Securing the Anywhere Organization

Any location, any device, any resource

Wana Tun

Global Solutions Engineer (CISSP, CEH, GNFA)

26th Feb 2021

SOPHOS

The World Has Changed: Workers Are Remote

Pre 7%

20%

33%

↑ 74% in 2010's

During 62%

Post 43%

10x increase in Sophos Connect VPN

74% some remote working

Gartner

The World Has Changed: Cloud Use Has Soared

CONSUMING

CLOUD-BASED APPLICATIONS

Jira [wiki]

CREATING

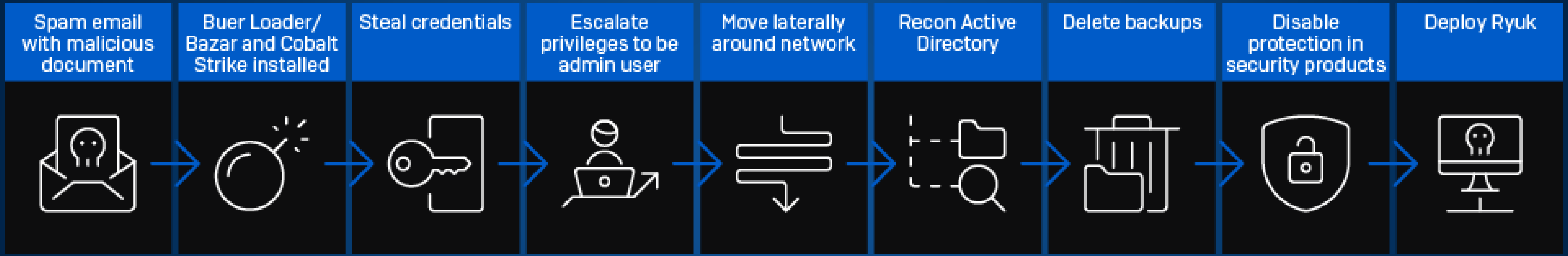
CLOUD INFRASTRUCTURE ENVIRONMENTS

aws

40%+ of the world’s data will be stored in hyperscale/cloud data centers by 2023

IDC

The World Has Changed: Attacks Are More Advanced


Spam email with malicious document
Buer Loader/ Bazar and Cobalt Strike installed
Steal credentials
Escalate privileges to be admin user
Move laterally around network
Recon Active Directory
Delete backups
Disable protection in security products
Deploy Ryuk

Ryuk ransomware attack kill chain

The World Has Changed: The Reality of Cyber Attacks

51%

hit by ransomware last year

73%

of ransomware attacks encrypted data

70%

had a cloud security incident in the last year

VansonBourne

SOPHOS

Today’s Challenge: Securing The Anywhere Organization

Any location	Secure connectivity
Any device	Secure computers, phones, tablets
Any resource	Secure data and workloads

SECURE CONNECTIVITY

Home

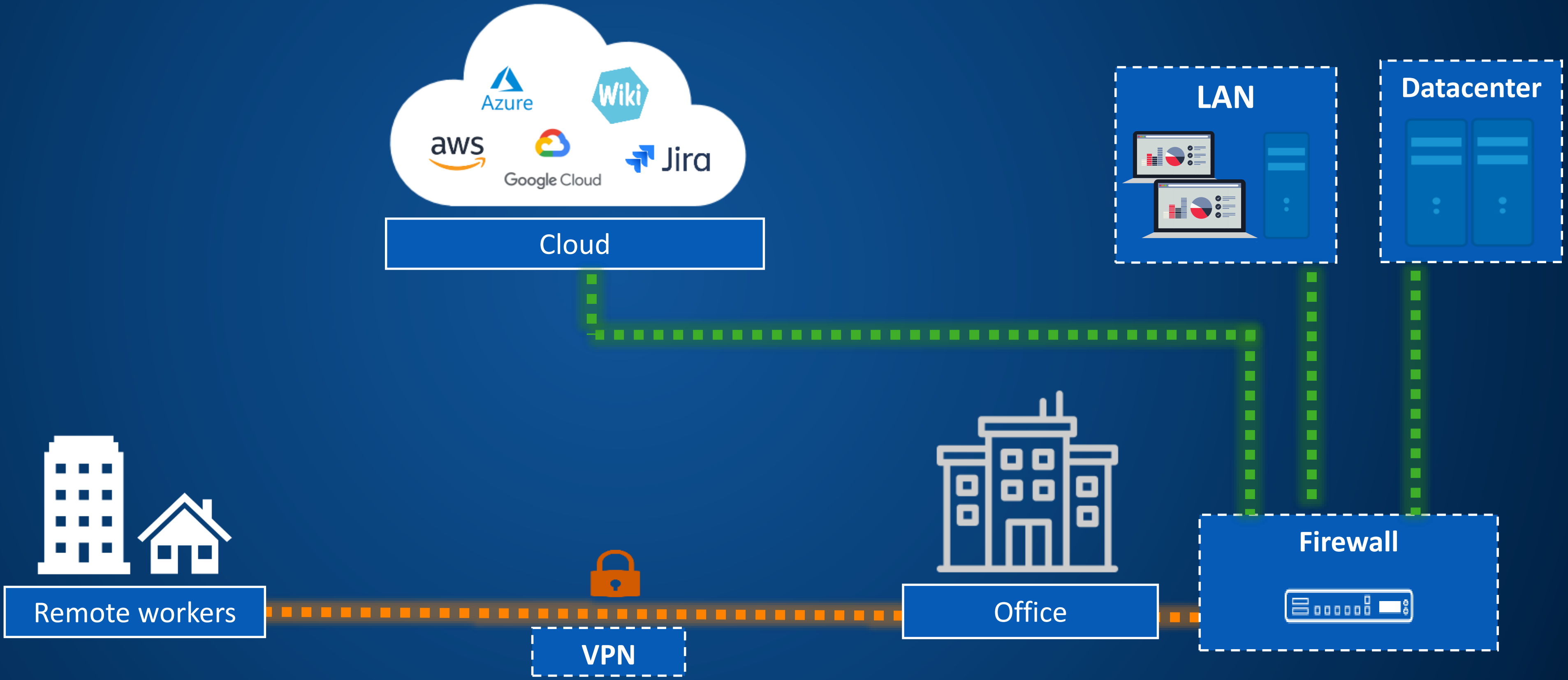
Office

Cafe

Customer Site

Car

Secure Access: VPN

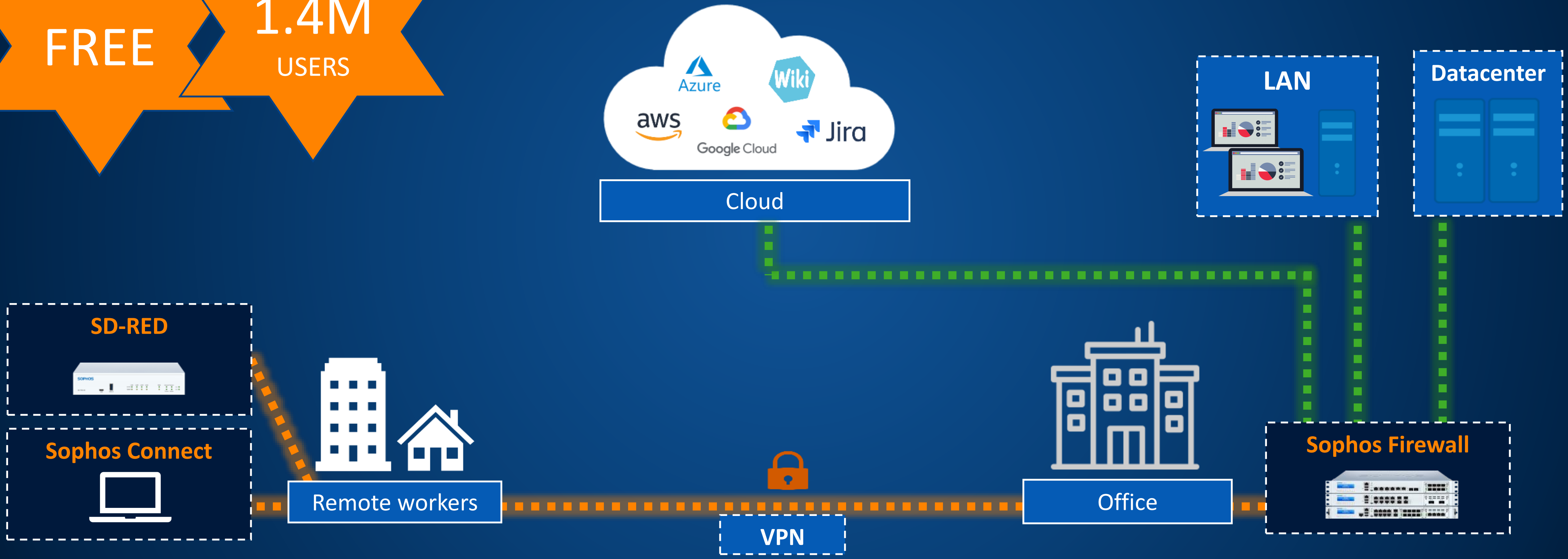


SOPHOS

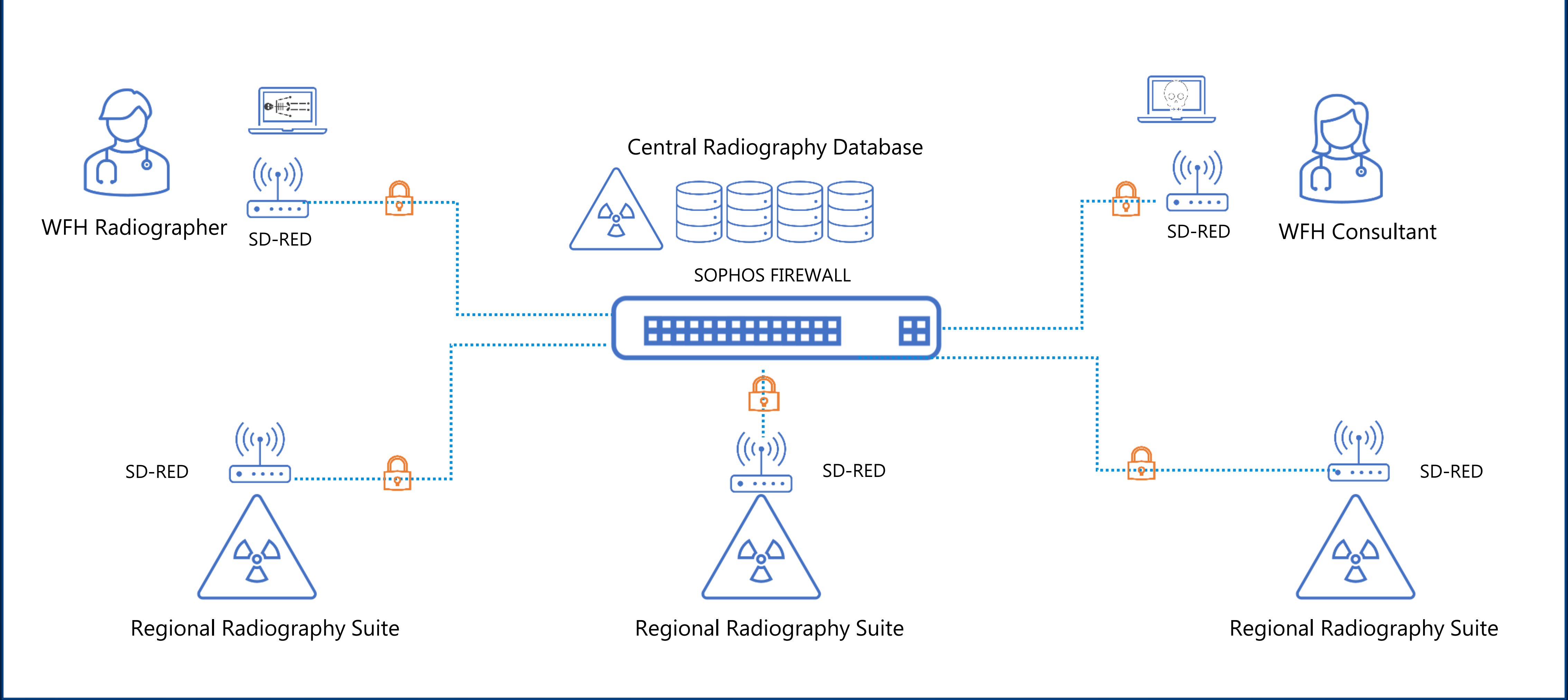
Secure Access: Sophos Firewall VPN

FREE

1.4M USERS



Secure Access: XG Firewall and SD-RED in Action


WFH Radiographer
SD-RED
Central Radiography Database
SOPHOS FIREWALL
SD-RED
WFH Consultant
SD-RED
SD-RED
SD-RED
Regional Radiography Suite
Regional Radiography Suite
Regional Radiography Suite

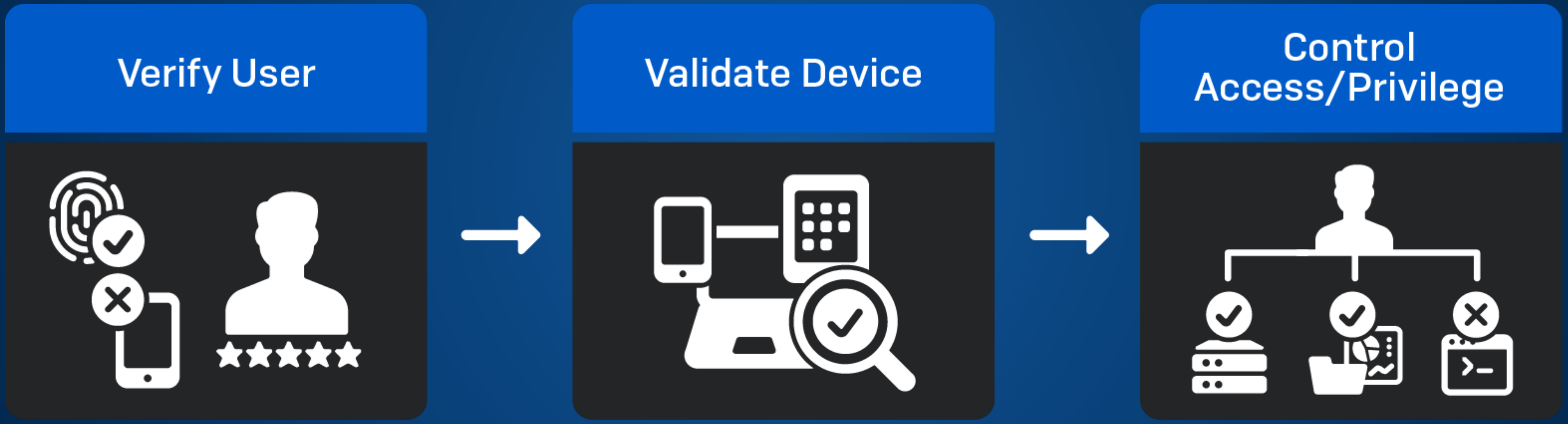
Remote Access Technology Is Evolving

Enhance Access Controls

Prevent Lateral Movement

Reduce Friction

Zero Trust Network Access (ZTNA)

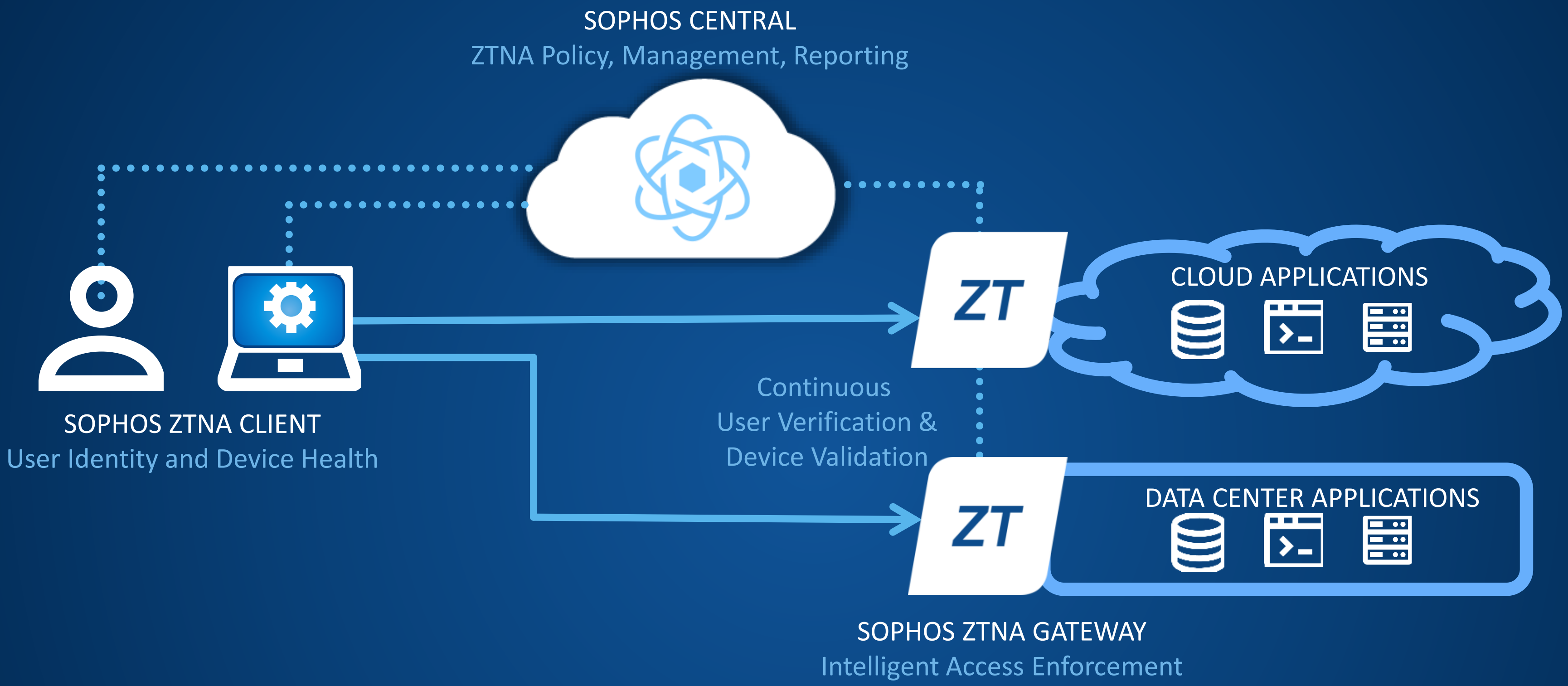


Verify User

Validate Device

Control Access/Privilege

Sophos ZTNA: Cloud-delivered, Cloud-Managed


SOPHOS CENTRAL

ZTNA Policy, Management, Reporting

SOPHOS ZTNA CLIENT

User Identity and Device Health

Continuous
User Verification &
Device Validation

SOPHOS ZTNA GATEWAY

Intelligent Access Enforcement

ZTNA Client

- Easy deployment
- Transparent and frictionless
- Integrates identity and device health continuously
- Windows, Mac*, Mobile*

**Roadmap*

Sophos Central

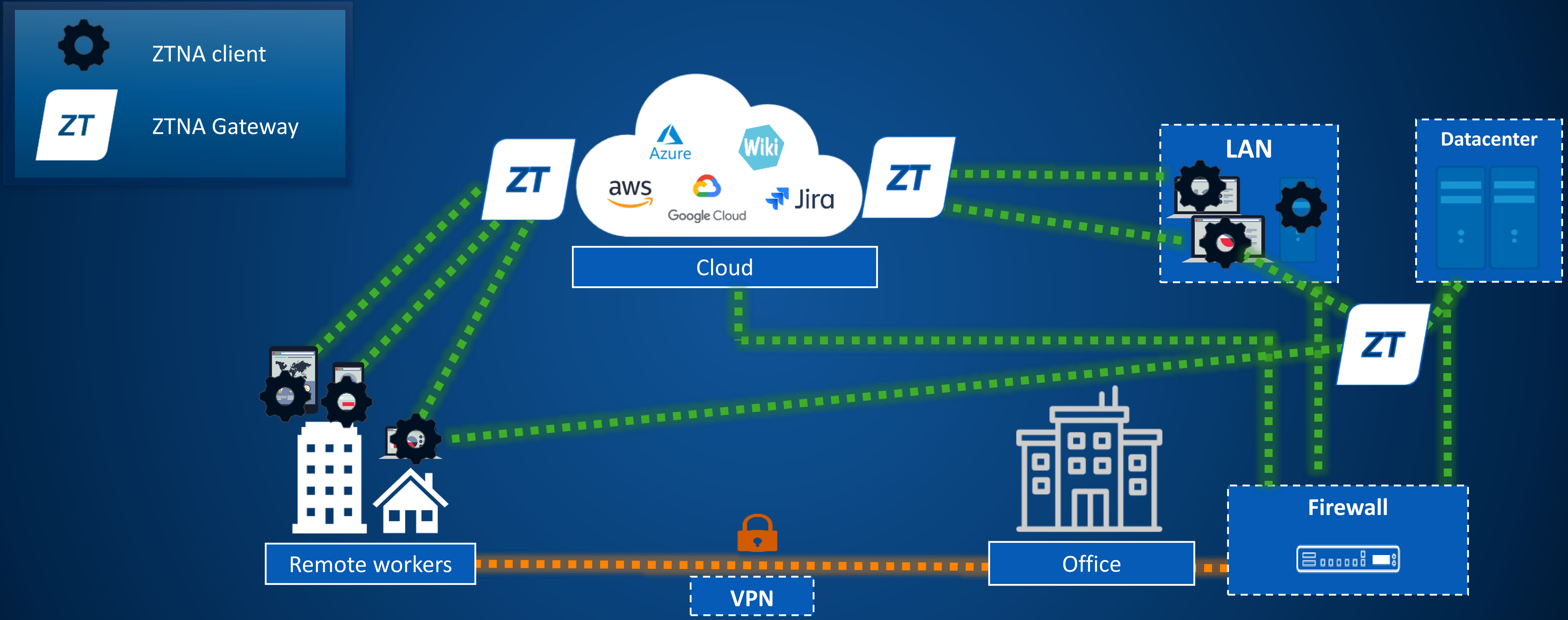
- Central management
- Granular policy controls
- Insightful reporting
- Manage alongside other Sophos products

ZT ZTNA Gateway

- Software/VM based for cloud
- Continuously verifies and validates access based on policy
- Log and event data shared with Sophos Central

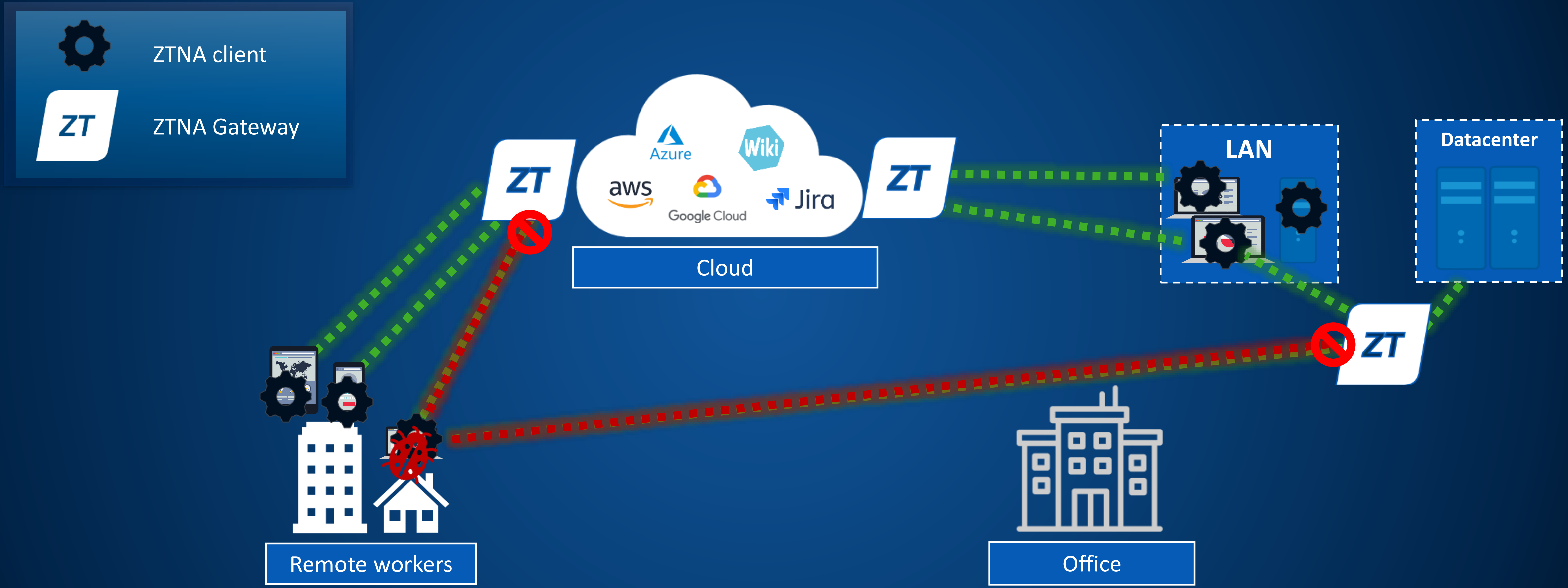
SOPHOS

Sophos ZTNA



SOPHOS

Sophos ZTNA


ZTNA client
ZT
ZTNA Gateway
ZT
Azure
Wiki
aws
Google Cloud
Jira
Cloud
ZT
LAN
Datacenter
ZT
Remote workers
Office

Sophos ZTNA: Delivering the Future

Enhance Access Controls

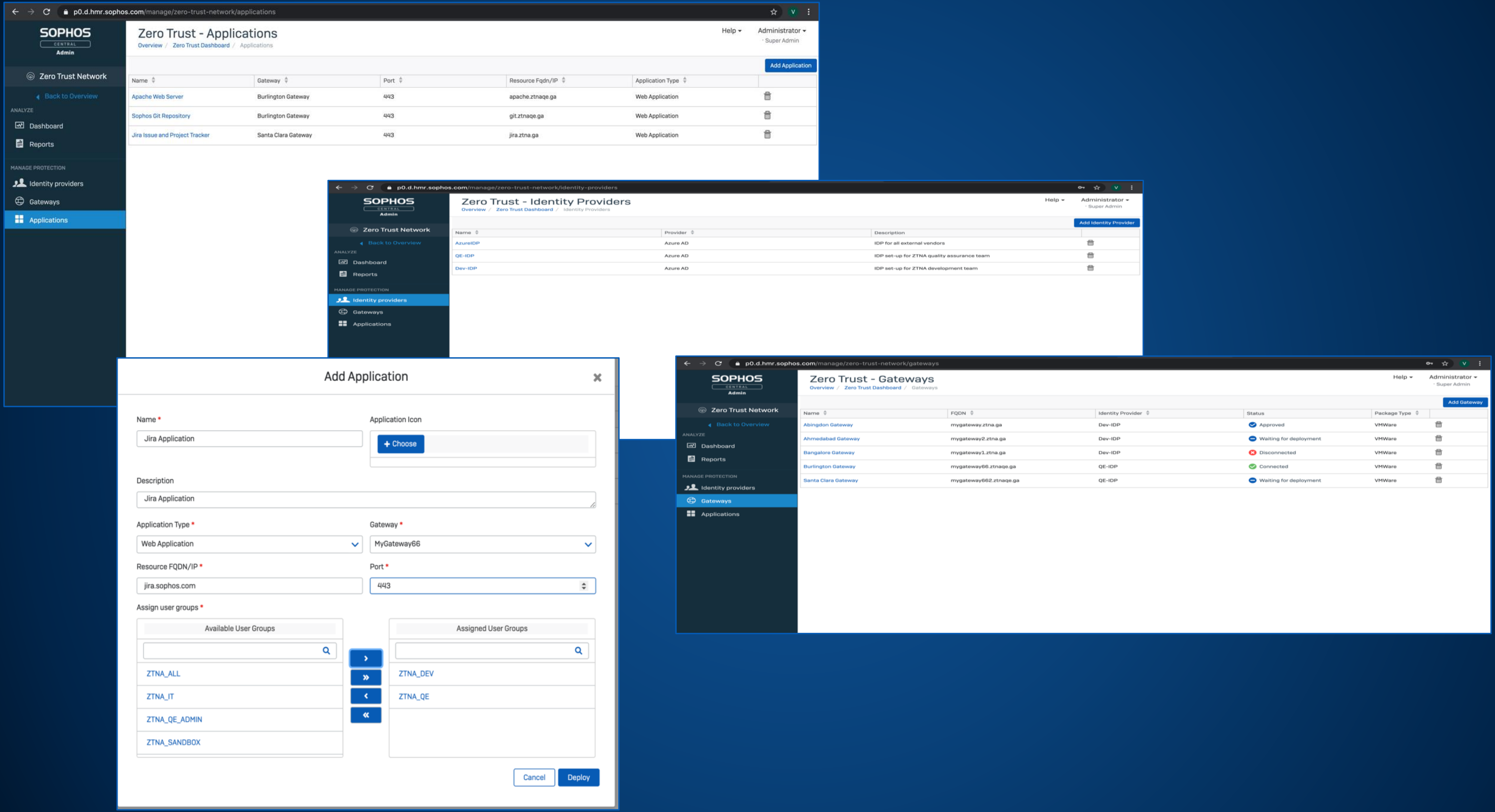
- Granular controls based on policy and risk
- No implicit trust – continual assessment of identity and device health

Prevent Lateral Movement

- Access granted to resources, not the whole network

Reduce Friction

- Easy enrollment
- Transparent connectivity that ‘just works’



Zero Trust - Applications

Overview / Zero Trust Dashboard / Applications

Name	Gateway	Port	Resource Fqdn/IP	Application Type
Apache Web Server	Burlington Gateway	443	apache.ztnaqe.ga	Web Application
Sophos Git Repository	Burlington Gateway	443	git.ztnaqe.ga	Web Application
Jira Issue and Project Tracker	Santa Clara Gateway	443	jira.ztna.ga	Web Application

p0.d.hmr.sophos.com/manage/zero-trust-network/identity-providers
Add Identity Provider

Zero Trust - Identity Providers

Overview / Zero Trust Dashboard / Identity Providers

Name	Provider	Description
AzureIDP	Azure AD	IDP for all external vendors
QE-IDP	Azure AD	IDP set-up for ZTNA quality assurance team
Dev-IDP	Azure AD	IDP set-up for ZTNA development team

Zero Trust - Gateways

Overview / Zero Trust Dashboard / Gateways

Name	FQDN	Identity Provider	Status	Package Type
Abingdon Gateway	mygateway.ztna.ga	Dev-IDP	Approved	VMWare
Ahmedabad Gateway	mygateway2.ztna.ga	Dev-IDP	Waiting for deployment	VMWare
Bangalore Gateway	mygateway1.ztna.ga	Dev-IDP	Disconnected	VMWare
Burlington Gateway	mygateway66.ztnaqe.ga	QE-IDP	Connected	VMWare
Santa Clara Gateway	mygateway662.ztnaqe.ga	QE-IDP	Waiting for deployment	VMWare

Add Application

Name *: Jira Application

Application Icon: + Choose

Description: Jira Application

Application Type *: Web Application

Gateway *: MyGateway66

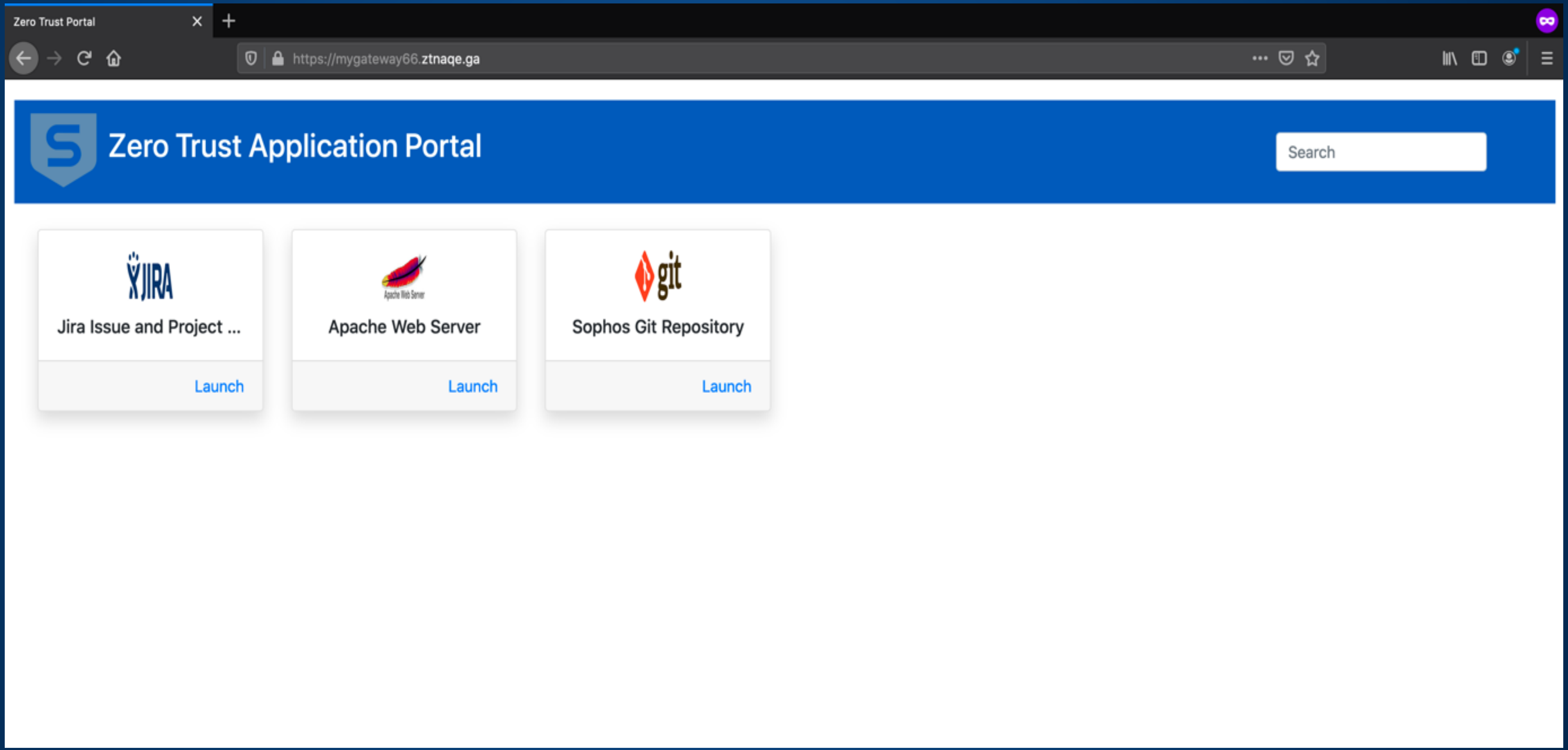
Resource FQDN/IP *: jira.sophos.com

Port *: 443

Assign user groups *

Available User Groups	Assigned User Groups
ZTNA_ALL	ZTNA_DEV
ZTNA_IT	ZTNA_QE
ZTNA_QE_ADMIN	
ZTNA_SANDBOX	

User Portal Screen



Sophos ZTNA

Now

Join the early access program

Mid-2021

Full availability

SECURE DEVICES

Mobile

Desktop

Server

macOS

Windows

Android

Chromebook

iOS

Linux

Intercept X: The World’s Best Endpoint Protection

Anti-ransomware

Unauthorised Encryption

Deep Learning AI

Unknown Executables

Anti-exploit

Exploits File-less Attacks

Foundational

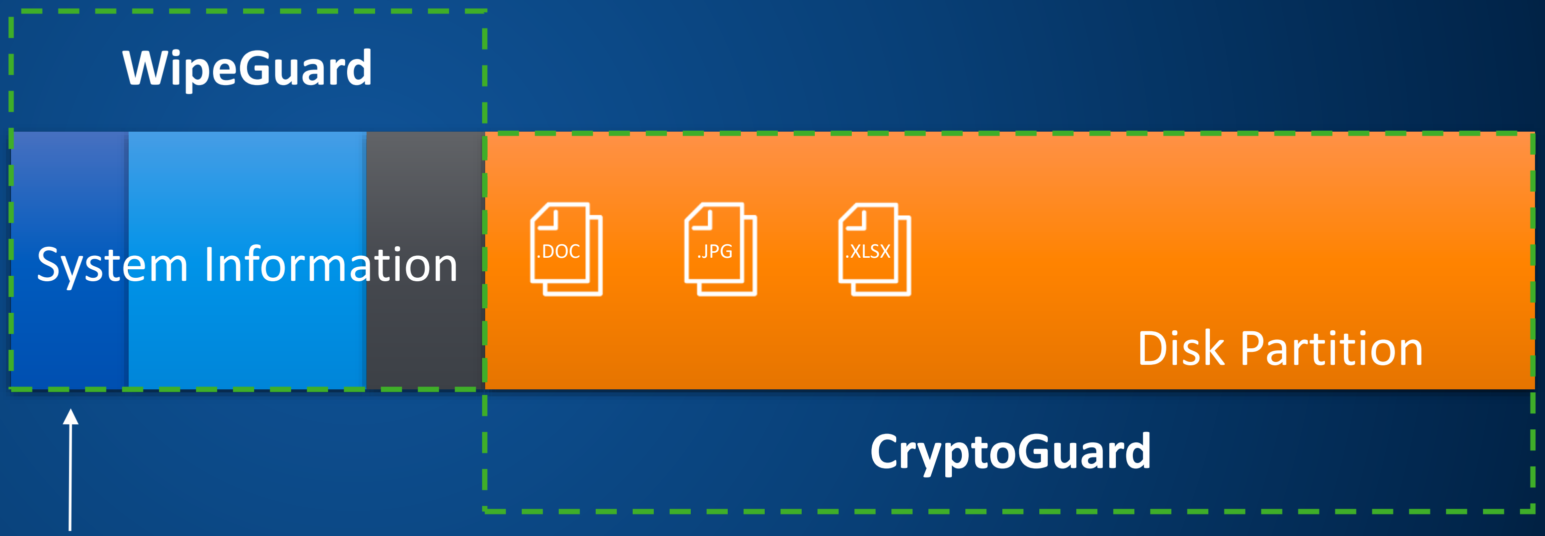
Known Threats

Intercept X: The World’s Best Endpoint Protection

Anti-ransomware

Unauthorized Encryption

Protects Disks and Boot Records



Master Boot Record (MBR)

Stops Unauthorized File Encryption

Intercept X: The World’s Best Endpoint Protection

Anti-ransomware

Unauthorised Encryption

Deep Learning AI

Unknown Executables

- ✓ Stops unknown threats
- ✓ Scales effectively
- ✓ Performs efficiently

Intercept X: The World's Best Endpoint Protection

Anti-ransomware

Unauthorised
Encryption

+

Deep Learning AI

Unknown
Executables

+

Anti-exploit

Exploits
File-less Attacks

Intercept X: The World's Best Endpoint Protection

Anti-ransomware

Unauthorised Encryption

+

Deep Learning AI

Unknown Executables

+

Anti-exploit

Exploits File-less Attacks

+

Foundational

Known Threats

Multiple layers of defense

SOPHOS

Intercept X: Securing Any Device, Any Platform

Desktop

Server

Mobile

Windows macOS

Windows Linux

Android / iOS / Chromebook

Human-led Threat Hunting

48%

Already do human-led threat hunts

48%

Plan to incorporate human-led threat hunts

VansonBourne

SOPHOS

Intercept X: Endpoint Detection and Response (EDR)

IT admins and security analysts

Threat hunting

IT hygiene

Intercept X: Endpoint Detection and Response (EDR)

Investigate

Powerful, out-of-the-box, customizable SQL queries

Why is a machine running slowly?

Are there programs running on the machine that should be removed?

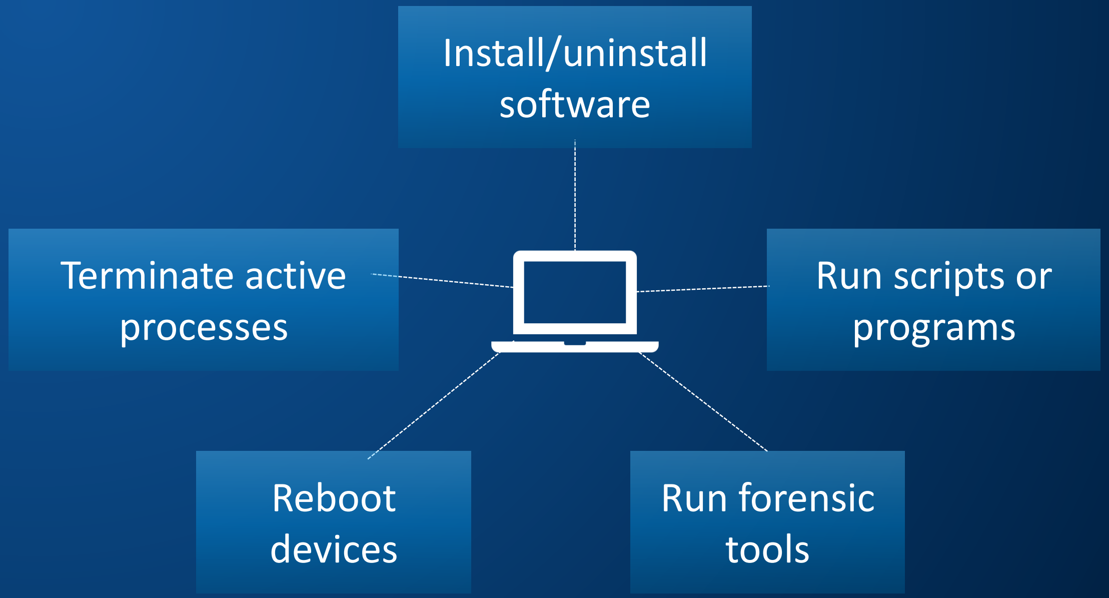
Which devices have unauthorized browser extensions?

Are processes trying to make a network connection on non-standard ports?

Are processes trying to make a network connection on non-standard ports?

Respond

Remotely access devices to remediate issues



Install/uninstall software

Terminate active processes

Run scripts or programs

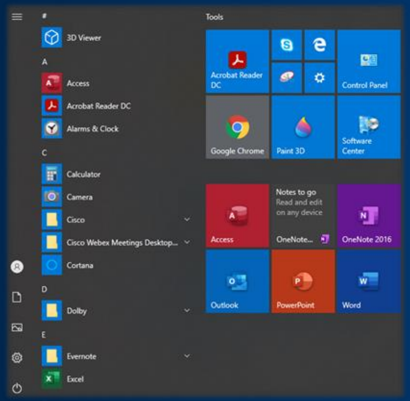
Reboot devices

Run forensic tools

Intercept X: Common EDR Use Cases

Chrome Running Slowly

- *Multiple user reports of chrome performance issues*
- Identify unauthorized chrome extensions have been installed
- Remotely access devices to uninstall chrome extensions



Software Queries:

- *Compliance and licensing usage*
- Check that sensitive files have been removed from devices
- Check haven’t exceeded software license usage
- Remotely access devices to remove files or software

Network Activity:

- *Want to check for signs of attempted breaches*
- Look for failed login attempts and active communication from PowerShell
- Remotely access devices to perform further analysis, isolate devices and terminate processes as needed

Phishing Investigation

- *Neutralize phishing attack*
- Identify users that clicked on a suspect link and if they downloaded files
- Check if files interacted with anything else
- Isolate affected devices, remove downloaded files and terminate suspect processes

SOPHOS

Shortage of Skilled Staff Is a Major Challenge

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 biggest challenge”

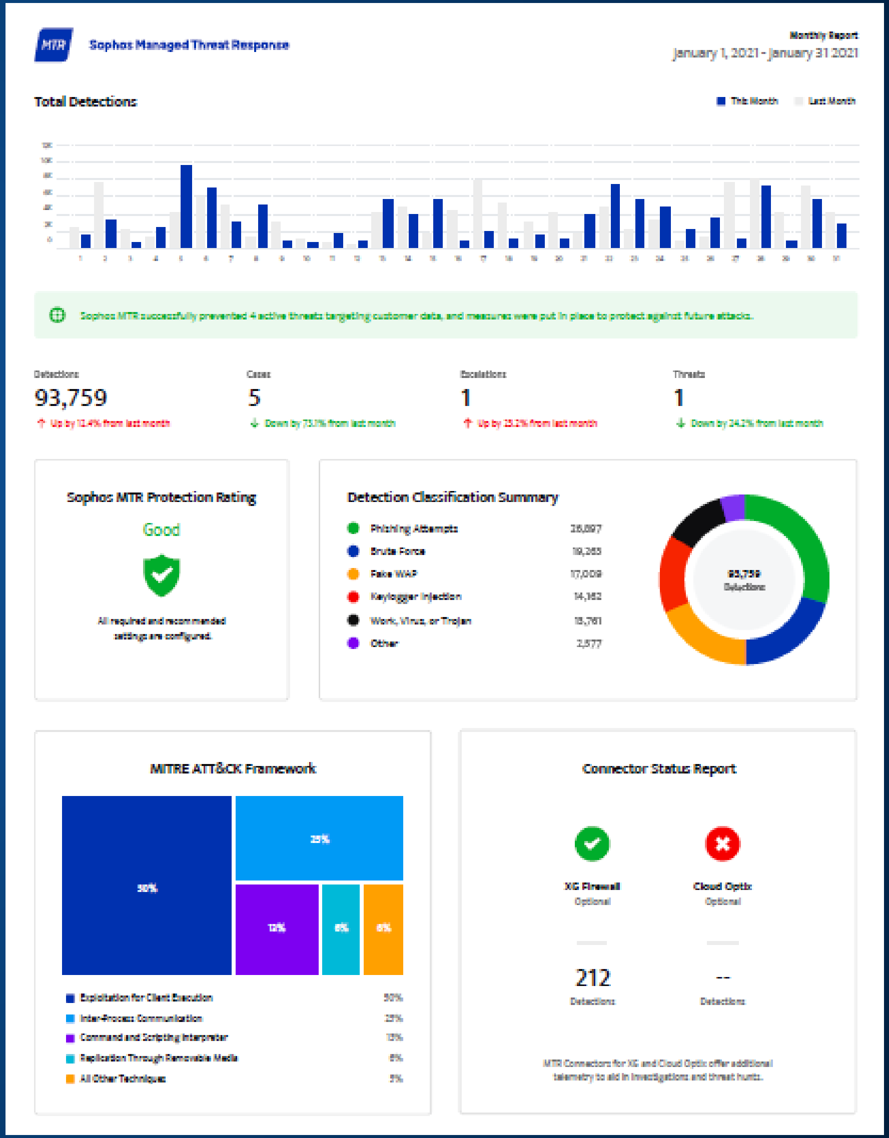
VansonBourne

Sophos Managed Threat Response

- ✓ 24/7 threat hunting, detection and response
- ✓ Delivered by an elite team as a fully-managed service, leveraging the power of SophosLabs
- ✓ You control how and when incidents are escalated and what actions we take for you
- ✓ Full transparency: weekly and monthly reports

Winner: Best Managed Security Services Offering

Channel Partner Insights Innovation Awards 2020



MTR Sophos Managed Threat Response

Monthly Report
January 1, 2021 - January 31 2021

Total Detections

Sophos MTR successfully prevented 4 active threats targeting customer data, and measures were put in place to protect against future attacks.

Detections	Cases	Escalations	Threats
93,759	5	1	1
↑ Up by 12.4% from last month	↓ Down by 73.7% from last month	↑ Up by 23.2% from last month	↓ Down by 24.2% from last month

Sophos MTR Protection Rating

Good

All required and recommended settings are configured.

Detection Classification Summary

● Phishing Attempts	26,897
● Brute Force	19,263
● Fake WAP	17,009
● Keylogger Injection	14,162
● Work, Virus, or Trojan	13,761
● Other	2,577

MITRE ATT&CK Framework

■ Exploitation for Client Execution	50%
■ Inter-Process Communication	25%
■ Command and Scripting Interpreter	13%
■ Replication Through Removable Media	6%
■ All Other Techniques	5%

Connector Status Report

✓ XG Firewall	✗ Cloud Optix
Optional	Optional
212	--
Detections	Detections

MTR Connectors for XG and Cloud Optix offer additional telemetry to aid in investigations and threat hunts.

The World's Best
Endpoint Protection

EDR for Security Analysts
and IT Administrators

Managed Detection &
Response

Sophos Mobile: Secure Unified Endpoint Management

Stops threats

- Industry leading threat protection by Intercept X
- Secures iOS, Android Chrome OS, W10 & macOS devices

Secures data

- Full device or container-only management
- Remotely deploy apps, policies and settings including email

Cuts admin

- Flexible self-service portal
- Users can enroll devices, reset passwords and get help themselves

SECURE DATA AND WORKLOADS

SaaS/Public Cloud

On Premises

macOS

Windows

Linux

PROTECT DATA AND WORKLOADS

Detect, query and secure hybrid cloud workloads

Secure data on on-premises servers

Intercept X for Server

Sophos Cloud Optix

SECURE THE NETWORK

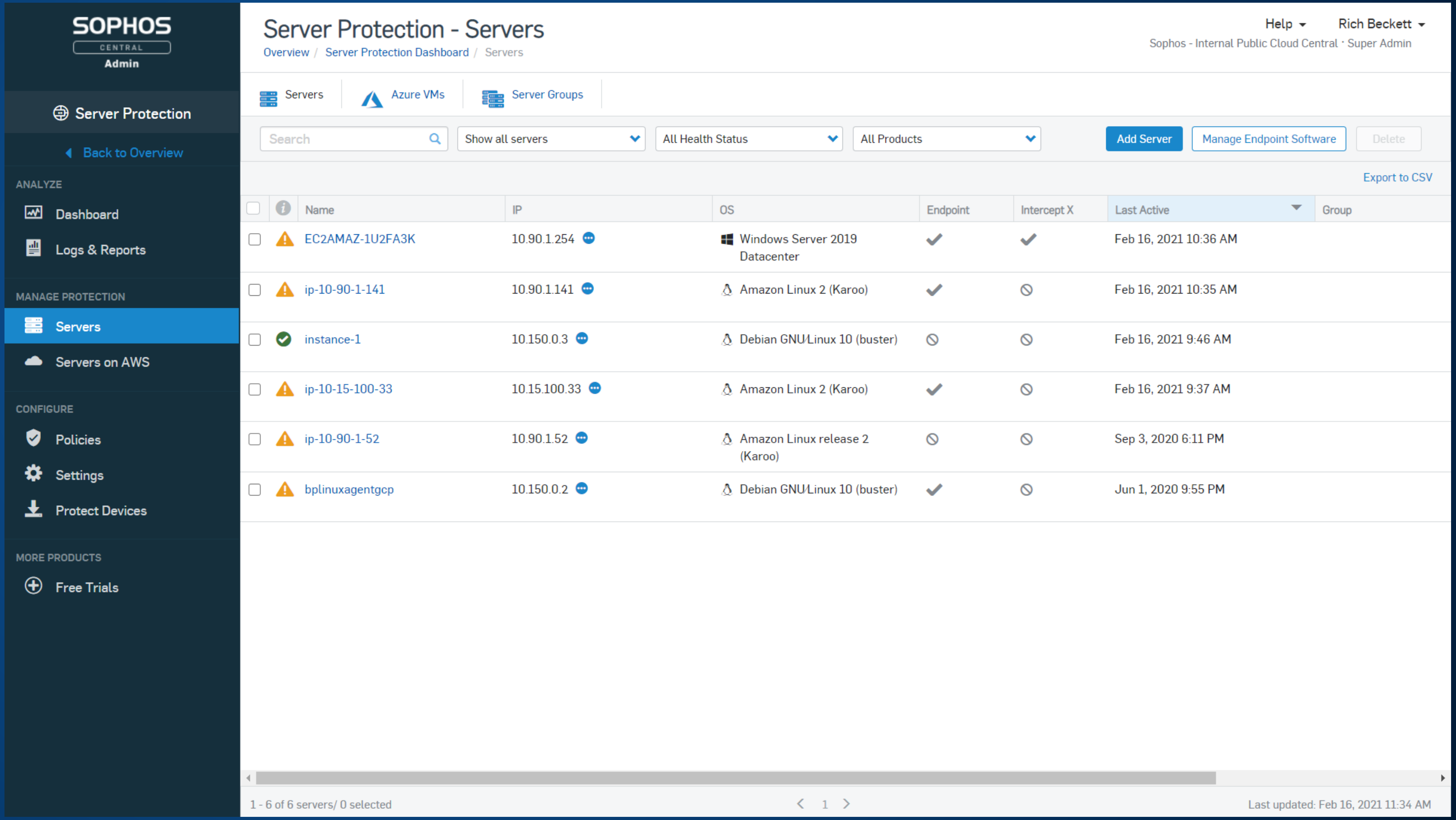
Secure cloud-based and on-premises networks

Sophos Firewall

Protect Data and Workloads

Sophos Intercept X Advanced for Server

- ✓ **Stop advanced threats** including ransomware, and server-specific malware
- ✓ **Lock down your servers**. Control what can run and get notification of unauthorized change attempts
- ✓ **Manage everything centrally** from one console, including mixed cloud **and** on-premises scenarios.



Server Protection - Servers

Overview / Server Protection Dashboard / Servers

□		Name	IP	OS	Endpoint	Intercept X	Last Active	Group
□	⚠	EC2AMAZ-1U2FA3K	10.90.1.254	Windows Server 2019 Datacenter	✓	✓	Feb 16, 2021 10:36 AM	
□	⚠	ip-10-90-1-141	10.90.1.141	Amazon Linux 2 (Karoo)	✓	⊘	Feb 16, 2021 10:35 AM	
□	✓	instance-1	10.150.0.3	Debian GNU/Linux 10 (buster)	⊘	⊘	Feb 16, 2021 9:46 AM	
□	⚠	ip-10-15-100-33	10.15.100.33	Amazon Linux 2 (Karoo)	✓	⊘	Feb 16, 2021 9:37 AM	
□	⚠	ip-10-90-1-52	10.90.1.52	Amazon Linux release 2 (Karoo)	⊘	⊘	Sep 3, 2020 6:11 PM	
□	⚠	bplinuxagentgcp	10.150.0.2	Debian GNU/Linux 10 (buster)	✓	⊘	Jun 1, 2020 9:55 PM	

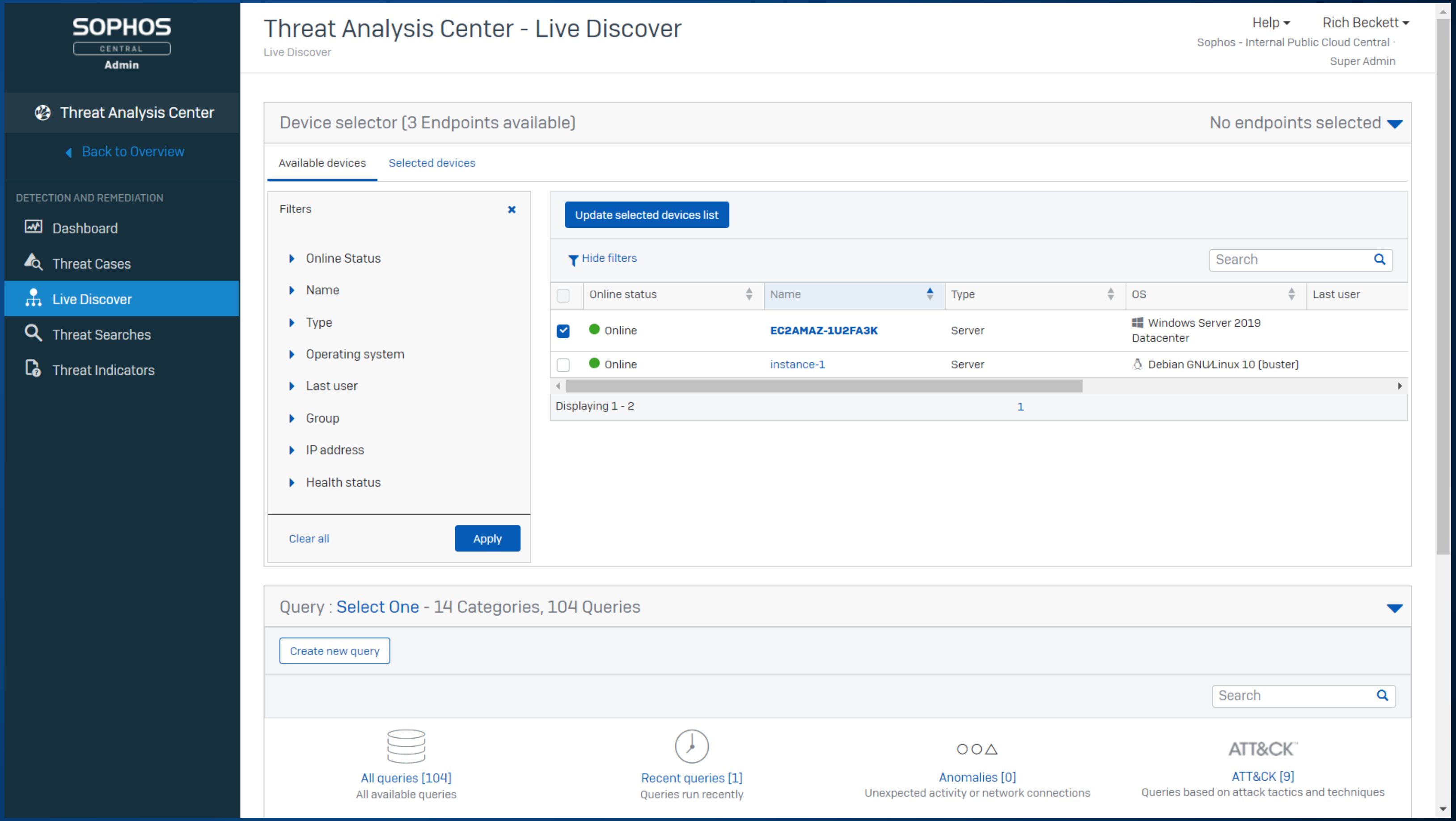
1 - 6 of 6 servers/ 0 selected

Last updated: Feb 16, 2021 11:34 AM

Protect Data and Workloads

Sophos Intercept X Advanced for Server ***with EDR***

- ✓ **Catch evasive threats -** search for issues, and understand what happened
- ✓ **Automatically detect cloud workloads** and S3 buckets and databases
- ✓ **Detect insecure cloud deployments** with constant AI monitoring



Threat Analysis Center - Live Discover

Live Discover

Sophos - Internal Public Cloud Central - Super Admin

Device selector (3 Endpoints available) — No endpoints selected

Available devices | Selected devices

	Online status	Name	Type	OS	Last user
☑	● Online	EC2AMAZ-1U2FA3K	Server	Windows Server 2019 Datacenter	
□	● Online	instance-1	Server	Debian GNU/Linux 10 (buster)	

Displaying 1 - 2 1

Query : Select One - 14 Categories, 104 Queries

All queries [104]
All available queries

Recent queries [1]
Queries run recently

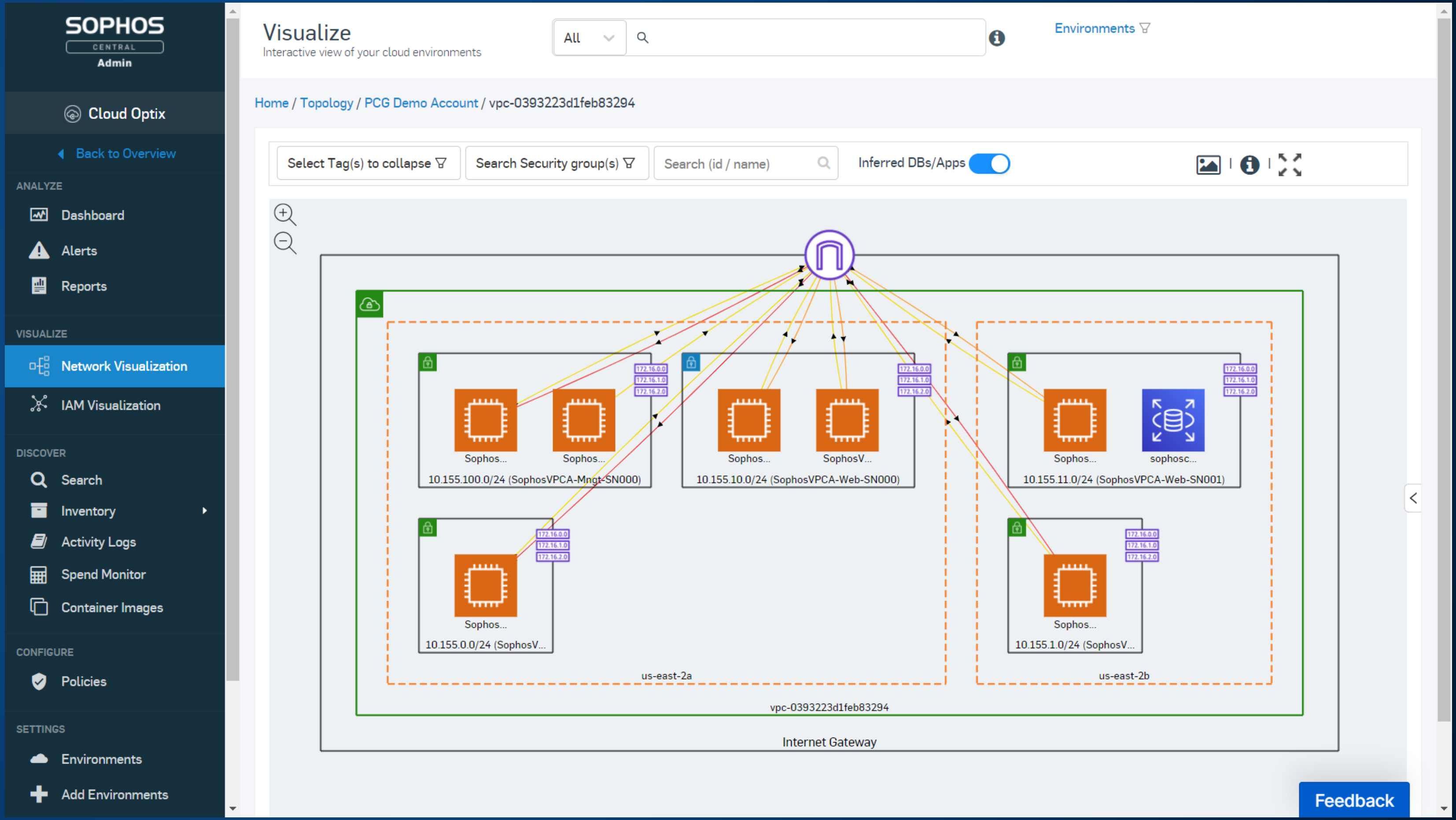
Anomalies [0]
Unexpected activity or network connections

ATT&CK [9]
Queries based on attack tactics and techniques

Protect Data and Workloads

Sophos Cloud Optix

- ✓ Get asset and network traffic visibility for AWS, Azure, and Google Cloud
- ✓ Continually monitor for security risks, over-privileged IAM access, spend anomalies
- ✓ Get risk-based prioritization of security issues
- ✓ Optimize spend for AWS and Azure on a single screen.
- ✓ Identify Sophos Firewalls and workload protection on AWS



SOPHOS

See the Wood for the Trees

> *"With Sophos Cloud Optix, we significantly minimize alert fatigue. The powerful artificial intelligence built into Sophos Cloud Optix correlates the data and shows us what is truly meaningful and actionable"*

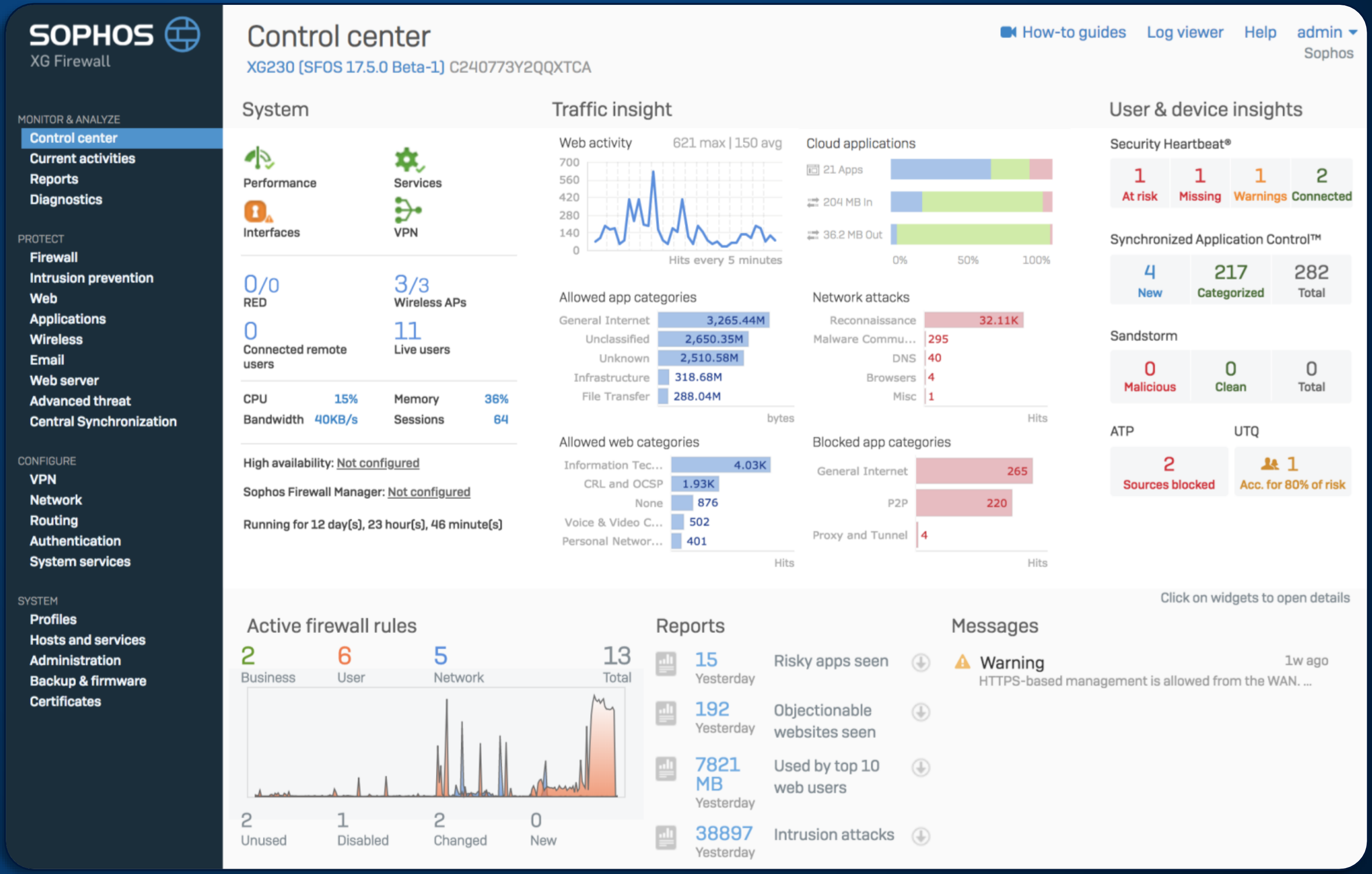
Ross McKerchar, CISO at Sophos

SOPHOS

Secure the Network

Sophos XG Firewall

- ✓ Multi-layered protection for network infrastructure
- ✓ Powerful all-in-one solution for IPS, ATP, remote user and site connectivity
- ✓ Cloud application visibility and shadow IT discovery
- ✓ Flexibility to run as standalone or HA solution



SOPHOS
XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central Synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Control center

XG230 (SFOS 17.5.0 Beta-1) C240773Y2QQXTCA

How-to guides | Log viewer | Help | admin
Sophos

System

Performance | Services
Interfaces | VPN

0/0 RED | 3/3 Wireless APs
0 Connected remote users | 11 Live users

CPU	15%	Memory	36%
Bandwidth	40KB/s	Sessions	64

High availability: Not configured

Sophos Firewall Manager: Not configured

Running for 12 day(s), 23 hour(s), 46 minute(s)

Traffic insight

Web activity — 621 max | 150 avg

Cloud applications

Allowed app categories

General Internet	3,265.44M
Unclassified	2,650.35M
Unknown	2,510.58M
Infrastructure	318.68M
File Transfer	288.04M

bytes

Network attacks

Reconnaissance	32.11K
Malware Commu...	295
DNS	40
Browsers	4
Misc	1

Hits

Allowed web categories

Information Tec...	4.03K
CRL and OCSP	1.93K
None	876
Voice & Video C...	502
Personal Networ...	401

Hits

Blocked app categories

General Internet	265
P2P	220
Proxy and Tunnel	4

Hits

User & device insights

Security Heartbeat®

1	1	1	2
At risk	Missing	Warnings	Connected

Synchronized Application Control™

4	217	282
New	Categorized	Total

Sandstorm

0	0	0
Malicious	Clean	Total

ATP: 2 Sources blocked
UTQ: 1 Acc. for 80% of risk

Click on widgets to open details

Active firewall rules

2	6	5	13
Business	User	Network	Total

2	1	2	0
Unused	Disabled	Changed	New

Reports

15 Yesterday	Risky apps seen
192 Yesterday	Objectionable websites seen
7821 MB Yesterday	Used by top 10 web users
38897 Yesterday	Intrusion attacks

Messages

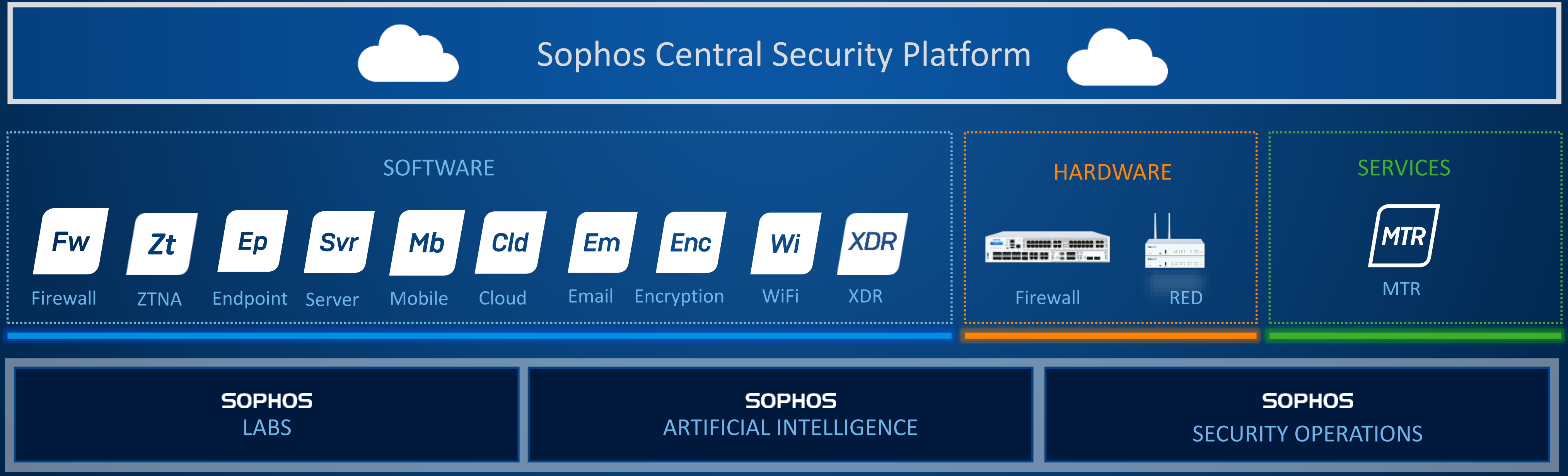
⚠ Warning — 1w ago
HTTPS-based management is allowed from the WAN. ...

CENTRAL MANAGEMENT

Sophos Central: Unifying Cybersecurity Platform

400,000 users +

FREE



Sophos Central Security Platform

SOFTWARE

Fw Firewall

Zt ZTNA

Ep Endpoint

Svr Server

Mb Mobile

Cld Cloud

Em Email

Enc Encryption

Wi WiFi

XDR XDR

HARDWARE

Firewall

RED

SERVICES

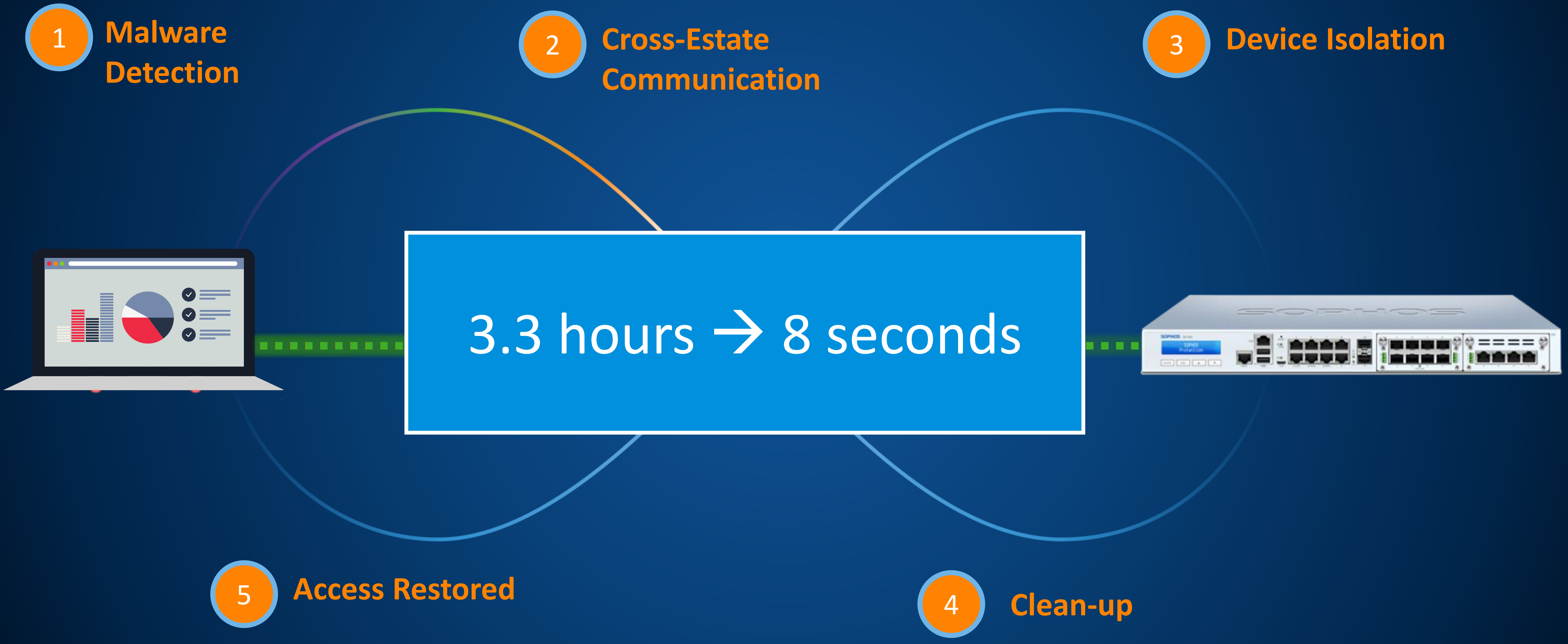
MTR MTR

SOPHOS LABS

SOPHOS ARTIFICIAL INTELLIGENCE

SOPHOS SECURITY OPERATIONS

Synchronized Security: Automated Response



1 Malware Detection

2 Cross-Estate Communication

3 Device Isolation

3.3 hours → 8 seconds

4 Clean-up

5 Access Restored

Slashing Admin Workload by Half

Advanced Protection

Single Platform

Shared Intelligence

Automated Response

50%+

reduction in admin workload

85%

reduction in security incidents

To sum up…

Securing The Anywhere Organization with Sophos

SECURE CONNECTIVITY

- Sophos Firewall VPN/RED
- Sophos ZTNA

SECURE DEVICES

- Sophos Intercept X with EDR
- Sophos MTR
- Sophos Mobile

SECURE DATA AND WORKLOADS

- Sophos Intercept X for Server
- Sophos Cloud Optix
- Sophos Firewall

CENTRAL MANAGEMENT

- Sophos Central

End

SOPHOS

Cybersecurity evolved.