Prednosti uporabe MDR storitev z integracijo telemetrije drugih proizvajalcev

SOPHOS

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

72%

of organizations saw an increase in the volume/ complexity/impact of cyberattacks last year

69%

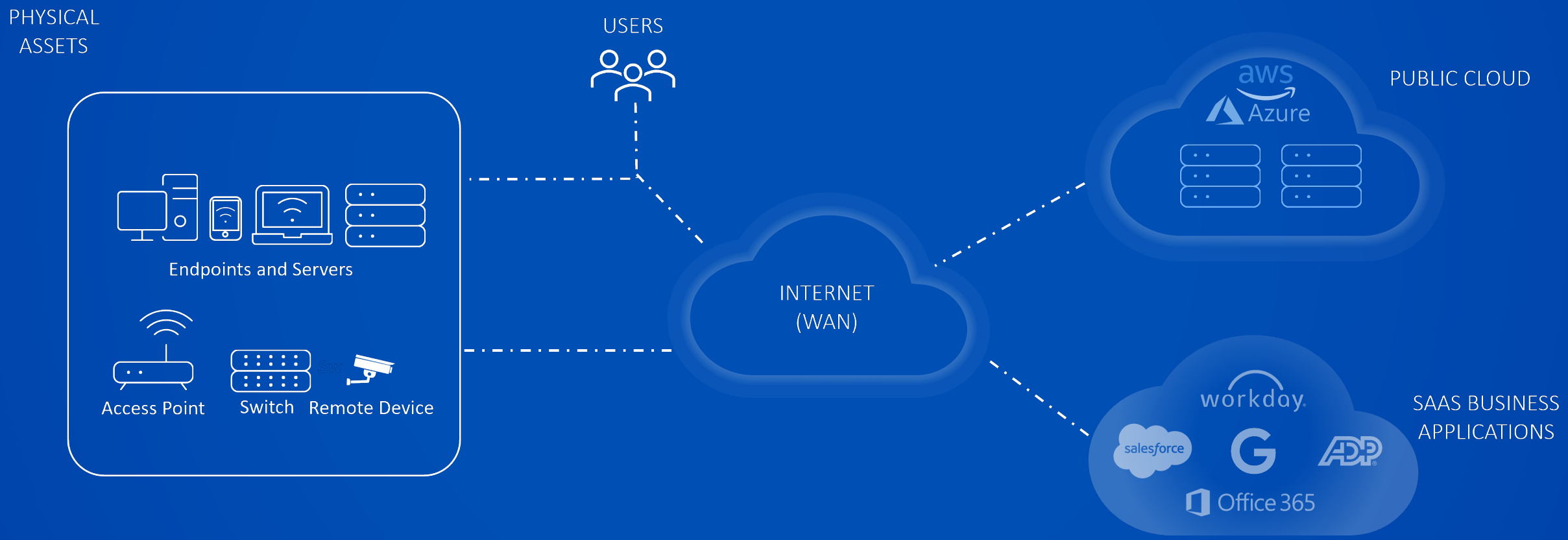
of IT pros have seen their cybersecurity workload increase over the last year

$1.4M

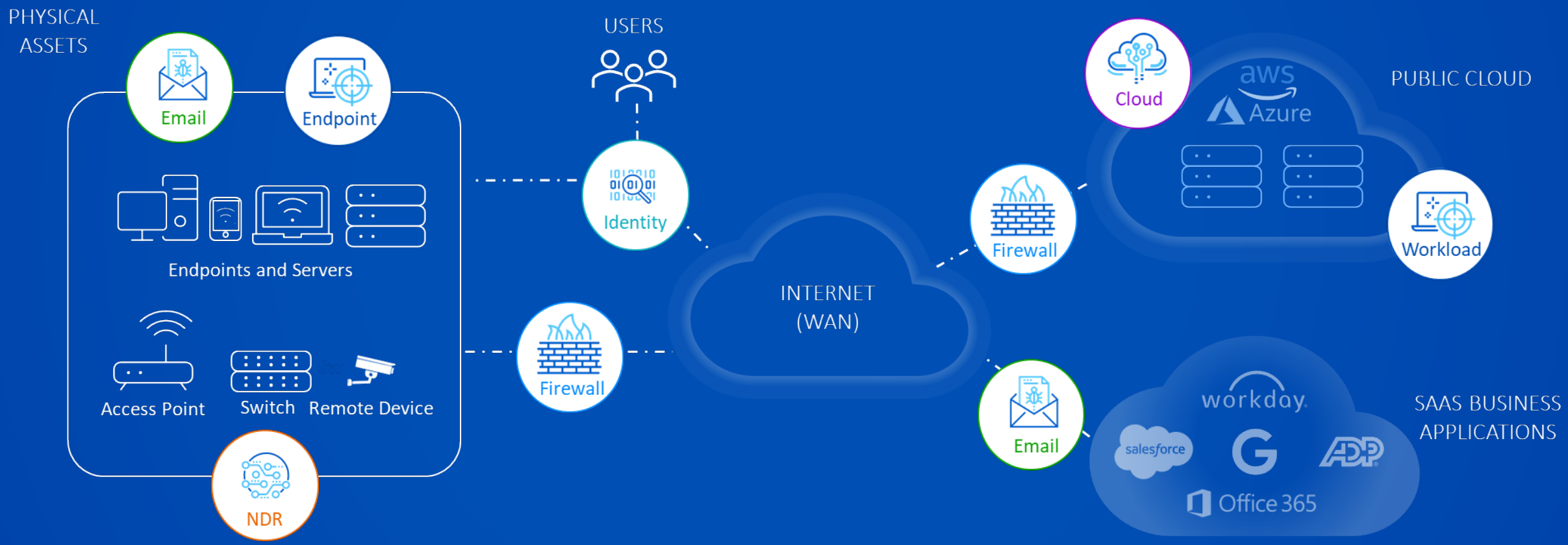
average ransomware remediation cost

SOPHOS

Today's Environments are Complex and Dispersed



Security Tools Are Deployed Across the Environment



SOPHOS

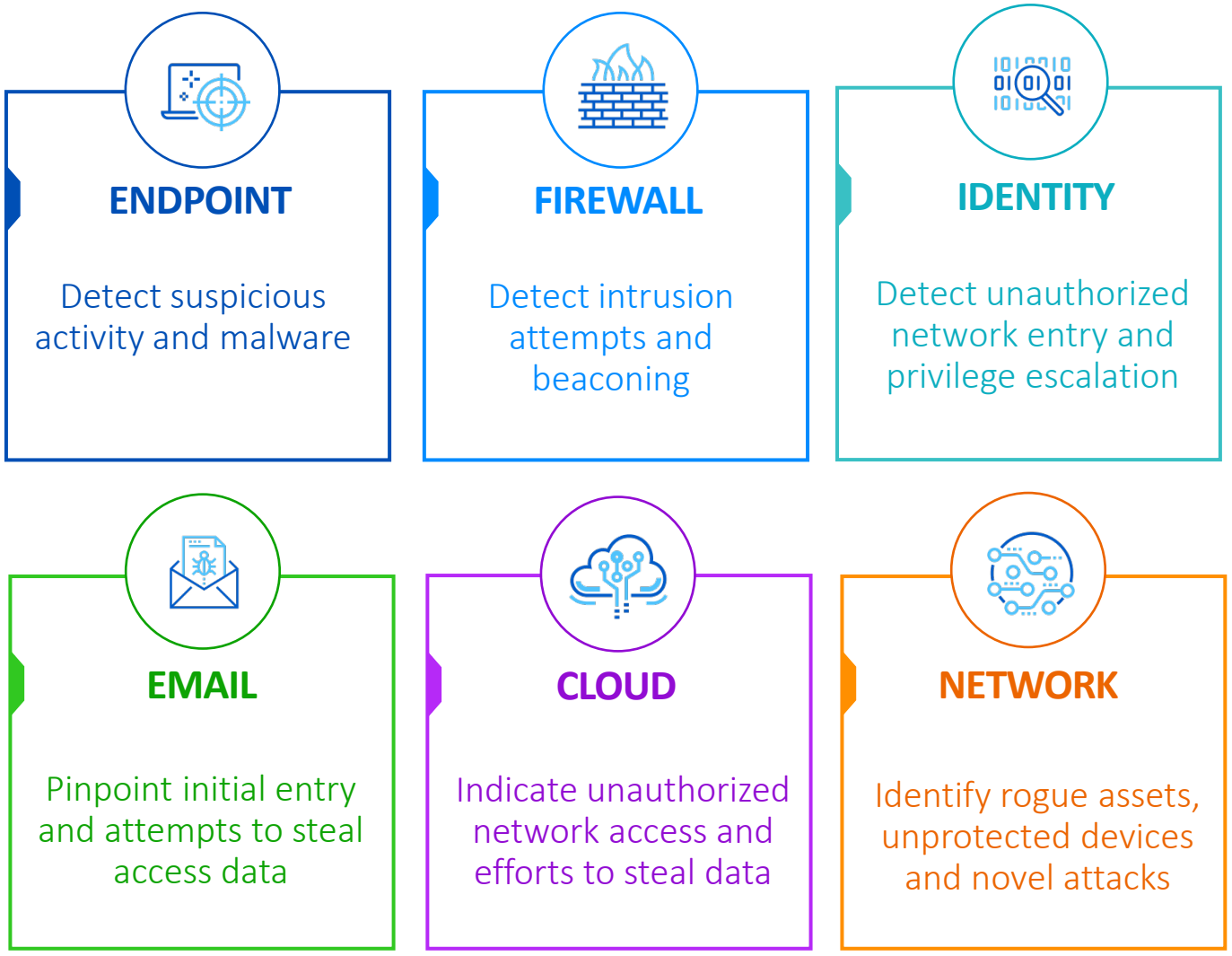
What is Managed Detection and Response (MDR)?

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

SOPHOS

SOC vs MDR

Each Tool Plays an Important Role in Identifying Threats



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

Leveraging the Telemetry Is Challenging

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=0x20000000000000 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=

EMAIL TELEMETRY

{"senderAddress":“**SENDER.NAME@XXXX.com**","**recipientAddress":“FIRST.LAST@XXXXX.com**","**fileName":"Factura_RSS190815AN5_8613_XEXX010101000.pdf**","fileType":"application/pdf","result":"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_enabled":"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**"}}

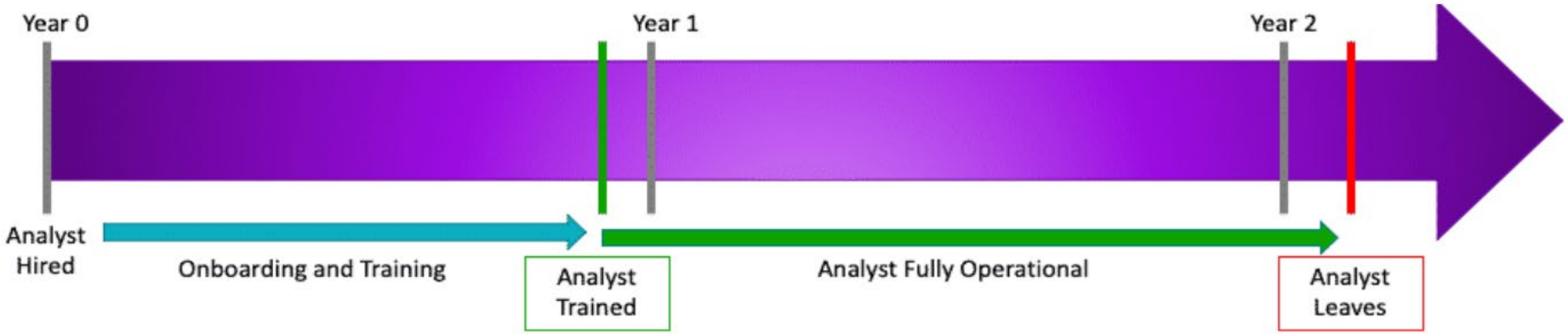
The Threat Landscape Today

The time to hire and train one analyst is almost one year and on average the analyst stays slightly more than two years.

$7.5K

Avg Org spends per employee on cybersecurity

Resource Intensive



3Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"

Threat Detection and response Process

Scenario 1: Spearphishing Attack

Attack Scenario

User opens a spearphishing email and clicks a link that downloads a malicious file

MITRE | ATT&CK®

TACTIC	Initial Access	Execution	Defense Evasion	Persistence
TECHNIQUE	Spearphishing Link	Malicious File	Process Injection	Schedule Task

▲ INITIAL DETECTION

Threat Containment Actions

- Isolate the affected user's device
- Remove the malicious file
- Remove the scheduled task
- Notify the customer of actions taken and provide remediation guidance

Incident Response and Root Cause Analysis

- Locate the spearphishing email/URL that delivered the malicious link/file used to execute the attack
- Investigate if other users received the spearphishing email associated with this attack
- Notify the customer and provide remediation guidance

Remediation Guidance

- Block the sending domain from the email client and/or email security product
- Reset the credentials of any users impacted by the attack

Scenario 2: Attempted Ransomware Deployment

Attack Scenario

Attacker uses a valid account to access a VPN, moves laterally through the environment, and attempts to deploy a ransomware payload via PsExec.

MITRE | ATT&CK®

TACTIC	Initial Access	Lateral Movement	Discovery	Execution	Impact
TECHNIQUE	External Remote Services	Remote Desktop Protocol	Domain Account	Service Execution	Data Encrypted for Impact

▲ INITIAL DETECTION

Threat Containment Actions

- Isolate the affected server
- Disable the affected account(s)
- Add any artifact to the blocked items list
- Terminate any actively running processes
- Notify the customer of actions taken and initiate **Incident Response**

Incident Response and Root Cause Analysis

- Initiate incident response procedures
- Identify and immediately begin triaging the device where activity originated from
- Perform analysis to identify any locations the compromised account accessed
- Request and review VPN logs if available to determine access location
- Perform malware analysis on any new payload

Remediation Guidance

- Perform domain wide password reset starting with administrative accounts
- Deploy AV estate-wide to all unprotected devices
- Modify policies to enforce best practices
- Implement MFA on the Remote VPN

Sophos MDR

Managed Detection and Response for Any Environment

Delivered using **natively integrated XDR**...

...or through highly compatible **hybrid XDR**

Sophos

- Sophos XDR
- Sophos Firewall
- Sophos Cloud
- Sophos Email
- Sophos NDR
- Sophos Endpoint

Endpoint

Microsoft, CrowdStrike, McAfee, SentinelOne, Check Point, Trend Micro, Malwarebytes, BlackBerry Cylance

Firewall

paloalto Networks, Fortinet, Check Point, Cisco, SonicWall

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

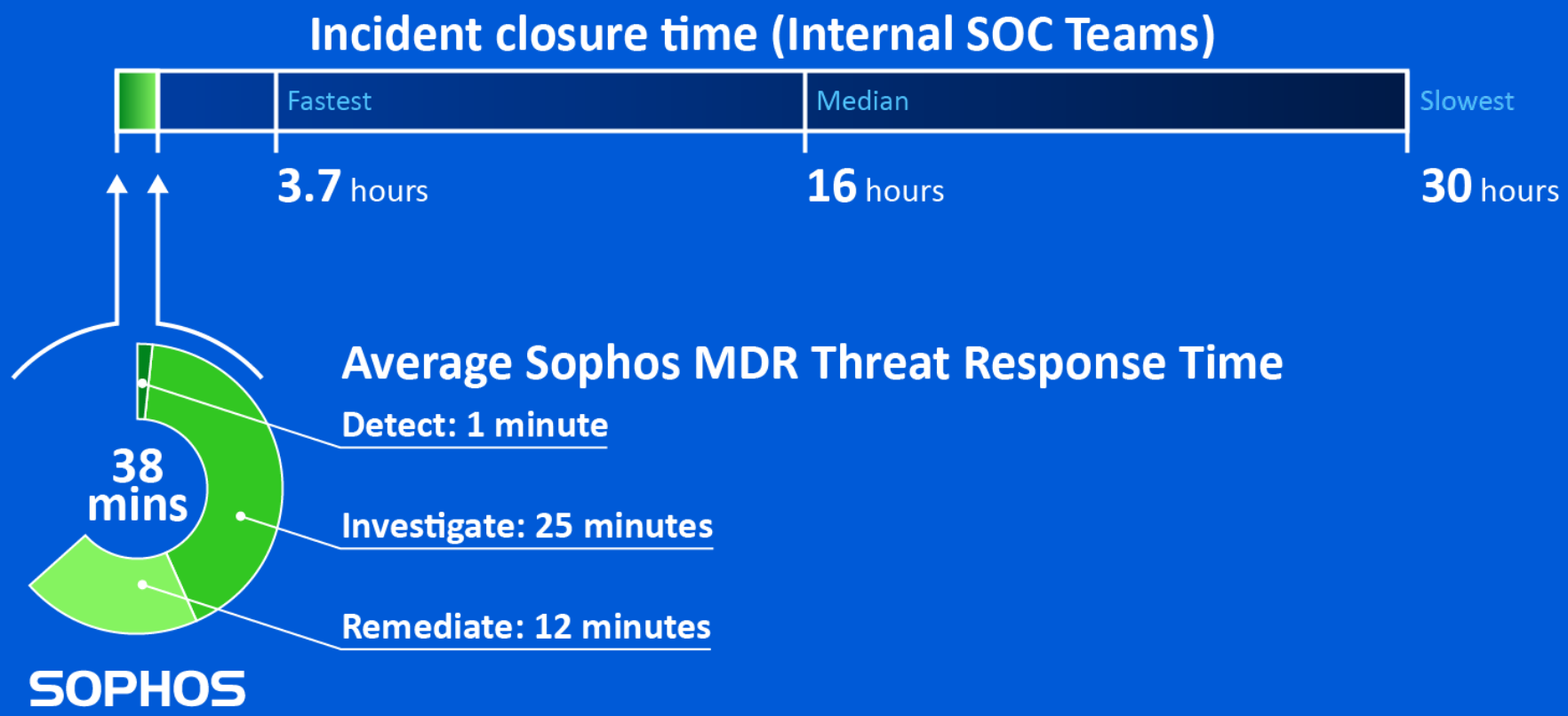
Microsoft [Azure IDP, ATA], okta, Duo

Network

DarkTrace, Forcepoint

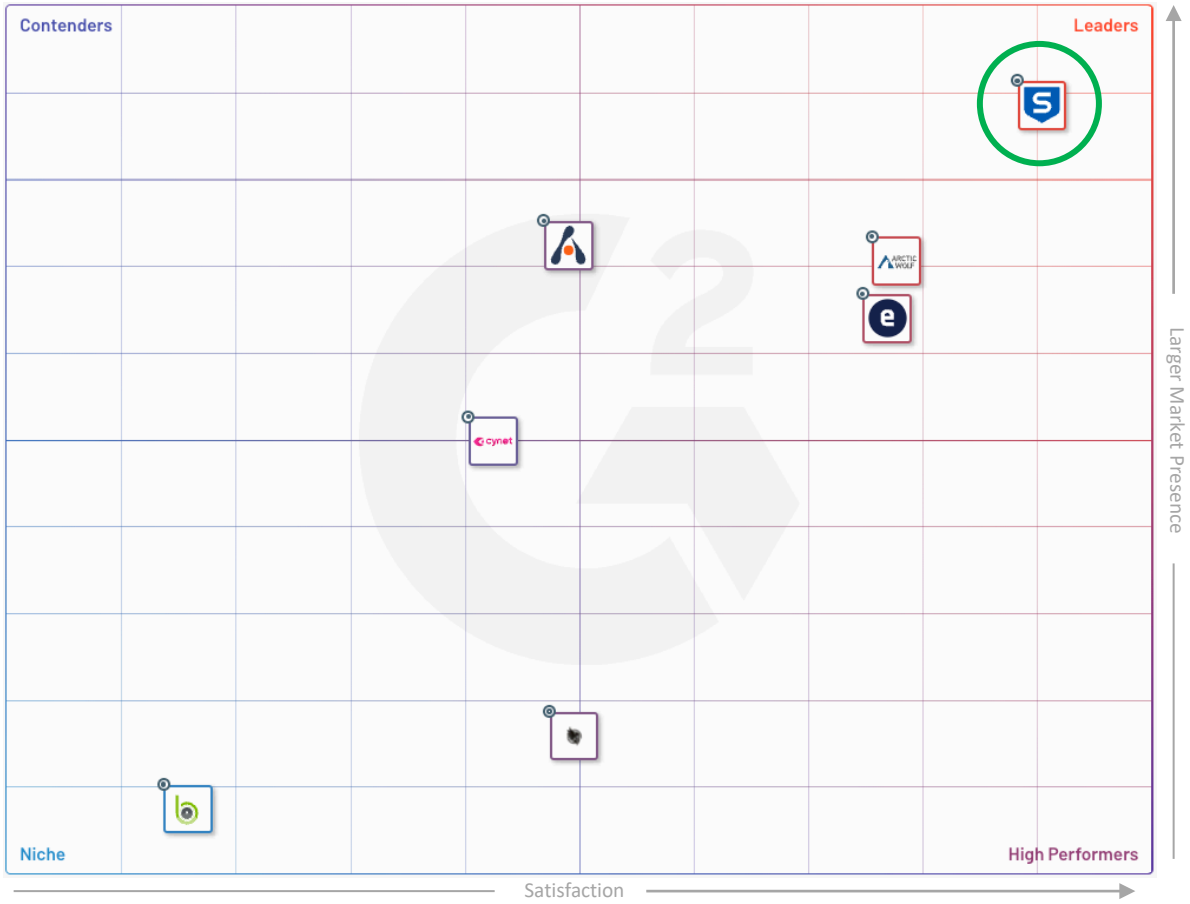
SOPHOS

World Leading Detection and Response Times



G2: MDR Service Ratings

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



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

Gartner
Peer Insights™

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

Sophos MDR

4.8
Average Rating

97%
Would Recommend

Based on 256 Reviews

Sophos Endpoint

4.8
Average Rating

95%
Would Recommend

Based on 539 Reviews

Sophos Firewall

4.8
Average Rating

95%
Would Recommend

Based on 362 Reviews

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

SOPHOS

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

SOPHOS

SOPHOS

Cybersecurity delivered.