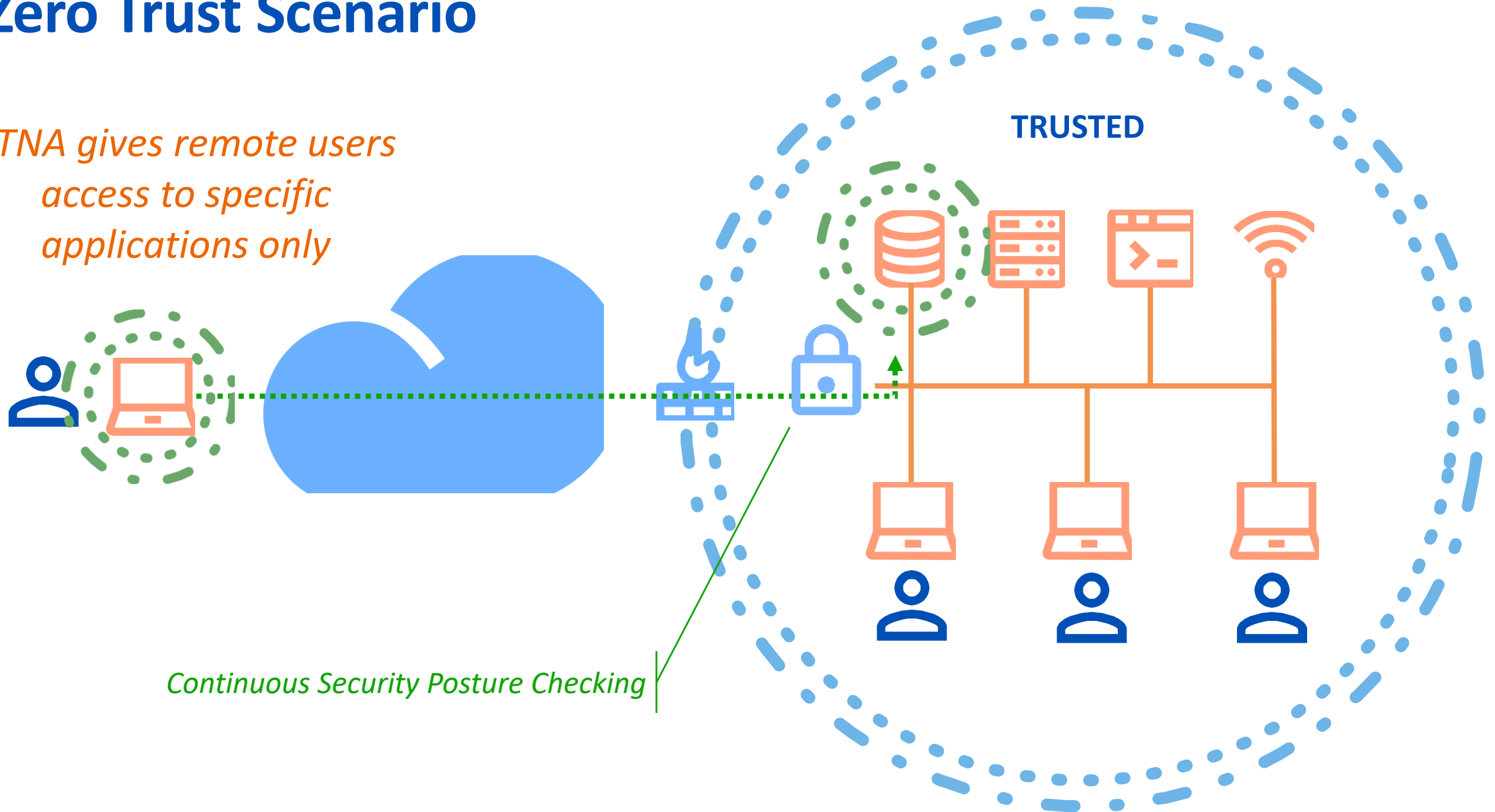
- The ultimate cloud management
- Easy ZTNA deployment alongside Intercept X or stand-alone
- Granular policy controls
- Insightful reporting

ZTNA GATEWAY

- Software/VM-based for cloud
- Intelligently and continuously verifies and validates access based upon policy
- Initial support for VMware ESXi and AWS with other platforms to follow
- Log and event data shared with Sophos Central

Zero Trust Scenario

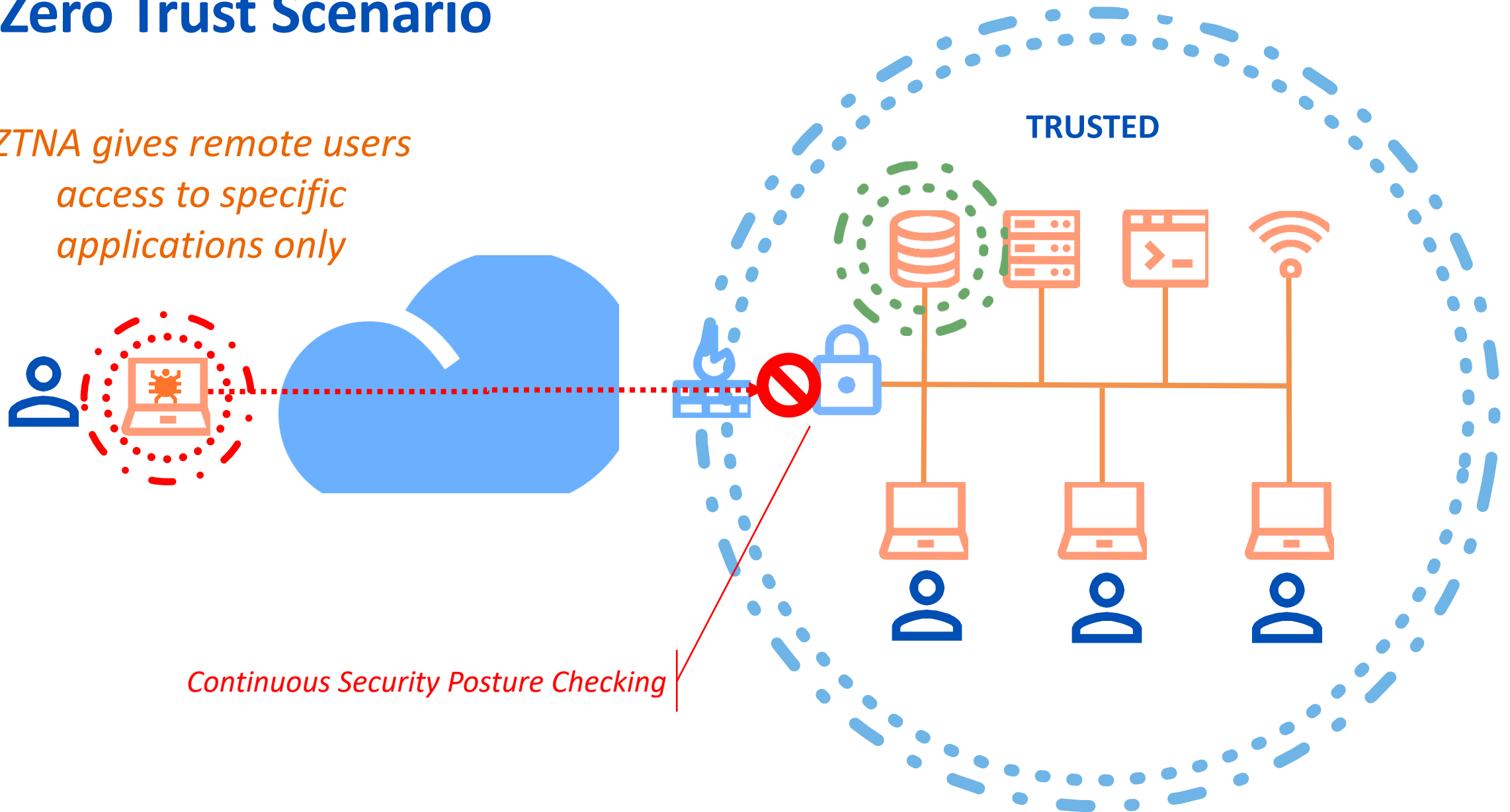
ZTNA gives remote users access to specific applications only



Continuous Security Posture Checking

Zero Trust Scenario

ZTNA gives remote users access to specific applications only



Continuous Security Posture Checking

Applications – ZTNA controls access to your apps

Typical apps you can control with ZTNA...
(Any self-hosted app or system)



Typical apps you can't control...
(Any SaaS app)



...requires Web Control and/or CASB

ZTNA and Intercept X

Component Installation Options ✕

Use this option to install only some of your licensed software on **new machines**.

If you'd like to add software to a machine that's already managed, select it on the [Computers](#) page and use the '**Assign/Unassign Software**' button.

Choose which Endpoint Protection components you'd like to download

- Sophos Intercept X Advanced
- Device Encryption
- Zero Trust Network Access

Cancel

Download Installer

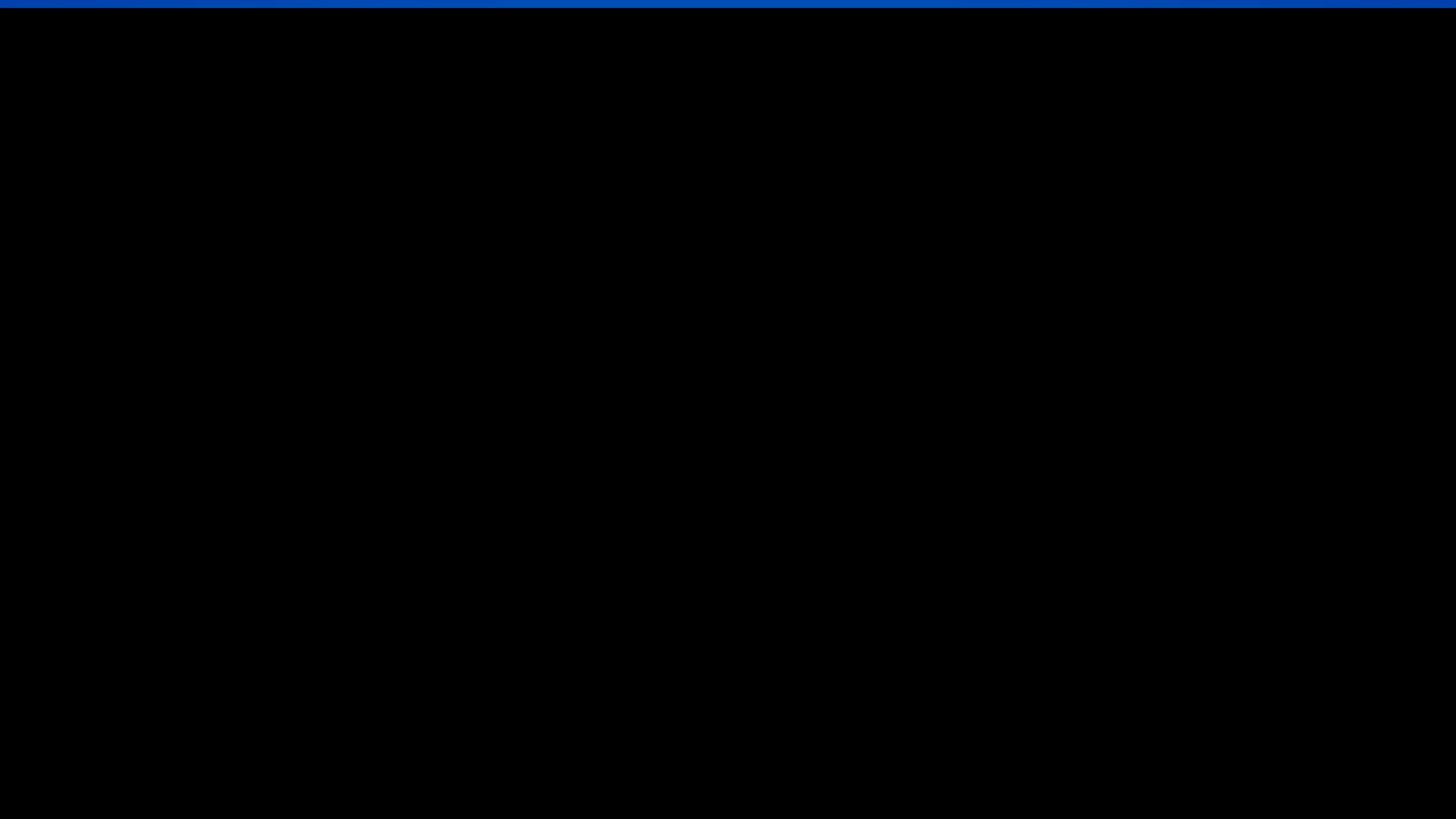
ZTNA Agent:

- Easy to deploy while installing Intercept X or later
- It enables Synchronized Security to check device health continuously

The screenshot shows the Sophos Status window with the following content:

- SOPHOS** logo and navigation tabs: Status (highlighted), Events, Detections, Settings.
- Your device is protected** (indicated by a green checkmark icon).
- No malware or PUAs** (indicated by a shield icon) with a **Scan** button.
- Zero Trust Network Access : Configured** (indicated by a ZT icon).

ZTNA Demo





Recycle Bin



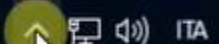
Google Chrome



Type here to search



45°F Partly sunny



12:56 PM



Recycle Bin



SophosTest...



Microsoft Edge



SophosTester



FileZillaPor...



SophosSetup



ZTNA Compa...



ztna



detections



ubuntu-ser...



SRBsample



detections



Ubutnu-SS...



ChromeSe...



ZTNA 2 AWS Applicatio...



Google Chrome



kali.sophos...

kali - kali.sophoslab.it - Remote Desktop Connection

Login to kali



Session

username

password

OK

Cancel




SOPHOS Status Events Detections Admin sign-in

Threat detected
Please contact IT.

No malware or PUAs

Zero Trust Network Access : Configured
Authenticated User : letterio.laspada@sophoslab.it

Login to kali



Session:

username:

password:

OK Cancel

Microsoft Edge
SophosTester
FileZillaPor...
SophosSetup
ZTNA Compa...
ztna
detections
ubuntu-ser...
SRBsample
detections
Ubutnu-SS...
ChromeSe...
ZTNA 2 AWS Applicatio...
Google Chrome



SOPHOS Status Events Detections Admin sign-in

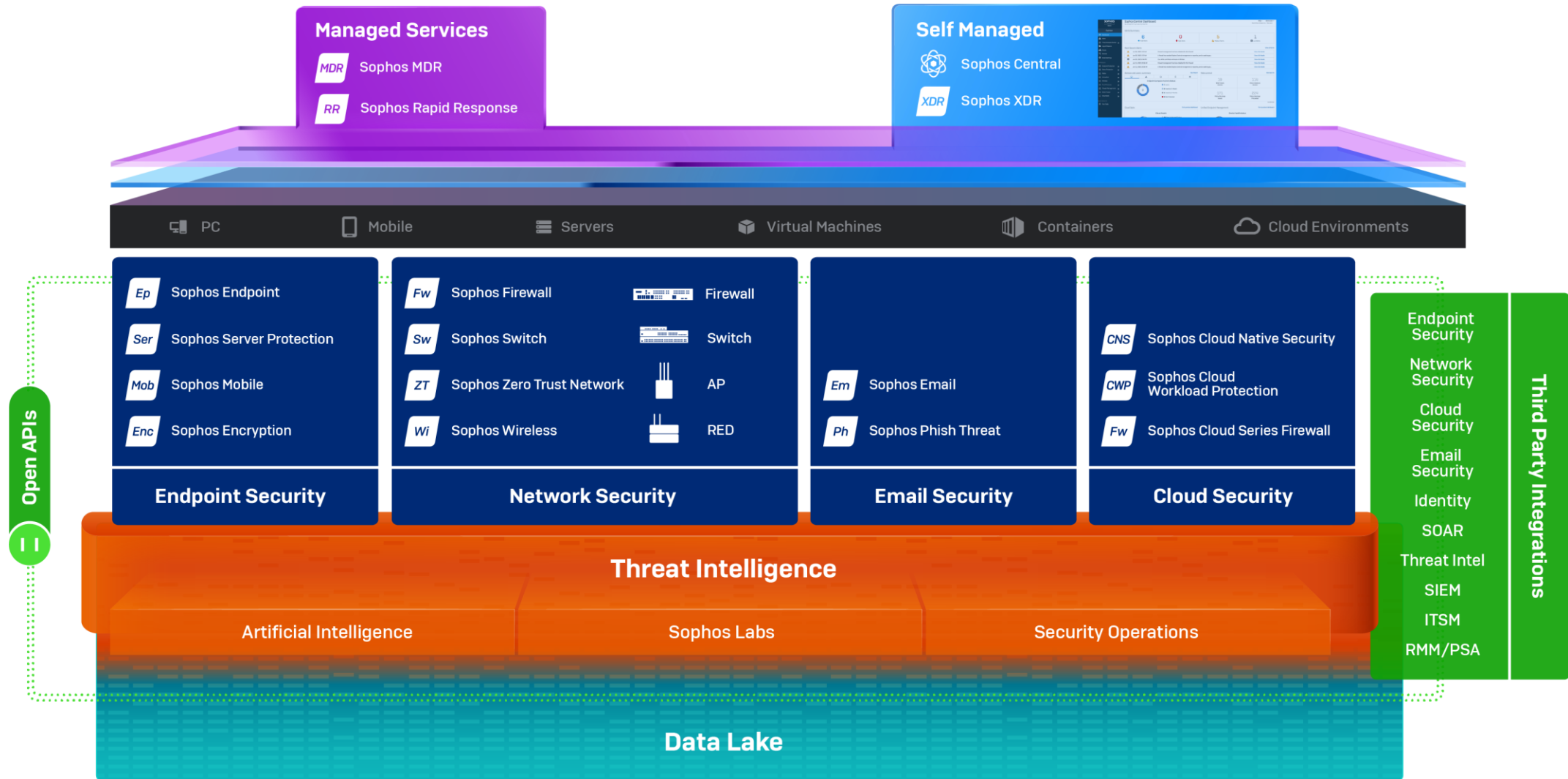
Your device is protected

No malware or PUAs Scan

Zero Trust Network Access : Configured
Authenticated User : letterio.laspada@sophoslab.it

Help | About

Adaptive Cybersecurity Ecosystem





MDR/NDR Roadmap

SOPHOS

Investing to deliver market leading solutions



Launch Sophos MDR	Launch Sophos NDR	Integrate Sophos Factory
<ul style="list-style-type: none">▪ NOW: MDR+NDR EAPs▪ NOW: MDR launch with 3rd party integrations▪ Next Year: Additional 3rd Party Integrations	<ul style="list-style-type: none">▪ NDR Sensor w/5 ML models to detect threats▪ HyperV Support to extend addressable market▪ Hardware appliance QA for 2023 release	<ul style="list-style-type: none">▪ Content and capabilities to support MTR and XDR via native Factory integration with Central

NSG Roadmap

Growing 500 user space (Distributed Enterprise)

SFOS 19.5 (H2 FY23)

SFOS 20 (H2 CY23)*



Networking and SD-WAN

- **SD-WAN Load Balancing** – across multiple SD-WAN links for maximum performance
- **Double IPsec capacity** – with current tunnel support now at 10,000 up from 4,650
- **Dynamic Routing** – with OSPFv3 (IP6) support and a new next-gen routing engine
- **5G LTE** – hardware module support for select XGS desktop models: XGS 116(w), 126(w), 136(w)



High Availability Enhancements

- **Status and Visibility** – with a new control center widget, enhanced status panel, and new node names for easy device identification
- **HA Link Redundancy** – supports up to 4 links for added redundancy
- **VLAN Support Enhancements** – for the dedicated HA link and VLAN interface monitoring



Networking and SD-WAN

- SD-WAN HTTPS Probing
- DHCP relay over xfrm interface
- IPsec connection stateful failover
- Route table segregation
- SD-WAN FEC Link Remediation
- DataCenter Interconnects (25E/50E/100GE)
- IPv6 Support – Logo ready, Dynamic Routing (BGPv6, PIPng) DHCP-PD, NAT64



High Availability Enhancements

- Faster HA failover
- Failover when a critical component or service fails
- Bring Aux in a real hot standby state (Services related to control plane)



Quality of Life Improvements

- **Hosts and Service Object Search** – using free text
- **Enhanced .log File Storage** – for better troubleshooting
- **Azure AD SSO** – for web console UI login authentication
- **Enhanced 40G Interface Support** – including auto-detection of advanced port configurations and breakout of 40G interfaces



Performance

- **TLS FastPath** – utilizing the Xstream Flow Processors in select XGS Series appliances to accelerate TLS traffic decryption for improved performance (XGS 4300, 4500, 5500, 6500)
- **XGS 7500/8500** – Setting a new benchmark for price-performance



Quality of Life Improvements

- Object reference
- Granular services controls in ACL
- Backup-restore enhancements – w/non-w, port mapping visibility
- Better firmware upgrade/downgrade
- Actionable alerts/notifications
- Enhanced log viewer
- Interface migration – easily migrate low speed interface to high speed



Ecosystem and Cross-Sell

- Pre-defined Sophos own facility resource
- Azure AD SSO – for captive portal and Sophos connect authentication
- Auto-import 3rd party threat feed
- Support Synchronized Security in a clustered HA environment

Network Security Strategy



Connect Anywhere Anyhow

- Enabling and consolidating form factor connectivity within a hybrid infrastructure
- SME friendly – while providing forward and backwards compatibility



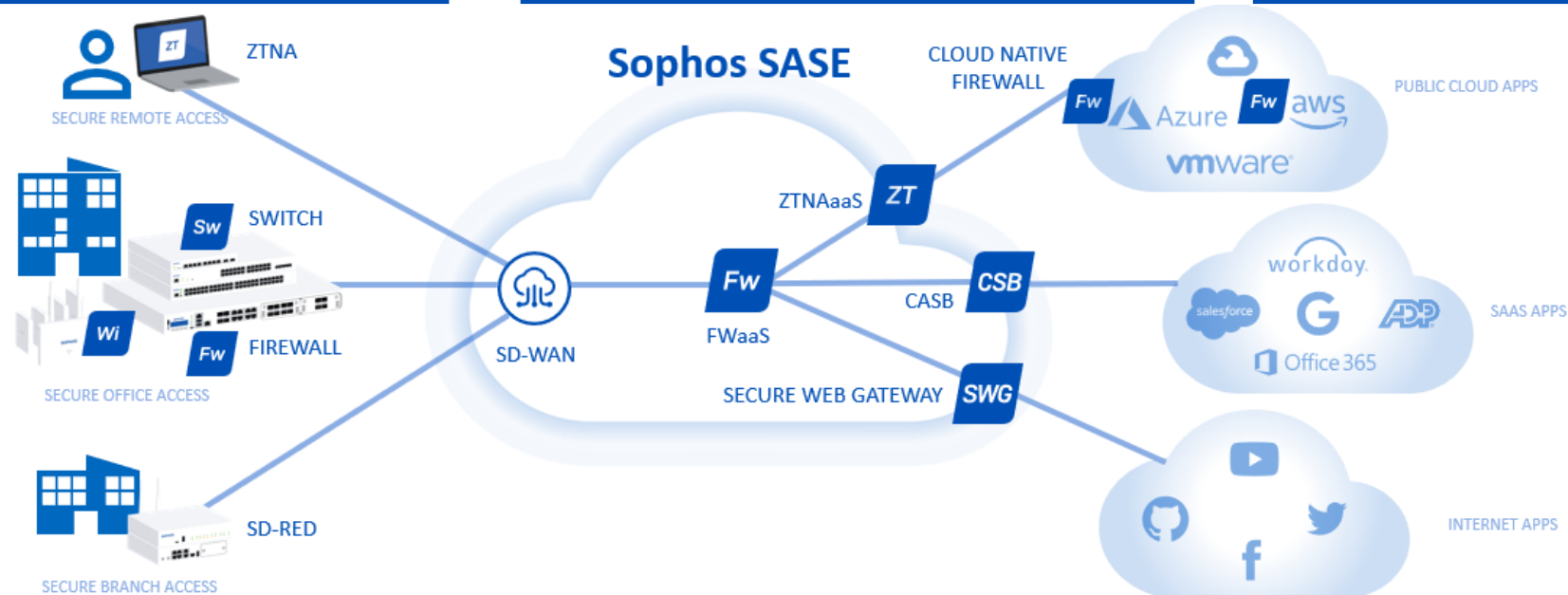
Set Policy Once – Enforce Everywhere

- Unifying security policies across multiple network security enforcement points
- Floating security that follows the user and business entity helping address the dynamic network



Powerful Protection

- Cross-Product threat detection and response for hybrid network deployments
- Providing powerful and layered protection for customer driven use cases (Network, SAAS, Cloud)



SOPHOS