TODAY'S WEBINAR

Cybersecurity as a Service: A Way to Achieve Superior Cybersecurity Outcomes ft Sophos

MicroAge®

cStor™
A MicroAge® Company

MicroAge®

ABOUT US

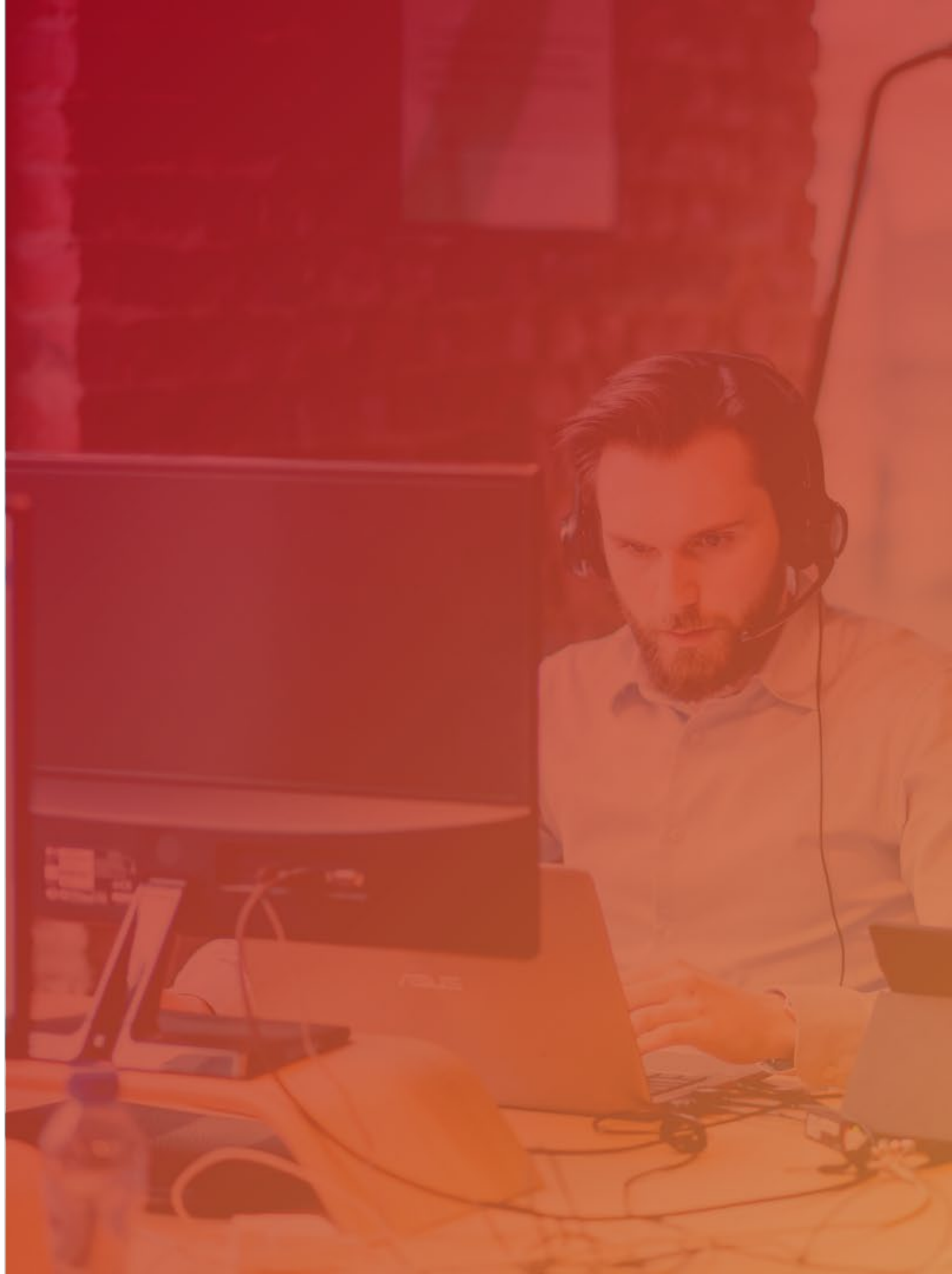
MicroAge is an award-winning technology solutions and services provider, specializing in IT services and cloud. For nearly five decades, MicroAge has empowered businesses to advance, secure, accelerate, and transform—moving quickly with technology changes to drive business forward.

Our consulting services division, cStor, serves as an elite team of specialized consultants who bring unique expertise to our clients in cybersecurity, data center, technology implementations, managed IT services, and more.

CERTIFICATIONS

At MicroAge, we empower our associates to keep learning to help you navigate your challenges. Our experts have experience and deep certifications including hundreds of partner certifications.

MicroAge has achieved **ISO 9001:2015** certification, demonstrating our commitment to maintaining quality systems and processes—ensuring our clients receive the best possible outcome.



INDUSTRIES

Every organization must transform into a technology company to remain competitive—no matter how you serve your customers. MicroAge supports organizations across verticals, brings deep expertise and professional certifications.

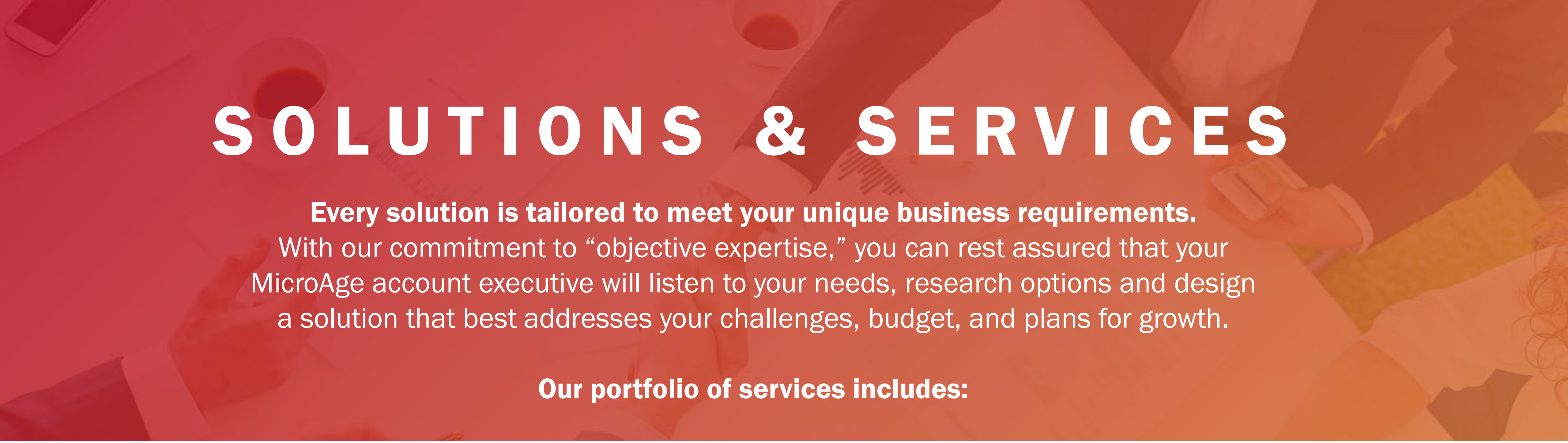
- Aerospace/Defense
- Agriculture/Farming
- Architectural/Engineering
- Commercial
- Communications/Telecom
- Construction
- Distribution
- Energy/Utilities
- Federal Government
- Financial/Banking
- Healthcare
- Higher Education
- Hospitality/Entertainment
- Insurance
- K-12 Education
- Legal
- Manufacturing
- Nonprofit
- Pharmaceuticals
- Real Estate
- Retail
- State & Local Government
- Technology
- Transportation/Logistics

SOLUTIONS & SERVICES

Every solution is tailored to meet your unique business requirements.
With our commitment to "objective expertise," you can rest assured that your MicroAge account executive will listen to your needs, research options and design a solution that best addresses your challenges, budget and plans for growth.

Our portfolio of services includes:

- Cloud
- Cybersecurity
- Data Center
- Data Migration
- Disaster Recovery
- Help Desk
- Hyper Converged Infrastructure
- Implementation
- IT Consulting
- Managed Services
- ManageWise
- Microsoft 365 & Azure
- Networking
- Power & Cooling
- Renewals & Contract Co-terming
- Software
- Staff Augmentation
- Storage
- Unified Communications
- Virtualization



SOLUTIONS & SERVICES

Every solution is tailored to meet your unique business requirements.
With our commitment to “objective expertise,” you can rest assured that your MicroAge account executive will listen to your needs, research options and design a solution that best addresses your challenges, budget, and plans for growth.

Our portfolio of services includes:

Cybersecurity

- Cloud
- Cybersecurity
- Data Center
- Data Migration
- Disaster Recovery
- Help Desk
- Hyper Converged Infrastructure
- Implementation
- IT Consulting
- Managed Services
- ManageWise
- Microsoft 365 & Azure
- Networking
- Power & Cooling
- Renewals & Contract Co-terming
- Software
- Staff Augmentation
- Storage
- Unified Communications
- Virtualization

PLEASE WELCOME

Mike Weaver

Channel West Sales Engineer

MicroAge®

cStor™
A MicroAge Company

Sophos MDR

Manage Detection and Response

Delivering Superior Security Outcomes Through Cybersecurity as a Service

Mike Weaver – Channel West Sr. Sales Engineer

mike.weaver@sophos.com

The Cybersecurity Challenge

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

Cyberthreats Are Accelerating in Volume and Sophistication

- 57% of organizations report an increase in the number of attacks over the past year[1]
- **78% increase** in the number of organizations hit by ransomware last year[1]
- "It's nearly impossible for organizations to outrun threat actors and keep themselves, their customers, and employees safe" – IDG

Cybersecurity Tools Are Overwhelmingly Costly and Complex

- The average organization has more than **46 cybersecurity monitoring tools** in place
- Most sec ops teams are **drowning in alerts**
- The average organization spends $7.5K on cybersecurity per employee[2]

Hiring and Retaining Cybersecurity Experts Has Become Fiercely Competitive

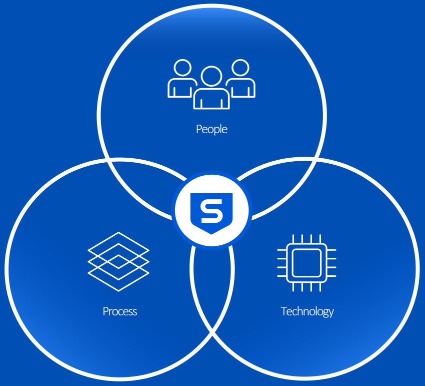
- The number of unfilled cybersecurity jobs worldwide **grew 350%** between 2013 and 2021
- In the US there are 1 million cybersecurity workers and **750,000 cybersecurity openings**
- Security Analysts cost $100-150K per year, and the annual cost to maintain a SOC is $2.86M[3]

[1] The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos
[2] Statista: https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3] Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"

The Solution: Cybersecurity as a Service - MDR

MANAGED DETECTION AND RESPONSE

Superior security outcomes delivered as a service

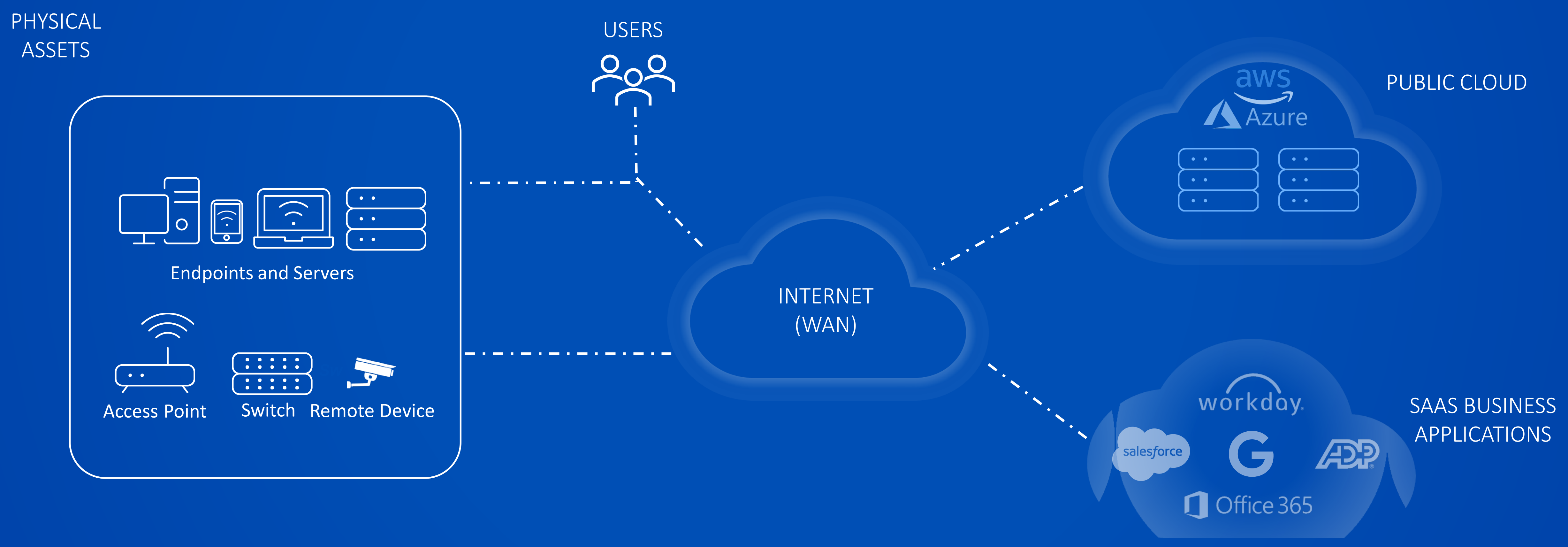


A fully-managed, 24/7 service delivered by over 500 threat experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent

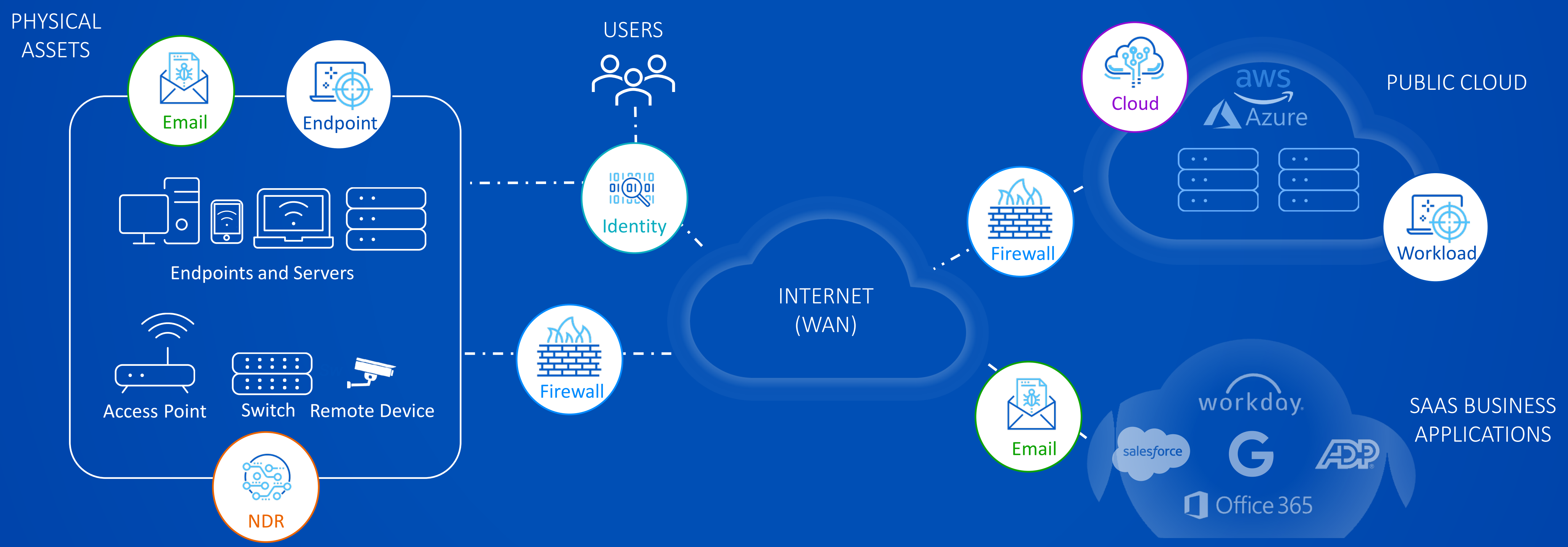
- ✓ **Instant Security Operations Center (SOC)**
- ✓ **24/7 Threat Detection and Response**
- ✓ **Expert-Led Threat Hunting**
- ✓ **Full-Scale Incident Response Capabilities**
- ✓ **Superior Cybersecurity Outcomes**

So how does MDR work?

Today’s Environments are Complex and Dispersed



Security Tools Are Deployed Across the Environment



SOPHOS

Each Tool Plays an Important Role in Identifying Threats

ENDPOINT

Detect suspicious activity and malware

FIREWALL

Detect intrusion attempts and beaconing

IDENTITY

Detect unauthorized network entry and privilege escalation

EMAIL

Pinpoint initial entry and attempts to steal access data

CLOUD

Indicate unauthorized network access and efforts to steal data

NETWORK

Identify rogue assets, unprotected devices and novel attacks

Combining Insights Accelerates Detection and Response

ENDPOINT + FIREWALL

- ➡ EP: Unknown process execution on 10.0.0.33
- ✚ FW: DLP Prevention on 10.0.0.33
- ✚ FW: Non-standard port usage on 10.0.0.33

INSIGHT: Data exfiltration attempts to be occurring on 10.0.0.33.

NETWORK + ENDPOINT

- ➡ NDR: Device communicating on the internal network
- ✚ EP: No known device under management

INSIGHT: Unmanaged device communicating on the network.

EMAIL + ENDPOINT + IDENTITY

- ➡ EM: Suspected phishing email in user's inbox
- ✚ EP: Suspicious file download
- ✚ EP: Unexpected access to lsass.exe
- ✚ ID: Abnormal location login to O365
- ✚ EM: Forwarding rule to external account created

INSIGHT: Successful phishing email has resulted in unauthorized access and potential Business Email Compromise

But Joining the Telemetry Up Is Incredibly Hard

Firewall Vendor A

```
<11>Aug 9 08:03:28 TDG-CDNDCFW01.CUSTOMER.ca CEF:0|VENDORA|VENDORA|9.1.10|MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553)|THREAT|4|rt=Aug
09 2022 13:03:27 GMT deviceExternalId=001701010750 src=45.58.21.70 dst=216.55.21.147 sourceTranslatedAddress=45.58.21.70 destinationTranslatedAddress=10.200.150.90 cs1Label=Rule
cs1=Outside-DMZ1-chatbot.tdg-dsg.com suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Outside cs5Label=Destination Zone cs5=DMZ_01
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ae2 cs6Label=LogProfile cs6=SOC.OS Agent cn1Label=SessionID cn1=447900 cnt=1 spt=36935 dpt=80 sourceTranslatedPort=36935
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x80412000 proto=tcp act=alert request="shell" cs2Label=URL Category cs2=license-expired flexString2Label=Direction
flexString2=client-to-server VENDORAActionFlags=0x2000000000000 externalId=12412496 cat=MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553)
fileId=12075418355151190 VENDORADGl1=0 VENDORADGl2=0 VENDORADGl3=0 VENDORADGl4=0 VENDORAVsysName= dvchost=TDG-CDCFW01 VENDORASrcUUID= VENDORADstUUID=
VENDORATunnelID=0 VENDORAMonitorTag= VENDORAParentSessionID=0 VENDORAParentStartTime= VENDORATunnelType=N/A VENDORAThreatCategory=code-execution
VENDORAContentVer=AppThreat-8585-7440 VENDORAAssocID=0 VENDORAPPID=4294967295 VENDORAHTTPHeader= VENDORAURLCatList= VENDORARuleUUID=62dbe5-718d-401-aa37-
b90540f748 VENDORAHTTP2Con=0 PanDynamicUsrgrp=
```

Firewall Vendor B

```
Sep 02 19:09:50 Firewall_Device CEF:0|Vendor B|Vendor B|vB|16384|utm:ips signature dropped|7|deviceExternalId=XG1Y5D3Z14803090 VENDORBlogid=1412013380 cat=utm:ips
VENDORBsubtype=ips VENDORBeventtype=signature VENDORBlevel=alert VENDORBvd=CUST-1 VENDORBseverity=high src=121.168.96.40 VENDORBsrccountry=COUNTRY dst=192.18.96.3
deviceInboundInterface=XYZ Primary VENDORBsrcintfrole=undefined deviceOutboundInterface=port20 VENDORBdstintfrole=undefined externalId=1861272610 act=dropped proto=6 app=HTTP
VENDORBpolicyid=88 VENDORBattack=vBulletin.Routestring.widgetConfig.Remote.Code.Execution spt=54430 dpt=80 dhost=192.18.96.3 deviceDirection=1 VENDORBattackid=48398
VENDORBprofile=Default IPS VENDORBref=http://www.vendorb.com/ids/4898 VENDORBincidentserialno=1672537750 msg=applications3:
vBulletin.Routestring.widgetConfig.Remote.Code.Execution, VENDORBcrscore=50 VENDORBcrlevel=critical VENDORBeventtime=16306090
```

Firewall Vendor C

```
AUG 16 2022 05:55:10 18B1694226F4 CEF:0|VENDORC|VENDORC FW SERIES|6.5.4.5-53|138|TCP Null Flag Attack|9|cat=32 gcat=3 smac=dc:f7:19:8:b8sd: src=9.234.15.254 spt=40942
deviceInboundInterface=X2 cs3Label=Untrusted dmac=1:b1:9:42:2:f6 dst=19.74.191.24 dpt=8073 proto=tcp/8073 in=60 cs6="TCP Flag(s): None" cnt=225 fw_action="drop"
```

But Joining the Telemetry Up Is Incredibly Hard

Firewall Telemetry

```
<11>Aug 9 08:03:28 TDG-CDNDCFW01.CUSTOMER.ca CEF:0|VENDORA|VENDORA|9.1.10|MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553)|THREAT|4|rt=Aug
09 2022 13:03:27 GMT deviceExternalId=001701010750 src=45.58.21.70 dst=216.55.21.147 sourceTranslatedAddress=45.58.21.70 destinationTranslatedAddress=10.200.150.90 cs1Label=Rule
cs1=Outside-DMZ1-chatbot.tdg-dsg.com suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Outside cs5Label=Destination Zone cs5=DMZ_01
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ae2 cs6Label=LogProfile cs6=SOC.OS Agent cn1Label=SessionID cn1=447900 cnt=1 spt=36935 dpt=80 sourceTranslatedPort=36935
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x80412000 proto=tcp act=alert request="shell" cs2Label=URL Category cs2=license-expired flexString2Label=Direction
flexString2=client-to-server VENDORAActionFlags=0x2000000000000 externalId=12412496 cat=MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553)
fileId=1207541835515119O VENDORADGl1=0 VENDORADGl2=0 VENDORADGl3=0 VENDORADGl4=0 VENDORAVsysName= dvchost=TDG-CDCFW01 VENDORASrcUUID= VENDORADstUUID=
VENDORATunnelID=0 VENDORAMonitorTag= VENDORAParentSessionID=0 VENDORAParentStartTime= VENDORATunnelType=N/A VENDORAThreatCategory=code-execution
VENDORAContentVer=AppThreat-8585-7440 VENDORAAssocID=0 VENDORAPPID=4294967295 VENDORAHTTPHeader= VENDORAURLCatList= VENDORARuleUUID=62dbe5-718d-401-aa37-
b90540f748 VENDORAHTTP2Con=0 PanDynamicUsrgrp=
```

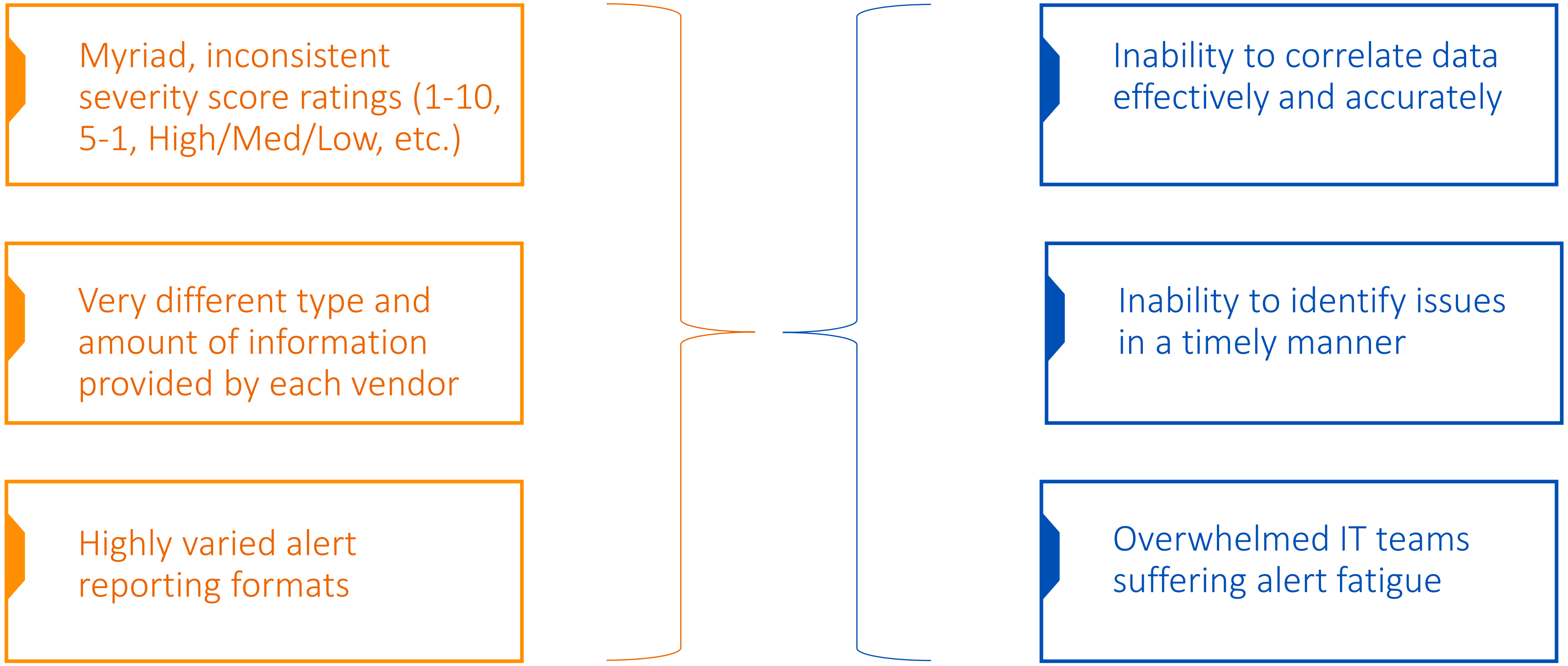
Email Telemetry

{"senderAddress":“**SENDER.NAME@XXXX.com**","**recipientAddress":“FIRST.LAST@XXXXX.com**","**fileName":"Factura_RSS190815AN5_8613_XEXX010101000.pdf**","fileType":"application/pdf","re
sult":"safe","**actionTriggered":"none, none"**,"date":"2022-10-06T03:09:12+0000","details":"Safe \r\nTime taken: 0 hrs, 0 min, 26 sec", "route":"inbound",
"messageId":"<SA1PR13MB4976F328D68BF6D1B7560BA6845C9@SA1PR13MB4976.namprd13.prod.outlook.com>",“subject":"ROCKA Specialty - Universal Lighting Virtual Septiembre
2022","fileHash":"9f1e0a25cb3b08d417bdced2ea226e010d76822420fd8265b8935668ddb4344a","**definition":"Default Attachment Protection**"}

Identity Telemetry

{"access_device":{"browser":"Edge","browser_version":"18.19044","epkey":"EPQ0KD7N0H1AJJ5IZRS4","flash_version":"uninstalled","hostname":null,"**ip":"194.8.207.139**","is_encryption_enable
d":"unknown","is_firewall_enabled":"unknown","is_password_set":"unknown","java_version":"uninstalled","location":{"city":"Hürth","country":"Germany","state":"North Rhine-
Westphalia"},"os":"Windows","os_version":"10","security_agents":"unknown"}, "alias":"","application":{"key":"DIHUCR02IM4WOZQGGOEP","name":"Sophos Trusted Endpoint"},"auth_device“
:{"ip":null,"location":{"city":null,"country":null,"state":null},"name":null},"**email":“FIRST.LAST@sophos.com**","event_type":"authentication","factor":"not_available","isotimestamp":"2022-06-
09T11:59:24.424377+00:00","ood_software":null,"**reason":"endpoint_is_not_trusted**", **"result":"denied**","timestamp":1654775964,"trusted_endpoint_status":"not trusted","txid":"05558fa5-
0145-4454-9aa5-8060493c41a2","user":{"groups":["AAD-DUOMFAUsers (from Azure sync \"Sophos Ltd\")"],"key":"DU9MZJV4IVSSZN49JGYT","**name":“FIRST.LAST**"}}

But Joining the Telemetry Up Is Incredibly Hard



Myriad, inconsistent severity score ratings (1-10, 5-1, High/Med/Low, etc.)

Very different type and amount of information provided by each vendor

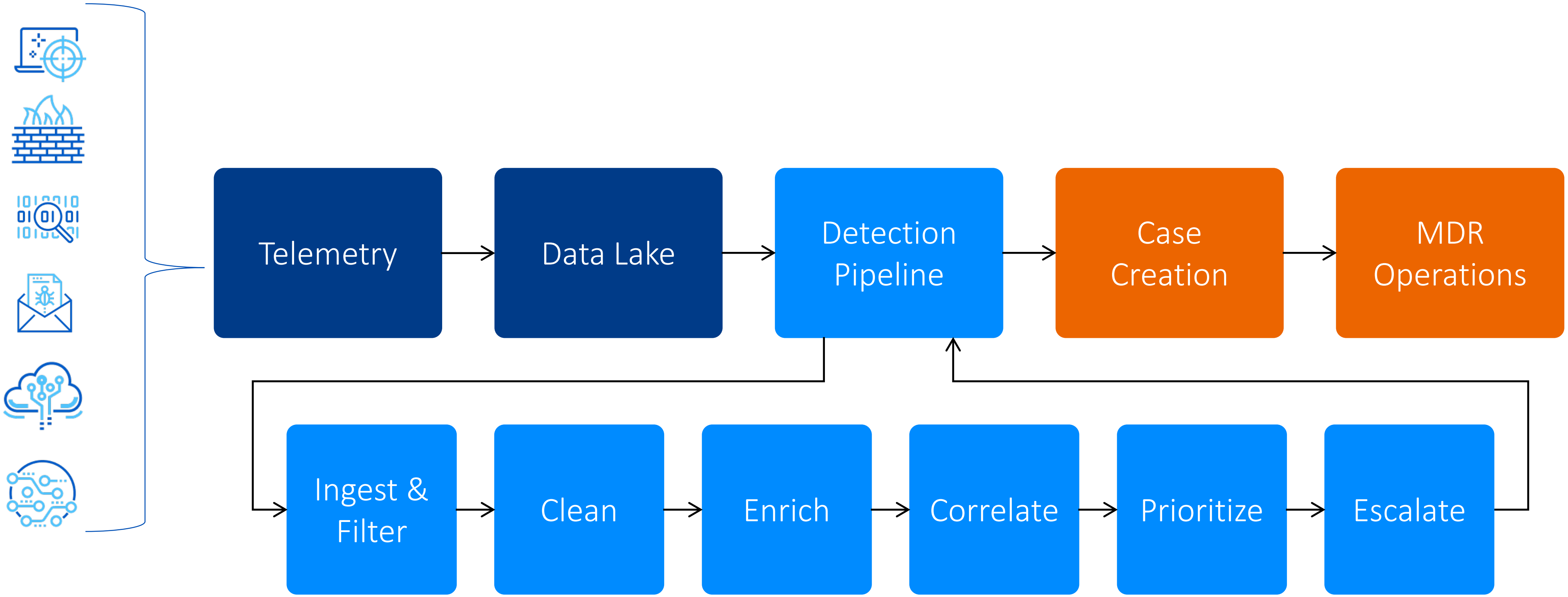
Highly varied alert reporting formats

Inability to correlate data effectively and accurately

Inability to identify issues in a timely manner

Overwhelmed IT teams suffering alert fatigue

How We Do It: Sophos MDR Security Event Flow



Telemetry

Data Lake

Detection Pipeline

Case Creation

MDR Operations

Ingest & Filter

Clean

Enrich

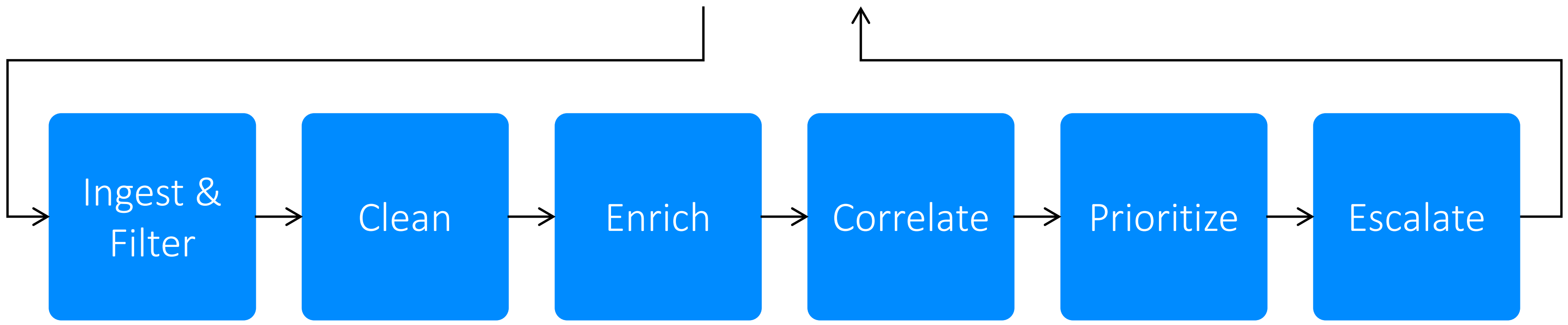
Correlate

Prioritize

Escalate

SOPHOS

Deep Dive into the Detection Pipeline



- **Ingest and Filter** – Ingest telemetry and filter unwanted noise
- **Clean** – Transform data into normalized schema and map to MITRE ATT&CK®
- **Enrich** – Add additional 3rd party threat intelligence and business context information
- **Correlate** – Cluster alerts based on entities, MITRE ATT&CK categorization, and time
- **Prioritize** – Score alerts and clusters to rank in order of prioritization
- **Escalate** – Logic that escalates certain clusters into cases for investigation

MDR Provider see something. Now What?

Threat Response vs. Incident Response

THREAT RESPONSE

The act of **containing** a threat to **disrupt** malicious activity

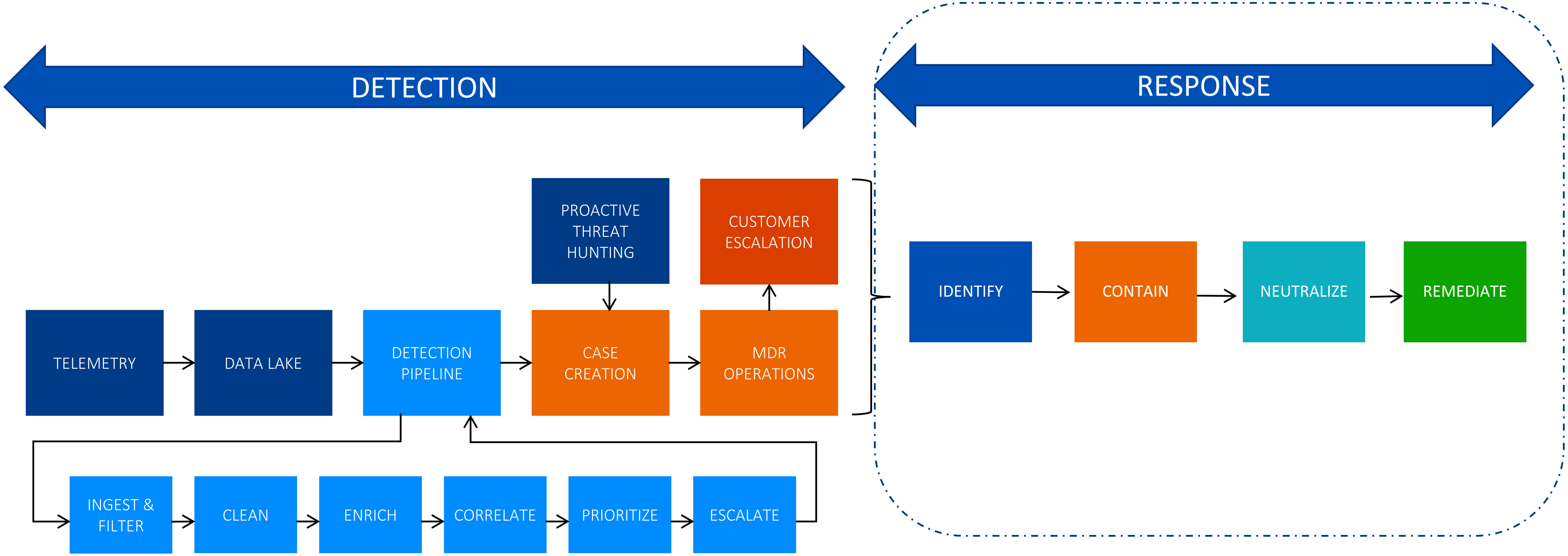
Goal: To prevent propagation and escalation of the attack and mitigate the risk of a threat elevating to an incident.

INCIDENT RESPONSE

The act of **removing an attacker** from the environment and **fully remediating** the threat

Goal: To determine the root cause, timeline and full scope of attack activity to ensure the adversary is fully removed from the environment. To provide retrospective guidance that can be implemented to mitigate the risk of a similar attack in the future.

Sophos MDR Workflow



Response Actions: Identify

IDENTIFY	**ACT: Identify** where an incident occurred, how it was discovered, the scope and business impact. **RECOMMEND:** Customer actions to increase insights

Response Actions: Contain

IDENTIFY

ACT: Identify where an incident occurred, how it was discovered, the scope and business impact.

RECOMMEND: Customer actions to increase insights

CONTAIN

ACT: Isolate, if possible, the *issues* and the *impacted systems* to prevent further damage. Remove all malware and artifacts.

RECOMMEND: Actions on customer-managed technologies

Common Threat Actor Tools and TTPs

- PowerShell
- Command and Control
- Malicious Files
- Persistence

Common Sophos MDR Disruption Techniques

- Isolate Device
- Remove Threat Artifact
- Disable User Account
- Kill Process

Common Customer Disruption Techniques

- Reset User Password(s)
- Suspend Account
- Isolate Device
- Block C2 Artifact
- Network Segmentation

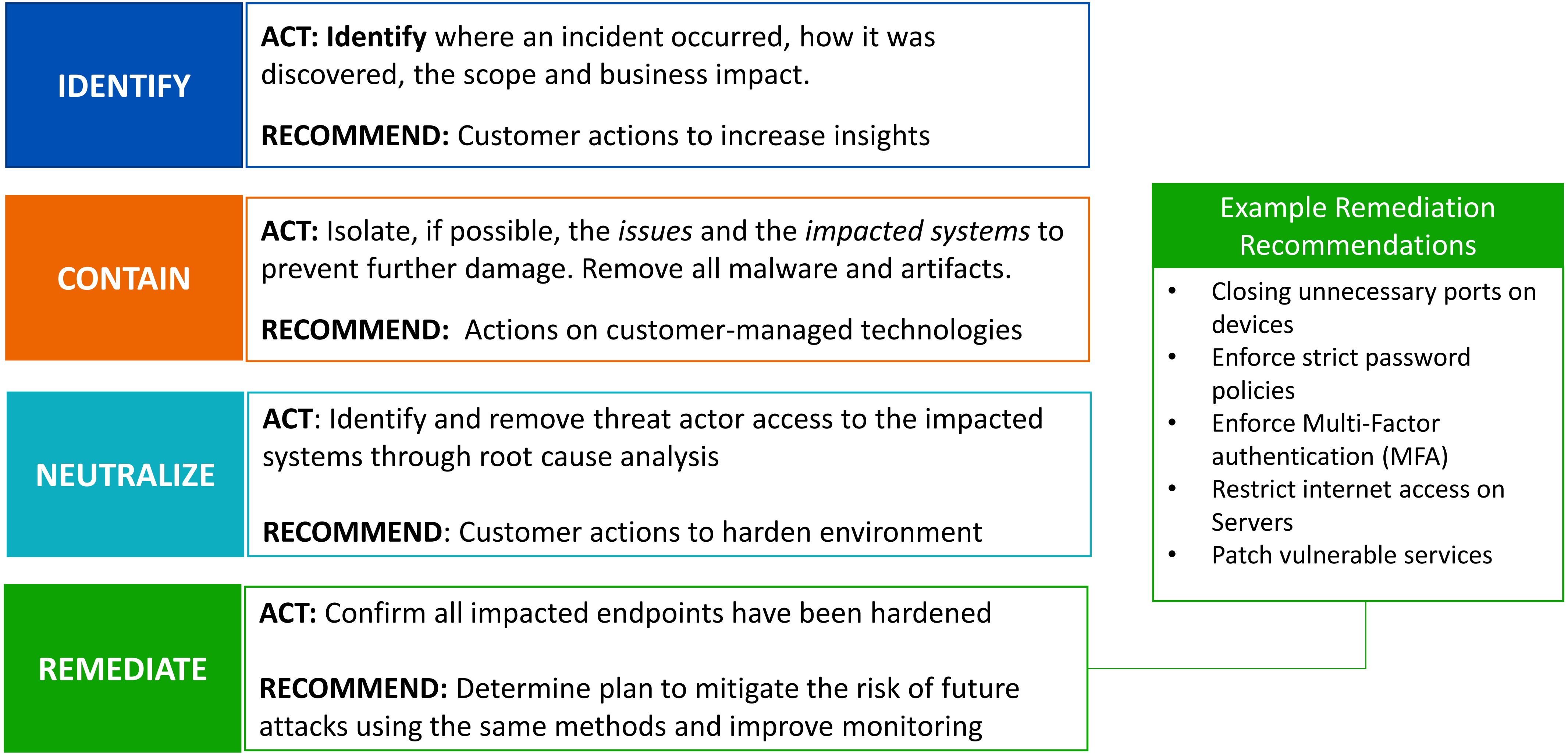
Response Actions: Neutralize

IDENTIFY	**ACT: Identify** where an incident occurred, how it was discovered, the scope and business impact. **RECOMMEND:** Customer actions to increase insights
CONTAIN	**ACT:** Isolate, if possible, the *issues* and the *impacted systems* to prevent further damage. Remove all malware and artifacts. **RECOMMEND:** Actions on customer-managed technologies
NEUTRALIZE	**ACT**: Identify and remove threat actor access to the impacted systems through root cause analysis **RECOMMEND**: Customer actions to harden environment

Root Cause Analysis includes:

- Initial Access and Delivery Method
- Patient Zero
- Incident Scope
- Incident Activity Timeline

Response Actions: Remediate



IDENTIFY

ACT: Identify where an incident occurred, how it was discovered, the scope and business impact.

RECOMMEND: Customer actions to increase insights

CONTAIN

ACT: Isolate, if possible, the *issues* and the *impacted systems* to prevent further damage. Remove all malware and artifacts.

RECOMMEND: Actions on customer-managed technologies

NEUTRALIZE

ACT: Identify and remove threat actor access to the impacted systems through root cause analysis

RECOMMEND: Customer actions to harden environment

REMEDIATE

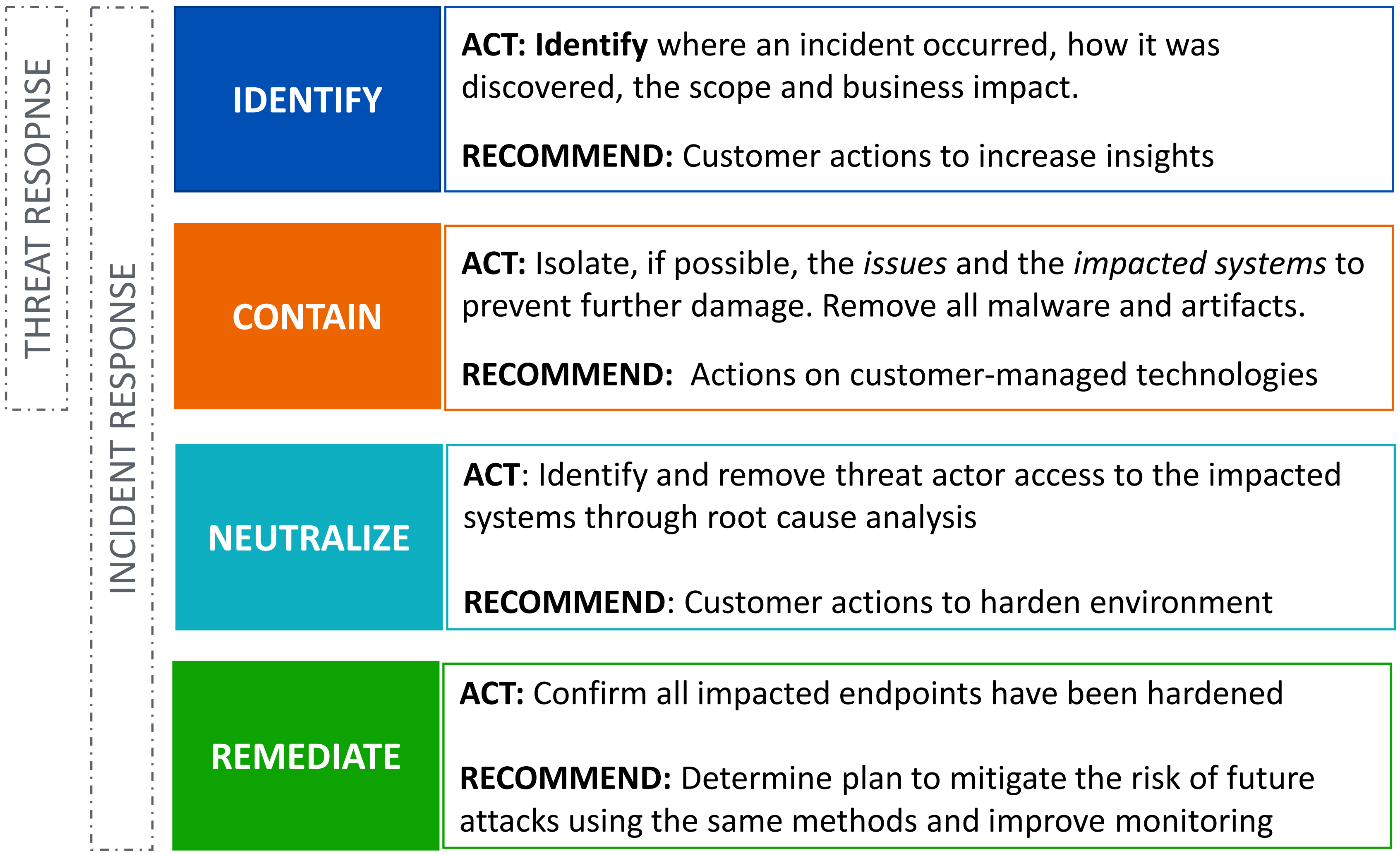
ACT: Confirm all impacted endpoints have been hardened

RECOMMEND: Determine plan to mitigate the risk of future attacks using the same methods and improve monitoring

Example Remediation Recommendations

- Closing unnecessary ports on devices
- Enforce strict password policies
- Enforce Multi-Factor authentication (MFA)
- Restrict internet access on Servers
- Patch vulnerable services

Threat Response vs. Incident Response



THREAT RESOPNSE

INCIDENT RESPONSE

IDENTIFY

ACT: Identify where an incident occurred, how it was discovered, the scope and business impact.

RECOMMEND: Customer actions to increase insights

CONTAIN

ACT: Isolate, if possible, the *issues* and the *impacted systems* to prevent further damage. Remove all malware and artifacts.

RECOMMEND: Actions on customer-managed technologies

NEUTRALIZE

ACT: Identify and remove threat actor access to the impacted systems through root cause analysis

RECOMMEND: Customer actions to harden environment

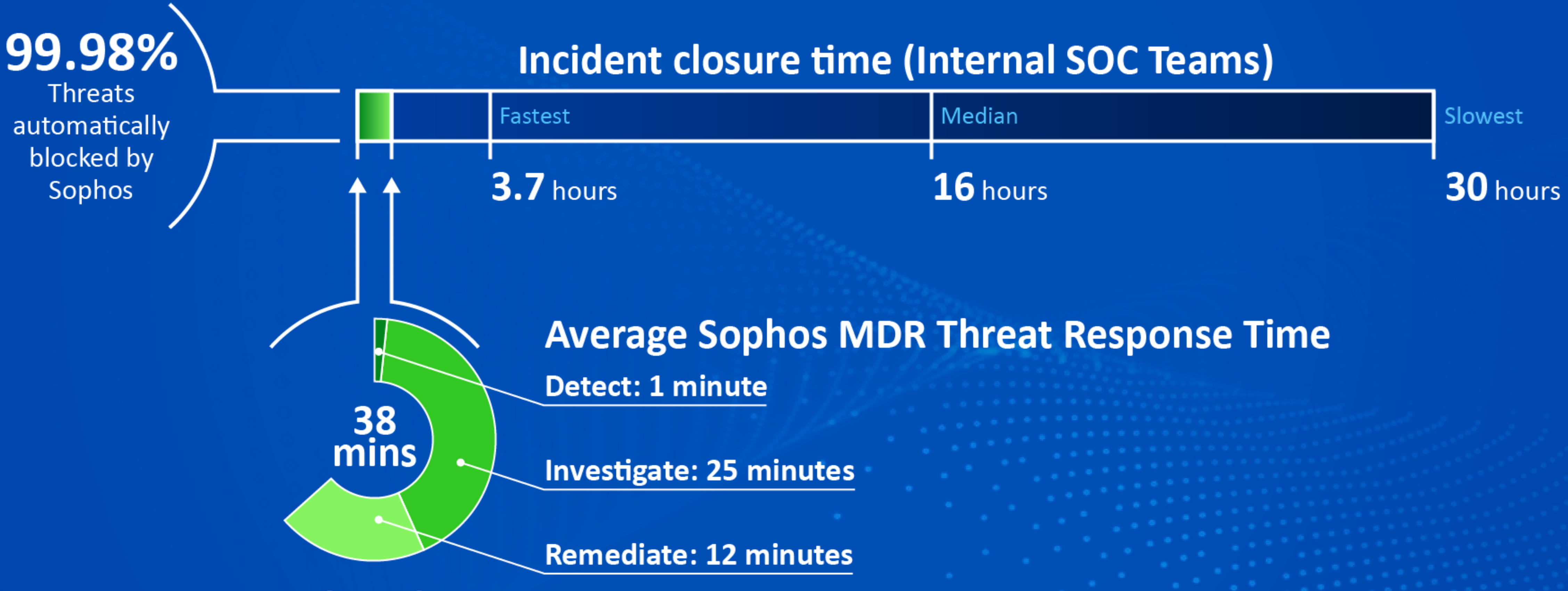
REMEDIATE

ACT: Confirm all impacted endpoints have been hardened

RECOMMEND: Determine plan to mitigate the risk of future attacks using the same methods and improve monitoring

Partnering with Sophos and MicroAge

Leading Detection and Response Times



99.98% Threats automatically blocked by Sophos

Incident closure time (Internal SOC Teams)

Average Sophos MDR Threat Response Time

Detect: 1 minute

Investigate: 25 minutes

Remediate: 12 minutes

SOPHOS

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

ARCTIC WOLF · red canary · eSENTIRE · expel · Secureworks

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

CROWDSTRIKE · SentinelOne · Microsoft · RAPID7 · cybereason

MDR 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 MDR Service Tiers

	Sophos MDR Essentials	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 Threat Cast”	✓	✓
Sophos Account Health Check	✓	✓
Expert-led threat hunting	✓	✓
Threat Response: active attacks are stopped and contained Uses full Sophos XDR Agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)	✓	✓
Direct call-in support during active incidents	✓	✓
Root Cause Analysis: performed to prevent future recurrence		✓
Full-scale Incident Response: threats are fully eliminated Requires full Sophos XDR sensor (protection, detection and response)		✓
Dedicated Incident Response Lead		✓
Sophos Breach Protection Warranty		✓

Sophos MDR Included Integrations

XDR Sophos XDR

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

Fw Sophos Firewall

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

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Ep Sophos Endpoint Protection

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

NDR Sophos Network Detection and Response

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

Third-Party Endpoint Protection

Compatible with...

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

Cld Sophos Cloud

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

Em Sophos Email

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

90-Days Data Retention

Sophos MDR Add-On Integrations

Firewall

Compatible with...

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

Public Cloud

Compatible with...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identity

Compatible with...

- Okta
- Duo

Network Security

Compatible with...

- Darktrace
- Forcepoint
- McAfee (web gateway)

Email

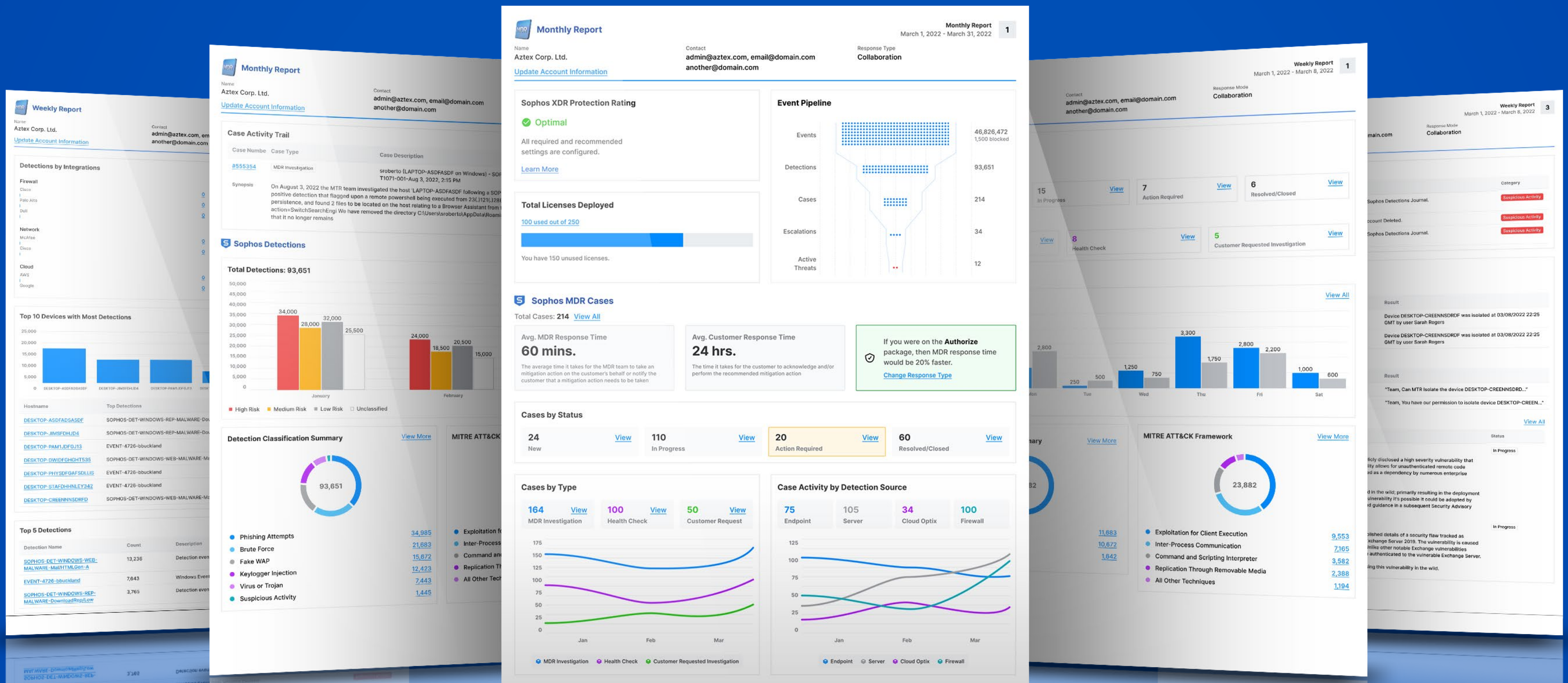
Compatible with...

- Proofpoint
- Mimecast

1-Year Data Retention

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

Monthly and Weekly Cybersecurity Reports



Monthly Report

Monthly Report
March 1, 2022 - March 31, 2022 | 1

Name
Aztex Corp. Ltd.
Update Account Information

Contact
admin@aztex.com, email@domain.com
another@domain.com

Response Type
Collaboration

Sophos XDR Protection Rating

Optimal

All required and recommended settings are configured.

Learn More

Total Licenses Deployed

100 used out of 250

You have 150 unused licenses.

Event Pipeline

Events	46,826,472 1,500 blocked
Detections	93,651
Cases	214
Escalations	34
Active Threats	12

Sophos MDR Cases

Total Cases: **214** View All

Avg. MDR Response Time
60 mins.
The average time it takes for the MDR team to take an mitigation action on the customer's behalf or notify the customer that a mitigation action needs to be taken

Avg. Customer Response Time
24 hrs.
The time it takes for the customer to acknowledge and/or perform the recommended mitigation action

If you were on the **Authorize** package, then MDR response time would be 20% faster.
Change Response Type

Cases by Status

24 New	110 In Progress	20 Action Required	60 Resolved/Closed

Cases by Type

164 MDR Investigation	100 Health Check	50 Customer Request

Case Activity by Detection Source

75 Endpoint	105 Server	34 Cloud Optix	100 Firewall

Sophos Breach Protection Warranty

At Sophos, we make your cybersecurity our responsibility. The Sophos Breach Protection Warranty is included at no additional charge with our Sophos MDR Complete subscription. It covers up to $1 million in response expenses for qualifying customers.

Trusted Protection for Complete Peace of Mind

More organizations trust Sophos for MDR than any other security vendor. With the Sophos Breach Protection Warranty, Sophos MDR Complete customers enjoy the reassurance and peace of mind that comes with having financial coverage if a breach happens.

Clear, Comprehensive Coverage

- Automatically provided – no need to apply
- Included with one-, two-, and three-year subscriptions
- Included with new and renewal license purchases
- Covers endpoints, servers, and devices running Windows and macOS
- No warranty tiers that restrict coverage
- No additional license purchase requirements

Included with Sophos MDR Complete

The warranty is included automatically and at no additional charge with new purchases or renewals of Sophos MDR Complete annual subscriptions. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

Up to $1 Million in Response Expenses

The warranty covers response expenses following a ransomware incident within an environment protected by Sophos MDR Complete:

- Up to $1,000 per breached machine
- Up to $1 million in total response expenses
- Up to $100,000 ransom payment (as part of per-device limit)

Reflecting the reality of today’s operating environments, breached machines include endpoints, servers, and Windows and macOS devices. The warranty covers a wide range of incurred expenses, including data breach notification, PR, legal, and compliance.

Warranty Overview

- Up to $1 million in total response expenses
- Up to $100,000 for ransom payment (as part of per-device limit)
- Up to $1,000 per breached machine
- Covers a range of incurred expenses, including data breach notification, PR, legal, and compliance

For full terms and conditions of the warranty, visit www.sophos.com/legal

Sophos MDR for Microsoft Defender

93%

find the execution of essential security tasks challenging

Identifying the different signals is a complex task

Defenders then need to apply insights and threat intelligence to understand the best course of action

Microsoft Event Title	Event Type
Suspicious URL clicked	Initial Access
Malicious files or network connections associated with the 3CXDesktopApp.exe process	Malware
New User Account Created	Persistence
TS_BL_Suspicious Eventlog Clear or Configuration Using Wevtutil	Defense Evasion
Process privilege escalation	Privilege Escalation
Attempt to turn off Microsoft Defender Antivirus protection	Defense Evasion
A file or network connection related to threat actor Storm-0867 detected	Credential Access
TS_BL_Script engines connecting to internet	Command and Control
Potential human-operated malicious activity	Suspicious Activity
TS_BL_Malicious Payload Download via Office Binaries	Execution
Emerging threat activity group DEV-0867 detected	Credential Access
Emerging threat activity group Citrine Sleet detected	Malware

Non-exhaustive list of MSFT Defender events

Sophos MDR for Microsoft Defender

Stop Advanced Threats with Microsoft + Sophos MDR

24/7 monitoring and response from a team of experts
Sophos MDR analysts monitor, prioritize, and respond to Microsoft Defender alerts 24/7, taking immediate action to stop confirmed threats

Detect and stop threats beyond Microsoft Defender
Proprietary Sophos detections, threat intelligence, and human-led threat hunts add additional layers of defense

Enhance visibility and contextualize Microsoft Defender alerts
Integrate additional Microsoft Security event sources included in your E3 or E5 license

Get immediate access to security operations experts
Sophos MDR analysts are available by phone 24/7, and detailed reporting on threat activity is available in Sophos Central

Microsoft Defender

Compatible with these Microsoft Security Event Sources

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Information Protection (Azure AD)
- MS O365 Security & Compliance Center
- Microsoft Azure Sentinel
- Office 365 Management Activity (unified audit logs)

Sophos MDR Service Tiers

	Sophos MDR for Microsoft Defender	
	Sophos MDR Essentials	**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 Response: active attacks are stopped and contained Uses full Sophos XDR Agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)	✓	✓
Direct call-in support during active incidents	✓	✓
Root Cause Analysis: performed to prevent future recurrence		✓
Full-scale Incident Response: threats are fully eliminated Requires full Sophos XDR sensor (protection, detection and response)		✓
Dedicated Incident Response Lead		✓
Sophos Breach Protection Warranty		✓

Your defenses can affect your Cybersecurity Insurance

Sophos Solutions Improve Insurability for U.S. Customers

cysurance

Automatic qualification for Sophos MDR users

- 4 fixed-price cyber insurance exclusively designed for Sophos MDR, providing up to $3.2M coverage
- Enhanced ransomware coverage included as standard
- All Sophos MDR customers in U.S. with up to $50M revenue automatically qualify for the fixed-price plans
- Custom quotes available for customers with higher annual revenue

cowbell®

Optimized pricing for Sophos Endpoint users

- Mutual customers can share their security posture with Cowbell via a custom Sophos Central connector
- Cowbell uses the insights to recognize and reward Sophos users' reduced cyber risk in their renewal offers
- Plus, Cowbell Prime 250 policyholders become eligible for a 5% premium credit when they enable the Cowbell Connector for Sophos Endpoint

Measured

Competitive pricing and coverage for Sophos EP users

- Customers who have implemented Sophos MDR or Sophos Endpoint products can reduce their cyber insurance premium by as much as 25%.
- Leverages Sophos Central APIs to assess security posture in Sophos Endpoint and create a customized risk report

Please note that Sophos is not a licensed insurance producer and does not sell, solicit or negotiate insurance products. By providing access to any third-party websites, Sophos is not recommending or endorsing any such third parties, or any products or services offered by such third parties. To the extent you access a third-party website from a Sophos website, please be advised that Sophos does not investigate, monitor, or check any third-party websites, or the content of such websites, for accuracy, appropriateness, or completeness, and you are solely responsible for your interactions with such third parties.

Gartner®
Peer Insights™

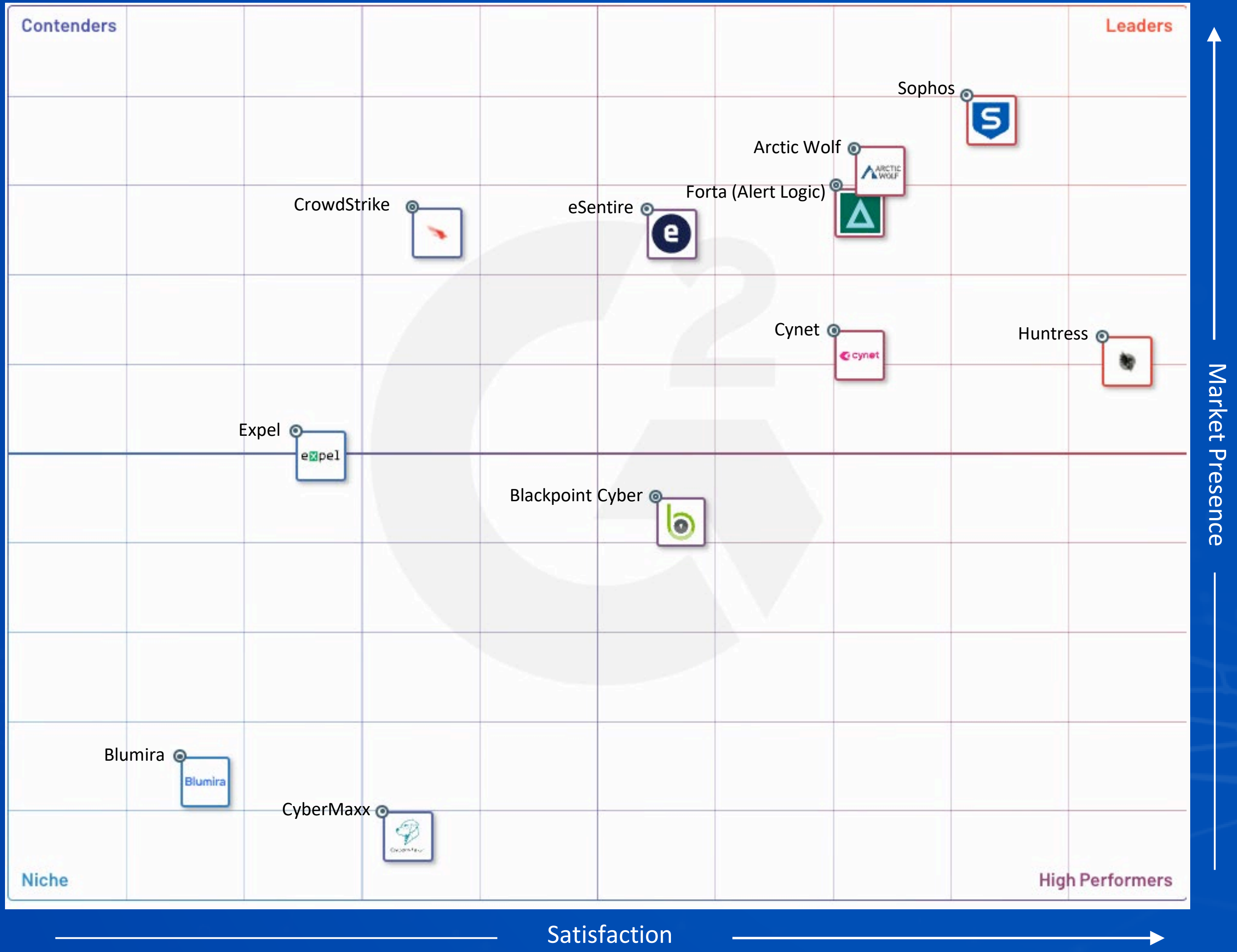
The **highest rated** and **most reviewed** solutions across MDR, Endpoint, and Firewall

Product	Average Rating	Would Recommend	Reviews	Competitor	Rating
MDR Sophos MDR	4.8	97%	Based on 256 Reviews	SentinelOne	4.5
				CrowdStrike	4.8*
				Arctic Wolf	4.8*
Ep Sophos Endpoint	4.8	95%	Based on 539 Reviews	Microsoft	4.4
				CrowdStrike	4.7
				Trend Micro	4.6
Fw Sophos Firewall	4.8	95%	Based on 362 Reviews	Fortinet	4.6
				Check Point	4.5
				Palo Alto Networks	4.5

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.

G2: A Leader in MDR Service Ratings



Sophos MDR is a **Leader** in the Overall, Mid-Market, and Enterprise segments

Rated the **Top Vendor** in the 2022 G2 Grid® for MDR Services serving the midmarket

2022 G2 Grid® for Managed Detection and Response (MDR) - Overall

SOPHOS

Cybersecurity delivered.

Q & A

MicroAge®

cStor
A MicroAge Company

CYBER WISE 2023 SCHEDULE

WEDNESDAY, SEP 13

Shielding Your Business: The Power of Proactive Managed Security Services from MicroAge

FEATURING

MicroAge®
Managed Security Services

THANK YOU

Mike Weaver
mike.weaver@sophos.com

MicroAge®

cStor™
A MicroAge Company