



Securing the Anywhere Organization

Any location. Any device. Any resource.

Securing the Anywhere Organization





Remote working is here to stay: according to Gartner, 74% of organizations expect some employees to work remotely once the pandemic is over¹. At the same time, the resources people need to do their jobs are also in multiple locations: on servers in the office; in cloud-based applications like Office 365 or Salesforce; and in private or public cloud environments on Amazon Web Services (AWS) and Microsoft Azure.

IT teams are tasked with protecting every user and every resource, no matter where they are. Meanwhile, bad actors continue to find better and more subversive ways to penetrate increasingly virtual organizations at every intersection.

Securing organizations where people and resources can be anywhere requires:

- Secure connectivity, so users can access resources from any location: home, on-site, or in the office
- Protection for the devices used to make those connections — desktops, laptops, mobile phones, and tablets
- Protection for the data and workloads that users need to access, whether they're in the cloud or on your local network
- Simple management, so IT teams can manage their distributed organizations from anywhere, without adding to their workload

Fortunately, Sophos supports all these areas. We offer a complete portfolio of next-gen security products packed with advanced protection capabilities. Everything is controlled via a single, web-based security platform which slashes day-to-day admin overheads while enabling IT teams to manage their organization's security from anywhere.

 CONNECT SECURELY	 PROTECT DEVICES	 SECURE RESOURCES	 SIMPLIFY MANAGEMENT
Enable users to access resources securely from any location	Secure all devices used by your workforce	Secure data and workloads in the cloud and on your local network	Enable your IT team to easily manage your cybersecurity, from anywhere
Sophos Firewall VPN/RED	Sophos Intercept X with EDR	Sophos Intercept X for Server	Sophos Central
Sophos ZTNA	Sophos Managed Threat Response	Sophos Cloud Optix	
	Sophos Mobile	Sophos Firewall	

This solution brief walks you through how Sophos addresses each of these requirements. It also explores the productivity and protection benefits customers see when employing a Sophos cybersecurity system to secure their organization.

Connect securely

There's no argument that the COVID pandemic has driven a massive increase in remote working. During May 2020, 62% of employed Americans were working from home (WFH). However, remote working was already a trend even before COVID hit, and many in-office employees were already transitioning to working from home a few days a week. In the UK, remote working climbed at a rate of 74% in the last decade, while in Australia about a third of the workforce was regularly WFH.

Remote working is a win-win for companies and staff: employees save commuting time and costs while enjoying added flexibility and greater productivity. Meanwhile, organizations reduce costs and turnover rates. But for IT teams, long-term remote working creates additional security challenges. Whether employees are logging in from their living rooms, visiting a customer location, or sipping coffee at a Wi-Fi hotspot thousands of miles across the globe, your network and data must remain protected at all times.

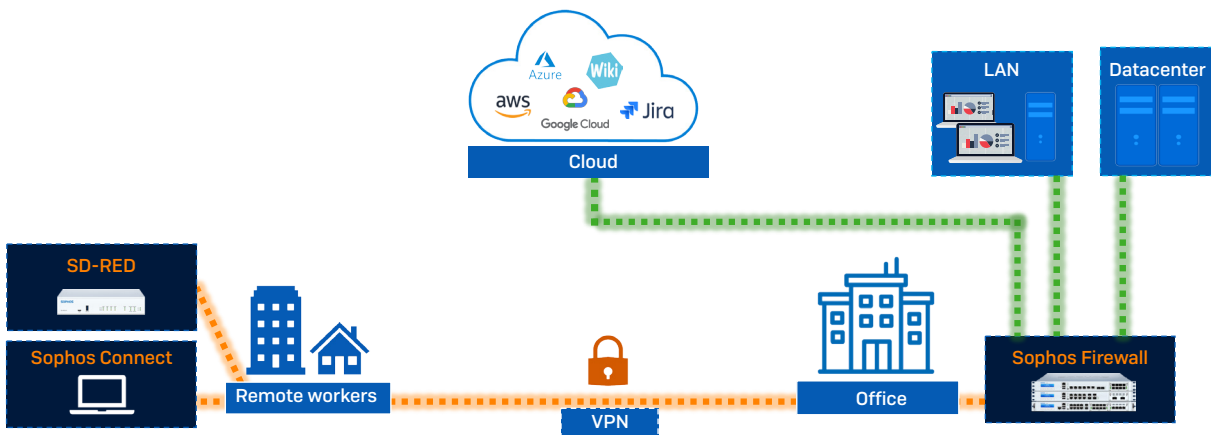
With Sophos, your employees can quickly, efficiently, and securely connect and work from anywhere, and we offer both traditional VPN-based and Zero Trust Network Access (ZTNA) options.

VPN

Use our free, easy-to-deploy **Sophos Connect VPN client** together with **Sophos Firewall** to connect remote workers to the main office and your cloud-based resources. With over 1.4 million users worldwide, Sophos Connect gives your remote users secure access to resources on the corporate network or public cloud from Windows and macOS devices.

For the ultimate in remote connectivity, **Sophos SD-RED** (Remote Ethernet Device) is a simple plug-and-play device that works with the **Sophos Firewall** to connect branch offices, remote sites, and individuals to your main network (whether physical or in the cloud).

It provides an always-on dedicated or split-tunnel VPN that's easy to deploy and manage with flexible options. It's also very small and portable, making it ideal for senior managers and other individuals who need to access a secure connection at any time, and from anywhere.

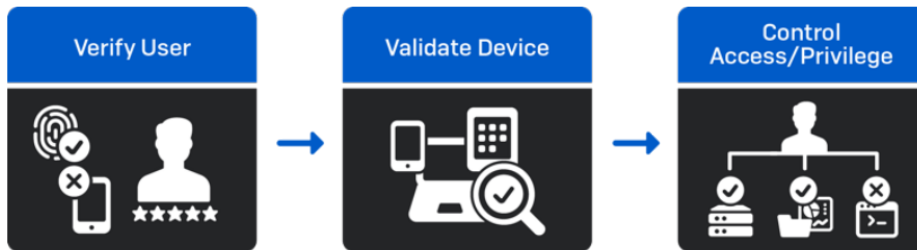


Secure remote connectivity with Sophos Firewall and Sophos Connect VPN and SD-RED

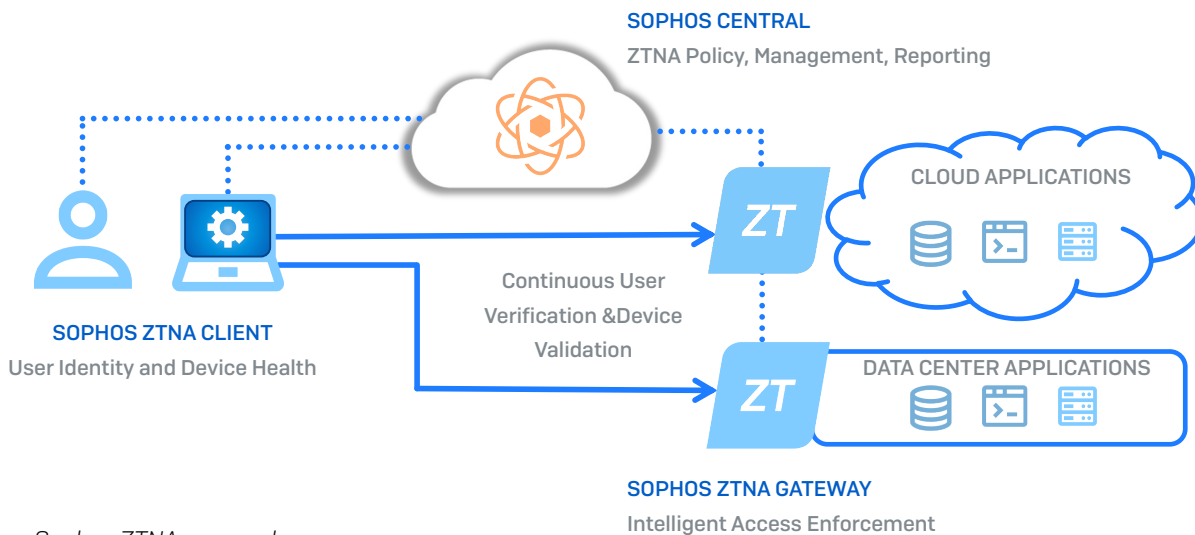
ZTNA

For years, VPN technology has successfully enabled workers to connect remotely. And it was a savior at the beginning of the pandemic, allowing organizations to quickly pivot to secure remote working in just days. However, many organizations are starting to want more than VPN was ever designed to deliver.

Sophos Zero Trust Network Access (ZTNA) is a great alternative to remote access VPN, enabling users to connect to corporate resources from any location in a straightforward and transparent way. At the same time, it also enhances your security by constantly verifying the user — typically with multi-factor authentication and an identity provider — and validating the health and compliance of the device.



Sophos ZTNA makes sure the device is enrolled, up-to-date, properly protected, and has encryption enabled. It then uses that information to make decisions based on customizable policies to determine user access and privilege to your critical networked applications.



Sophos ZTNA approach

With Sophos ZTNA, you can:

- ▶ Enhance your cyber defenses. Sophos ZTNA gives you very granular controls: any user, any device, any application can all be individually controlled based on individual corporate policy and the risk level you're comfortable with. It also eliminates the concept of implicit trust in an individual based on their presence on the network alone. Instead, it elevates protection and minimizes the risk of lateral movement within the network by continually assessing identity and device health before allowing access.
- ▶ Increase efficiency. Because Sophos ZTNA is managed through the Sophos Central platform, it's easy to enroll new users or support a changing work environment. Plus, it's more transparent for end-users and provides them with a friction-free "it just works" type of connection experience when compared to VPN.

Add Application ✕

Name * Application Icon

Description

Application Type * Gateway *

Resource FQDN/IP * Port *

Assign user groups *

Available User Groups	Assigned User Groups
<input type="text" value=""/>	<input type="text" value=""/>
ZTNA_ALL	ZTNA_DEV
ZTNA_IT	ZTNA_QE
ZTNA_QE_ADMIN	
ZTNA_SANDBOX	

Easily add applications with Sophos ZTNA

Whichever method you choose, Sophos award-winning security products will help you secure your employees in any location and on any device.

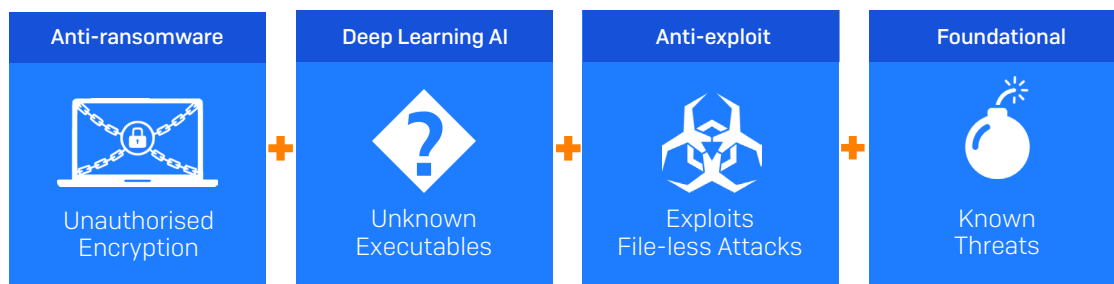
Protect devices

51% of organizations were hit by ransomware in the last year, with attackers succeeding in encrypting data in 73% of attacks².

Couple those alarming statistics with the need to secure all sorts of equipment — desktops, laptops, corporate and personal devices — and a slew of operating systems, from Windows, macOS, Linux, Android, Chromebook, and iOS, and you have an intense cybersecurity headache brewing.

Sophos Intercept X gives you the world's best protection across all these devices and platforms. You benefit from multiple layers of technology that stop attackers at numerous points in the kill chain, including:

- ▶ Anti-ransomware protection, which blocks the unauthorized encryption of files, hard disks, and boot records, restoring them to their safe state
- ▶ Deep Learning AI, which uses millions of file attributes to analyze threats and prevent both known and never-seen-before malware, stops them before they can execute
- ▶ Anti-exploit technology, to block exploits, active adversary techniques, and fileless and script-based attacks
- ▶ Foundational signature-based protection, which stops known threats



Plus, Sophos Intercept X secures any device on any platform – so your employees can work securely on any device they choose:

- Desktops and laptops running Windows and macOS
- Windows and Linux servers
- Virtual desktop environments hosted with cloud providers
- Mobile devices running Android, iOS, or Chromebook

Endpoint Detection and Response (EDR)

The most devastating cyber threats involve human-led attacks, often exploiting legitimate tools and processes such as PowerShell. Hands-on, live hacking enables attackers to bypass security products and protocols by modifying their tactics, techniques, and procedures (TTPs). When inside your network, attackers can move laterally to exfiltrate data, deploy ransomware, and install malware and backdoors for future attacks.

Stopping these human-led attacks requires human-led threat hunting. **Intercept X with EDR** (Endpoint Detection and Response) gives you the tools you need to perform threat hunts from the same console used to manage your Intercept X endpoint protection.

It's the first EDR designed for security analysts and IT administrators. While other EDR tools often require dedicated headcount or their own internal security operations center (SOC), Sophos EDR is simple to use without sacrificing the ability to perform robust analysis.

With Intercept X with EDR, you can investigate suspicious signals and threats—and improve your IT hygiene—with powerful out-of-the-box customizable SQL queries. Common use cases include:

- Chrome running slowly. Identify which unauthorized Chrome extensions have been installed
- Network activity check. Look for failed login attempts and active communication from PowerShell
- Software queries. Check that sensitive files have been removed from devices and/or that you haven't exceeded software license usage
- Phishing investigation. Identify users that clicked on a suspect link and if they downloaded files

Plus, you can remotely access devices using a command-line tool to remediate issues, such as rebooting devices, terminating active processes, running scripts or programs, editing configuration files, running forensic tools, and installing/uninstalling software.

Managed Detection and Response (MDR)

If you don't have the time, capacity, or expertise to run your own threat hunting and investigations, the **Sophos Managed Threat Response** (MTR) service is here to help.

Sophos MTR is a team of threat hunters and response experts who provide 24/7 monitoring, detection, and response capabilities delivered as a fully-managed service. They proactively hunt for and validate potential threats and incidents—and stop them before they can cause harm.

They also correlate data feeds from your Sophos protection solutions to identify indicators of compromise. Unlike other managed detection and response services, Sophos doesn't just notify you of issues; we also determine and apply the most appropriate actions to neutralize the threat.

Mobile Devices

When employees use personal devices for work, IT teams face the challenge of protecting company data without compromising user privacy. Our unified endpoint management solution, **Sophos Mobile**, secures iOS, Android, Chrome OS, Windows 10, and macOS devices. It lets you protect any combination of personal and corporate-owned devices with minimal effort and is ideal for BYOD (Bring Your Own Device) scenarios.

Sophos Mobile enables you to:

- Stop mobile threats. Get industry-leading defense against mobile malware, phishing, man-in-the-middle attacks, and more, all powered by Intercept X
- Secure corporate data. Choose full-device or container-only management, depending on your needs
- Reduce admin. The flexible self-service portal lets users enroll their personal macOS, Windows 10, or mobile devices, reset passwords, and get help – with no IT involvement

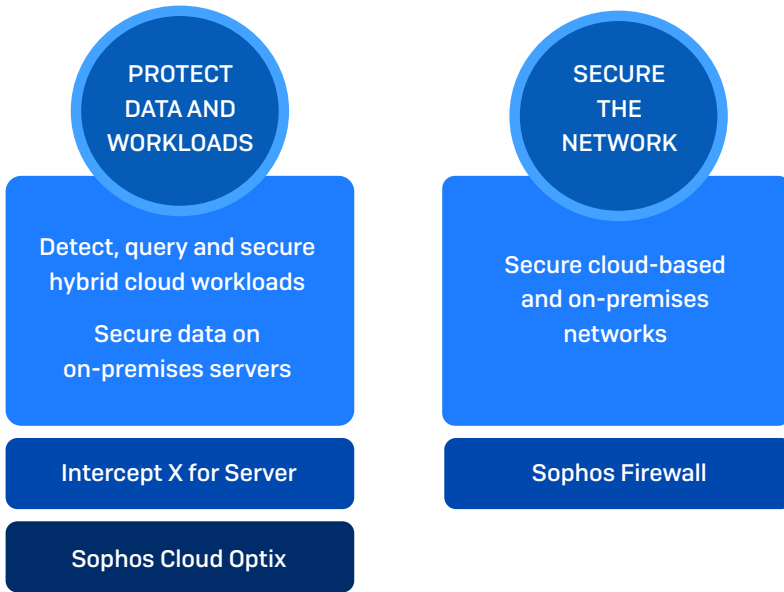
Secure resources

Depending on your organization's needs, you may be running servers on-premises, consuming cloud-based applications, or hosting resources in private and public cloud environments on AWS, Azure, or GCP. More likely, you're doing all of the above.

The cloud is rapidly becoming more and more central to most organizations' day-to-day operations. Because of this, cybercriminals are alert to opportunities provided by the cloud—so much so that 70% of companies using the public cloud suffered a cloud security incident in the last 12 months³.

When it comes to securing your resources—wherever they are located—you need to do two things:

1. Protect the data and workloads themselves
2. Secure the network they're on to keep intruders out



Protecting your data and workloads

Your data and workloads are your most important assets. **Sophos Intercept X for Server** secures cloud, on-premises, or hybrid workload environments. It protects Windows and Linux virtual machines and virtual desktops from the latest threats.

- ▶ Stop advanced attacks. Including ransomware, exploit-based attacks, and malware that has never been seen before
- ▶ Lockdown your server workloads. Control what can and can't run and get notifications for any unauthorized change attempts
- ▶ Manage everything centrally. Deploy and maintain everything from a single console, including mixed scenarios that include cloud workloads and on-premises servers

SOPHOS CENTRAL Admin

Server Protection - Servers

Overview / Server Protection Dashboard / Servers

Sophos - Internal Public Cloud Central - Super Admin

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					
ip-10-15-100-33	10.15.100.33					
ip-10-90-1-52	10.90.1.52					
bplinuxagentgcp	10.150.0.2					

Lock Down

During lockdown, Sophos Central creates an allow list of all the software currently on the server.

⚠ This may take some time – do not install or update software during this process.

Before locking the server, we recommend that you:

- Install any server roles or features.
- Install all Windows updates and restart if necessary.
- Clear the temporary files directory and any browser cache.
- Remove any downloaded installers that you don't plan to use.

For detailed information, see the [FAQs](#).

Cancel **Begin Lockdown**

1 - 6 of 6 servers/ 0 selected

Last updated: Feb 16, 2021 11:34 AM

You can also extend your EDR investigations to your servers, whether on-premises or in the cloud, with **Intercept X for Server with EDR**. This enables you to:

- ▶ Perform critical IT operations and threat hunting tasks. Identify performance issues, see what's installed where, and hunt down suspicious activity
- ▶ Automatically detect cloud workloads. Keep eyes on critical cloud services, including S3 buckets, databases, and serverless functions
- ▶ Detect insecure deployments. Rely on constant AI monitoring of your cloud environments and notification of irregularities

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. The sidebar on the left contains navigation options: Threat Analysis Center, Back to Overview, DETECTION AND REMEDIATION, Dashboard, Threat Cases, Live Discover (highlighted), Threat Searches, and Threat Indicators. The main content area is titled 'Threat Analysis Center - Live Discover' and shows a 'Device selector' for 3 endpoints. The 'Available devices' tab is active, displaying a table of devices. The table has columns for Online status, Name, Type, OS, and Last user. Two devices are listed: 'EC2AMAZ-1U2FA3K' (Windows Server 2019 Datacenter) and 'instance-1' (Debian GNU/Linux 10 (buster)). Below the table, there are statistics for queries, anomalies, and ATT&CK categories.

Online status	Name	Type	OS	Last user
<input checked="" type="checkbox"/>	EC2AMAZ-1U2FA3K	Server	Windows Server 2019 Datacenter	
<input type="checkbox"/>	instance-1	Server	Debian GNU/Linux 10 (buster)	

Query : Select One - 14 Categories, 104 Queries

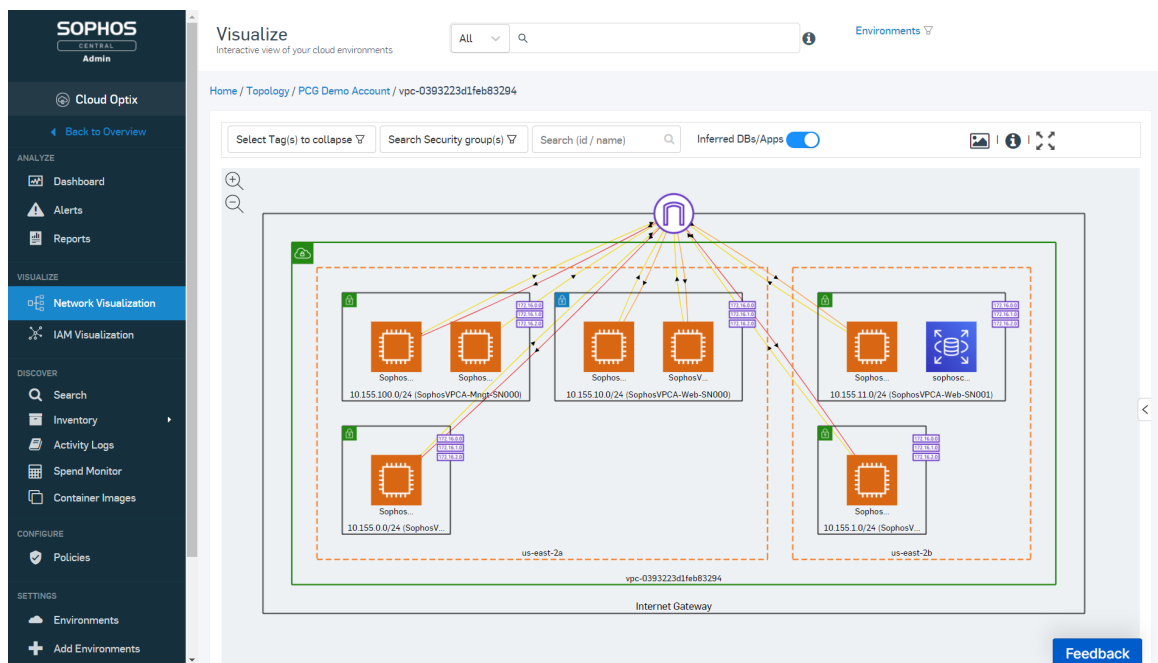
All queries [104] Recent queries [1] Anomalies [0] ATT&CK [9]

Extend your EDR investigations to your server

Protection is one side of the data and workload protection coin. Visibility is the other. You need a continuous and clear line of sight into what you have running and the ability to configure cloud provider services to prevent security breaches.

Sophos Cloud Optix, our Cloud Security Posture Management solution, gives you the visibility you need to secure your organization, including:

- ▶ Multi-cloud visibility. Detailed cloud resource inventory, including servers, containers, storage, network and IAM for AWS, Azure, and GCP
- ▶ Risk-based prioritization. Continually analyze configurations for security risks and over-privileged IAM access
- ▶ Compliance management. Continuously monitor compliance with out-of-the-box templates, custom policies, and collaboration tools
- ▶ Integrated security. Identify Sophos Firewalls and workload protection on AWS
- ▶ Cloud cost optimization. Manage AWS and Azure spending on a single screen



Sophos Cloud Optix

While security alerts for your cloud environments are helpful, with services such as Amazon GuardDuty providing great value, it's all too easy to get overwhelmed by the sheer volume of notifications. That can make it virtually impossible to recognize which notifications you actually need to deal with.

At Sophos, we use Sophos Cloud Optix to protect the Amazon Web Services environments used to host Sophos Central, our cybersecurity platform. One of the main benefits that our own security team has gained from Cloud Optix is the ability to focus on what's important.

"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 Mc Kerchar, VP and CISO, Sophos

Secure the network

To guard your resources, you also need to secure the networks that they run on. **Sophos Firewall** delivers unmatched protection and visibility for both on-premises, AWS, and Azure environments.

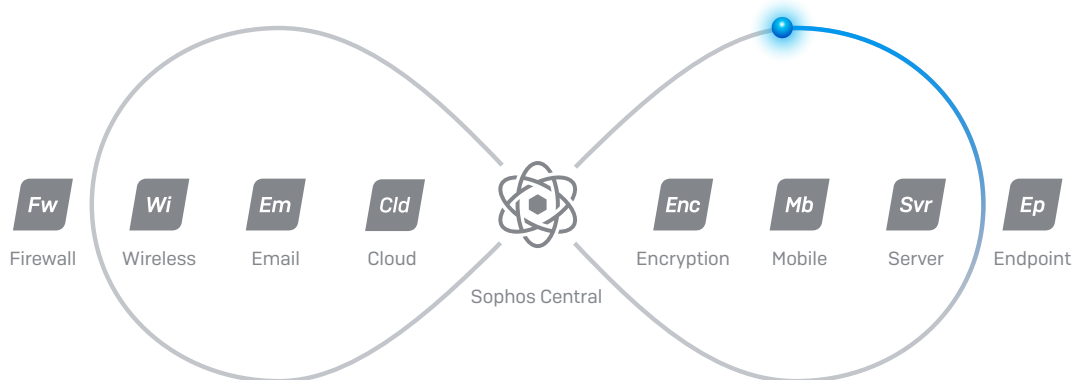
- Integrated, multi-layered protection to stop even the most advanced threats
- Powerful all-in-one solution for WAF, IPS, ATP, URL filtering, path-based routing, and country-level blocking, with extensive reporting, including full insight into user and network activity
- Cloud application visibility, shadow IT discovery, and automated threat response
- Ability to harden your cloud workloads against hacking attempts like SQL injection and cross-site scripting while providing secure access to users with reverse proxy authentication
- Flexibility to run as a standalone and high-availability solution

And to make cloud-based deployment easy, everything is available in a single, preconfigured virtual-machine image.

Simplify Management

With Sophos, you can manage all of your security through a single web-based platform: Sophos Central. No more jumping from console to console to secure your organization; everything is in one place. It also enables you to conduct cross-product investigations with ease, correlating data from multiple services easily.

And because Sophos Central is hosted in the cloud, it's ideal for dispersed IT teams. With over 400,000 users worldwide, you can relax knowing you're using the world's most trusted cybersecurity platform.



Securing the Anywhere Organization

Sophos Central also enables Sophos products to share real-time threat health and security information and work together to automatically respond to threats—what we call Synchronized Security. Benefits include:

- Automated incident response. If a Sophos product detects something suspicious—such as a malware infection or a device out of compliance—it shares this information with the rest of the cybersecurity system. The other products then respond automatically to the incident, in seconds. For example:
 - Sophos Firewall instantly isolates infected devices, preventing the threat from spreading and blocking lateral movement.
 - Intercept X automatically scans an endpoint when compromised mailboxes are detected, limiting the impact of email-borne threats.
 - Sophos Wi-Fi restricts network access for non-compliant devices, keeping rogue and insecure devices off your wireless network.
- Unique insights. IT teams enjoy increased visibility and control of their network, including the ability to:
 - Identify infected by name rather than IP address, speeding up security investigations.
 - Identify all apps on the network. On average, 43% of network traffic passes through as ‘unclassified,’ so the IT team has no idea if it’s good, bad, or malicious. With Synchronized Security, Sophos Firewall and Intercept X work together to automatically identify and classify ALL apps on the network.

Unmatched Protection. Unmatched Efficiency.

Running a Sophos cybersecurity system gives you next-gen protection, a single management platform, the sharing of threat intelligence across products, and automated incident response. Together, these capabilities deliver tremendous efficiency and productivity gains for IT teams.

In fact, customers running Sophos Intercept X and Sophos Firewall, managed through Sophos Central, consistently say that they are able to **double the efficiency of the IT team** while also enjoying **an 85% drop in security incidents**.

“Having tools that automatically detect and correct most security events enables our small IT team to manage the company’s security and prevent it being compromised.”

Chief Technology Officer, Software Services Provider

Securing Any location. Any device. Any resource.

There's no turning back from the move to flexible, remote working and the growing use of the cloud. They make lives easier, but they also pose new challenges for IT teams and new opportunities for bad actors. Securing this new environment requires secure connections, secure resources, and secure devices, wherever they are—without adding to IT overheads.

Sophos can help you address these modern challenges with powerful, trusted solutions.

Contact your Sophos representative to discuss your requirements, or activate a [no-obligation free trial](#) to take any of our products for a test drive.

1 <https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently>²

2. Footnote The State of Ransomware 2020, Sophos

3. Footnote The State of Cloud Security 2020, Sophos

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com