SOPHOS

Cybersecurity Guide for Government Agencies

Sophos' expert threat analysts and world-leading threat intelligence help you to identify and respond to advanced threats faster, 24/7.

Governments hold highly sensitive data, ranging from information on individual citizens to information related to national security and critical infrastructure that can be disrupted by cyberattacks. Securing this huge volume of data can be difficult, but not doing so can be catastrophic for a nation. Shrinking budget and resources of IT teams and a wide network of contractors and third-party suppliers that, if breached, can give entry into government networks, increase cybersecurity risks in government agencies.

Sophos secures government agencies against a wide range of cyberattacks, including human-led threats that technology alone cannot prevent. From managed detection and response (MDR) to endpoint and network security, Sophos enables government agencies to optimize their defenses and frees IT teams to focus on the business.

A Sophos Whitepaper. April 2023

Cybersecurity Challenges in Government Agencies

Government agencies are increasingly attractive targets for cybercriminals who may be financially or politically motivated to steal or manipulate sensitive data. Rapid digitization in government organizations and a significant rise in remote systems access as a result of the pandemic have led to a wider attack surface in government agencies. Expectedly, cyber threats in the government sector continue to grow in both volume and complexity.

A 2022 Sophos survey of 199 IT professionals working in the state and local government sector revealed that 58% of organizations were hit by ransomware in 2021 – a massive 70% increase in the rate of ransomware attacks over the previous year. 72% of respondents reported that their data was encrypted following an attack – one of the highest encryption rates across all sectors.

It's not just ransomware. The overall IT environment in the state and local government organizations has become even more challenging: 59% of organizations reported an increase in attack volume and complexity over the last year, and 56% reported an increase in the impact of attacks.

58%
of state/local government organizations hit with ransomware in 2021

72%
of attacks on state/local government sector resulted in data being encrypted

>1 Month
21% of state/local government organizations took over a month to recover following an attack

82%
in this sector who were hit by ransomware said it impacted their ability to operate

59%
in state/local government sector observed an increase in the volume and complexity of attacks

58%
data recovered by state/local government organizations after paying the ransom

63%
State/local government organizations whose data was encrypted used backups to restore data

80%
Cyber insurance coverage against ransomware in state/local government organizations

Source: Sophos' global survey on The State of Ransomware 2022

Behind these statistics are several changes in the threat landscape:

The professionalization of cybercrime
One of the most significant developments over the last year has been the development and professionalization of the cyber threat economy. Criminal groups increasingly specialize in a particular component of an attack, for example, initial access, ransomware, information-stealing malware, and more, and offer it as a service to other criminals. These 'as-a-service' models lower the skill threshold required to conduct an attack, increasing the volume of adversaries and threats.

These specialist services provide execution guidance and resources for their criminal customers, enhancing the effectiveness of the attacks. Illustrating this point, in March 2022, an associate of the Conti ransomware-as-a-service group published an archive that included a rich trove of documentation and guidance designed to instruct an "affiliate" attacker in the steps required to conduct a ransomware attack.

Attackers are also adopting many of the behaviors of legitimate IT service providers, including asking ransomware victims to 'rate their service' once they have decrypted the files post-payment.

The evolution of attacker tactics, techniques, and procedures
Adversaries frequently exploit weaknesses in organizations' security posture to avoid being stopped by security solutions. These include:

- **Exploiting unpatched vulnerabilities** – This was the number one method adversaries used to penetrate organizations in attacks that Sophos' incident responders were brought in to remediate last year, used in 47% of incidents.
- **Exploiting legitimate IT tools** – Many of the top tools used by IT professionals are also abused by adversaries, including PowerShell, PsExec, and PowerShell, to exploit stolen access data and credentials. By posing as legitimate users, attackers hope to trick their way into an environment.

The cybersecurity challenges for this sector don't end here. Government agencies also need to contend with insider threats (both malicious and accidental), strict regulatory compliance requirements, and third-party vendor risks, amongst other challenges.

Sophos Security for the Government Sector

Sophos delivers advanced cybersecurity solutions that enable the government sector to manage and reduce cyber risk. Our adaptive cybersecurity ecosystem provides a full portfolio of market-leading services and products that elevate our customers' defenses against even the most advanced threats, all powered by the unparalleled threat, AI, and security operations expertise of Sophos X-Ops.

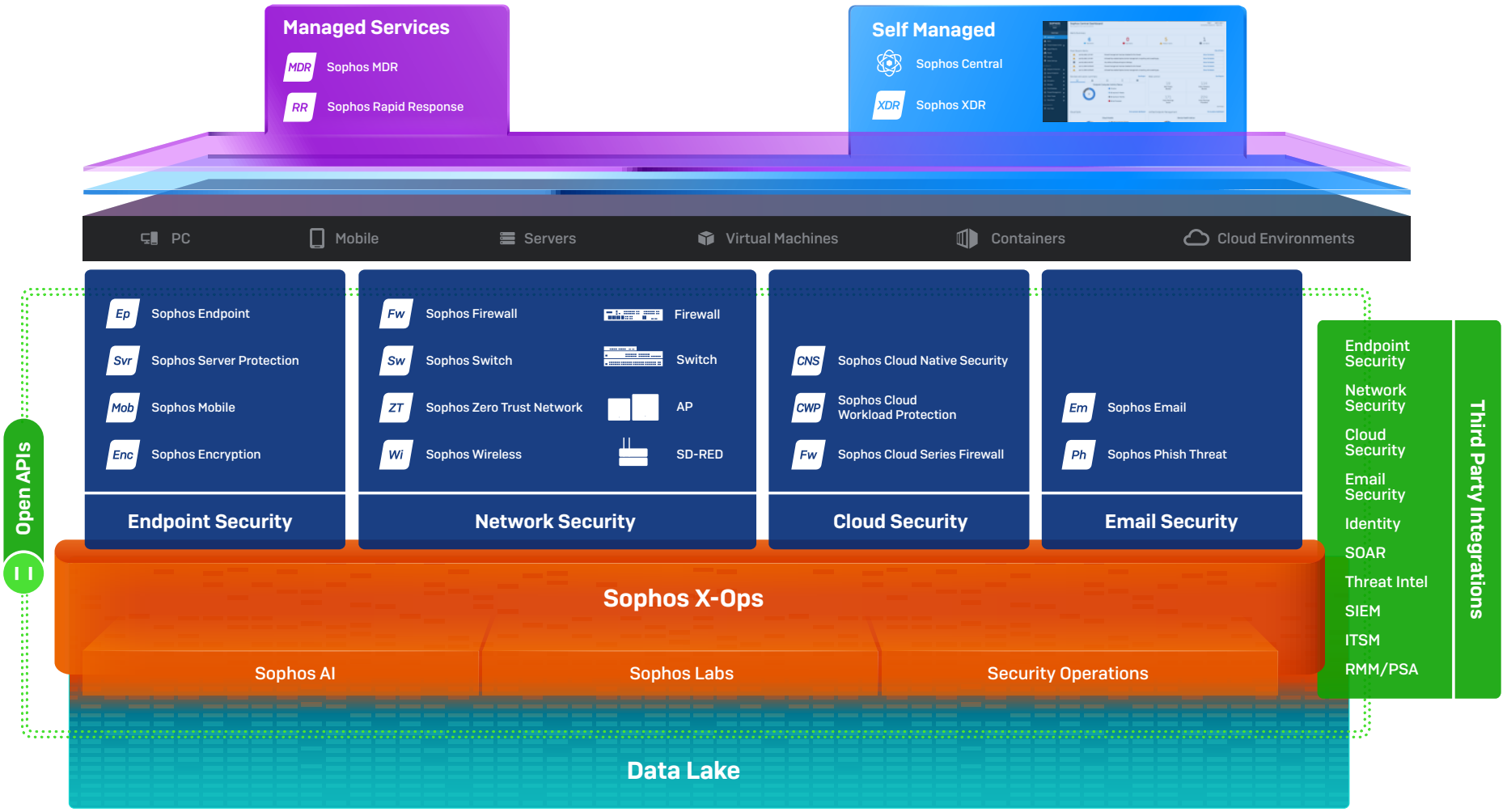
Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally.

No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos.

The **highest rated** and **most reviewed** MDR Service, Endpoint and Firewall on Gartner Peer Insights.

As of August 1, 2022

Sophos Adaptive Cybersecurity Ecosystem



Use Cases

Sophos can help address the most common cybersecurity challenges facing government agencies.

Stopping Advanced Human-Led Attacks, Including Ransomware

Sophos MDR is a fully-managed, 24/7 service delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.

"Sophos MDR frees us up to do more interesting and more development-style work rather than just day-to-day security support."

UK Independent Parliamentary Standards Authority

With Sophos MDR, our expert analysts detect and respond to threats in minutes – using your preferred technology – whether you need a full-scale incident response or assistance making more accurate decisions.

We use:

- Sophos' award-winning solutions, including our endpoint, firewall, cloud, and email protection
- Products from other vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others
- Any combination of our technology and other vendors' technology

Sophos MDR protects your organization from advanced attacks that technology solutions alone cannot prevent while increasing the return on your existing investments. As the world's most trusted MDR provider, we have unparalleled depth and breadth of expertise in threats facing the government sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one government organization customer to all other customers in the industry, elevating everyone's defenses.

MOST TRUSTED	TOP RATED	BEST PROTECTION
#1 Provider	**4.8/5** Gartner Peer Insights	**38 mins** to detect, investigate, respond
More organizations trust Sophos for MDR than any other vendor	Highest-rated and most reviewed MDR solution as of August 1, 2022	Our analysts are over 5X faster than the fastest in-house SOC teams

As of September 2022

Securing Against Phishing Attacks

Phishing attacks in government agencies are a growing issue and the impact can be enormous, given the scale and critical nature of the data they hold. Phishing attacks are becoming more sophisticated, more so in the context of government agencies where the intention could be to take over the victim's device for surveillance or spying, besides the usual reason for stealing credentials.

One of the best ways to stop phishing attacks is to train your employees on how to recognize a phishing scam. Create a positive security awareness culture in your organization with Sophos Phish Threat which offers a collection of more than 30 security awareness training modules to educate and test your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics.

Allow only trusted senders into your employees' inboxes with Sophos Email that scans all inbound messages for key phishing indicators such as brand spoofing and impersonation attempts in real-time using SPF, DKIM, and DMARC authentication techniques and email header anomaly analysis. This helps to spot and block phishing emails before they reach your users. You can further prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with the discovery of financials, confidential contents, and PII in all emails and attachments.

Most phishing attacks infect the access points to your network by luring recipients to click on a malicious link that leads to downloading malware on the device or giving access to sensitive data to hackers. To strengthen your network against phishing attacks you must strengthen your endpoint security. Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution.

To optimize your defenses, you need layered protection: multiple sophisticated security capabilities with each playing its part in defending against advanced attacks. Sophos Endpoint is packed with these layers of protection, including:

- Credential theft protection that prevents unauthorized system access.
- Exploit protection to stop the techniques adversaries use.
- Anti-ransomware protection which identifies and blocks malicious encryption attempts.
- Tamper protection that prevents adversaries from turning off defenses so they can deploy their payloads.

Combining multiple layers of protection technologies enables us to optimize our customers' defenses. Testament to the quality of our defenses – and the power of layered protection – we stop 99.98% of threats up-front (AV-TEST average score), and recently earned perfect scores in SE Labs endpoint protection report.

Protecting Against Hacktivism

The intent of hostile state-sponsored cyber attackers is political cyber warfare more than financial gain. They hack government systems to disrupt essential services, threaten national assets, and to bring embarrassment or erode trust in the government. Once hacked, government agencies become a gateway for cyber attackers to access systems of interlinked government departments, third-party vendors, and corporate entities working with them. Weak cyber defenses, unpatched and out-of-date systems and apps, and inadequate visibility into IT security incidents are a few reasons why government agencies are soft targets for acts of hacktivism.

Sophos Firewall offers powerful protection from the latest advanced cyber threats while accelerating your important SaaS, SD-WAN, and cloud application traffic. Recognized as a Gartner Customers' Choice for Network Firewalls 2022, Sophos Firewall tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain. It offers flexible and powerful segmentation options via zones and VLANs. This provides ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.

Sophos XDR can help you keep the systems and apps updated with regular patch management by offering the most complete view of your cybersecurity posture. By pulling in rich data from your network, email, cloud, and mobile data sources, it helps you locate systems and devices that are unpatched or have out-of-date software.

Sophos Managed Detection and Response (MDR) service reduces the threat response time dramatically for government agencies with a fully managed 24/7/365 service delivered by experts that are armed with critical visibility and context for seeing the entire attack path, enabling a faster, more comprehensive response to security threats that technology solutions alone cannot prevent. Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect citizens' data and classified information wherever it resides.

Protecting Citizens' and Classified Data

All government agencies have vast stores of information ranging from personally identifiable information (PII) on citizens: health, digital identification, and tax information, to sensitive commercial corporate data, and state and national level secrets. They need to protect this data to preserve national security and the privacy of citizens' data.

Safeguard critical data by training your employees to look out for potential threats and creating a positive security awareness culture in your organization with automated attack simulations and security awareness training with Sophos Phish Threat.

With the huge number of laptops lost, stolen, or misplaced every day, a crucial first line of defense against the loss or theft of devices and the data therein is full-disk encryption. Sophos Encryption can secure government data at rest with full disk encryption for Windows and macOS.

Get absolute control over who can access data on your network with Sophos ZTNA. Establish granular controls to block lateral movement and make sure that only authorized parties can access sensitive data.

Sophos Firewall's flexible and powerful segmentation options via zones and VLANs help you separate levels of trust on the network to reduce cyber-risk exposure to your data stores. For example, databases and servers can be segmented into a DMZ with stricter security measures than other parts of the network to keep the server hosting confidential data secure and separate from other network zones.

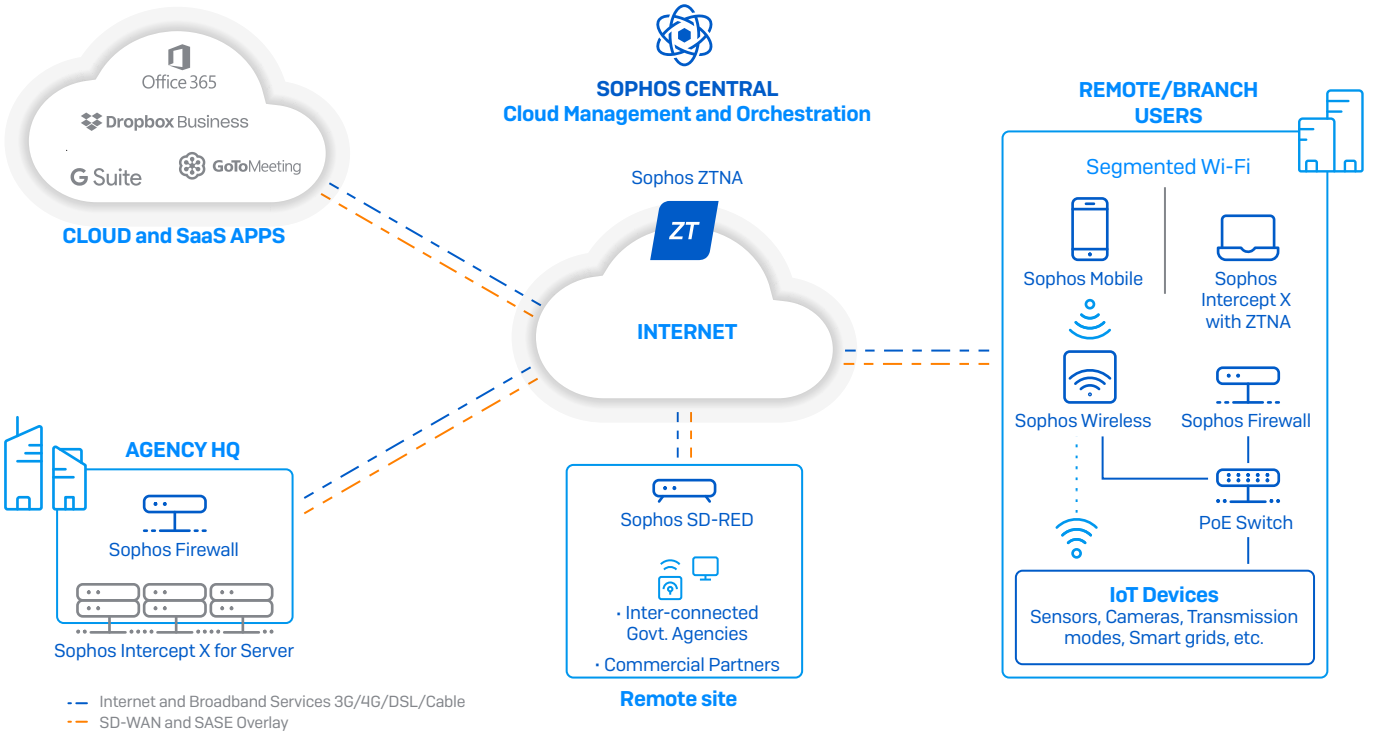
Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across your endpoint devices with Sophos Intercept X endpoint protection. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.

You can prevent data breaches with Sophos Email, which can create multi-rule DLP policies for users to ensure the protection of sensitive information with the discovery of confidential contents in all emails and attachments. It also seamlessly encrypts your sensitive data to stop breaches.

Securing Remote Access Environments

Government data is plentiful, fragmented, and often shared between different government agencies and commercial partners across multiple jurisdictions – all of which make secure remote access a critical need for this sector.

The Sophos Secure Access portfolio connects remote government sites, safely delivers critical cloud and SaaS applications, and facilitates the secure sharing of data and information. It consists of Sophos ZTNA to secure access to applications and data, Sophos SD-RED remote Ethernet devices to extend secure government networks to remote and branch sites, Sophos Wireless access points for easy and safe wireless networking, and Sophos Switch network access layer switches for secure access on the LAN. Everything is managed through Sophos Central, our all-in-one cloud-based security platform.



Protecting Against Insider Attacks

Understaffing and lack of training and resources in many government agencies result in overworked employees that have a higher probability to make mistakes that lead to security breaches. Furthermore, the risk of insiders with authorized access to classified data misusing their privileges is a critical threat that government agencies must act upon.

Get insights into your riskiest users and applications with actionable intelligence from Sophos User Threat Quotient (UTQ) that ensures your policies are enforced before your security is compromised. Take your protection a step further with Sophos Firewall, which protects your sensitive data from accidental or malicious disclosure with complete policy control over web categories, applications, removable media, and mobile devices used in your network. It offers user awareness across all areas of the firewall with user-based access policies for traffic shaping (QoS), and other network resources, regardless of the IP address, location, network, or device.

An alternative safeguard is the principle of least privilege where users have access only to the network resources they need. Sophos Cloud Optix, our Cloud Security Posture Management solution, connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real-time that can help you identify credential misuse or theft. An IAM visualization tool that provides a complete map of IAM relationships allows your IT teams to identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks quickly and easily.

Ensuring Application and Network Availability

Government organizations provide critical services, such as tax payments, healthcare, etc., online to citizens. To ensure continuous access to these services, government networks and applications must be available 24/7. However, attack vectors like malware and bots, social engineering attacks, and DDoS attacks threaten the smooth functioning of the government's online web and application services.

Sophos Firewall, with industry-leading machine learning technology and powered by SophosLabs Intelix, delivers advanced protection from the latest drive-by and targeted web malware, URL/malicious site filtering, and cloud-based filtering for offsite protection. Combined with our enterprise-class web application firewall, it protects your critical business applications from hacks and attacks while enabling authorized access.

The exploit prevention capabilities in Sophos Intercept X stop vulnerabilities in applications and operating systems from being exploited by attackers. Besides, the endpoint protection application control policies restrict the use of unauthorized applications in government systems.

You can stop the exploitation of vulnerabilities by adversaries with our Managed Detection and Response (MDR) service that provides 24/7 detection, investigation, and neutralization of suspicious activities by human threat experts who are kept up to date on the latest threat and vulnerability developments by Sophos X-Ops.

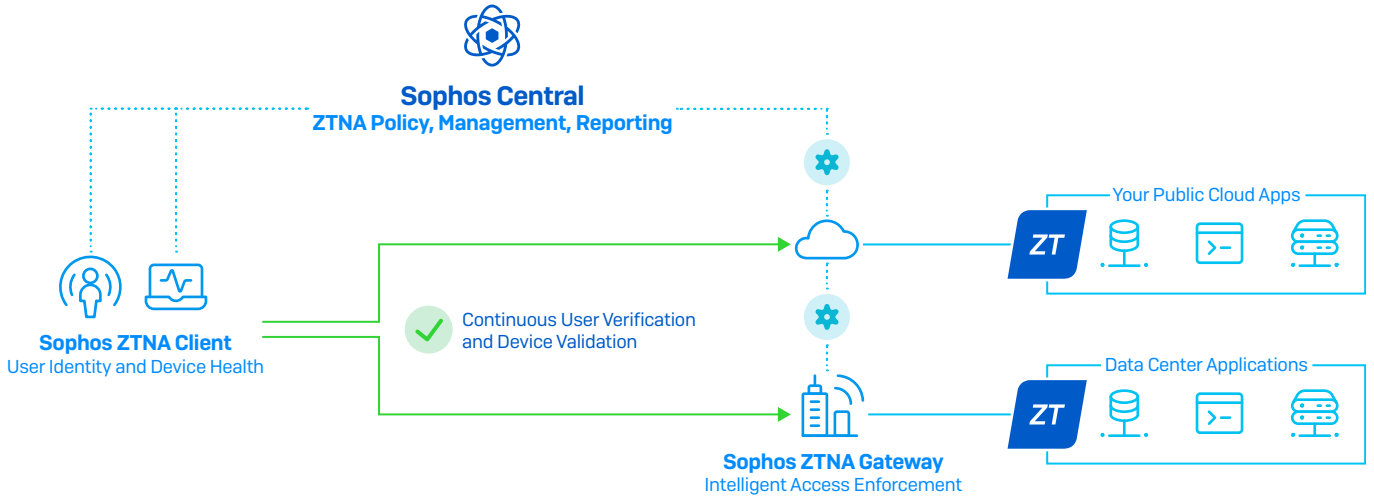
Reducing Risks from Third-party Vendors

It's not just government employees who introduce network access risks. Third-party users like social workers or healthcare staff, vendors, and commercial partners need continuous external access to the network from different devices – increasing the risk of data privacy breaches, fraud, and credential theft.

Defend against threats that infiltrate government agencies via third-party suppliers by using AI, exploit prevention, behavioral protection, and other advanced technologies in Sophos Intercept X. Plus, our powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.

Get 24/7 expert support with over 500 specialists working around the clock to proactively hunt for, validate, and remediate potential third-party vendor threats and incidents on your behalf with Sophos MDR.

Protect against third-party vendor attacks that rely on external access to your systems via very granular access controls with Sophos ZTNA, which authenticates requests from trusted partners, irrespective of their location. The unique integration of Sophos Endpoint and Sophos ZTNA automatically prevents compromised hosts from connecting to networked resources, preventing threats from moving laterally and getting a foothold on your network.



Securing Data Across Multi-Cloud Environments

Cloud adoption in government organizations offers benefits of flexibility, scalability, cost savings, increased collaboration, and easy shareability of information. But the cloud is also a major target for cybercriminals looking to exploit less established cybersecurity practices than in traditional on-premises environments.

Sophos Cloud Native Security provides complete multi-cloud security coverage across environments, workloads, and identities. It protects your cloud infrastructure and data with flexible host and container workload security for Windows and Linux. Multi-layered technologies protect against ransomware and other advanced attacks including cloud-native behavioral and exploit runtime detections that identify threats such as container escapes, kernel exploits, and privilege-escalation attempts. Plus, it also makes it easy to keep on top of your cloud spend. You can quickly identify if your account is being abused and eject the adversaries before they rack up a big bill.

Conclusion:

Cyberattacks like ransomware, DDoS attacks, exploits, and phishing can have severe business and reputational consequences for government agencies. Protecting your IT environments and sensitive data requires an integrated security approach.

Sophos protects your systems and data wherever they exist with our next-gen services and technologies while enabling you to consolidate your security management with a single vendor. All Sophos solutions are controlled through a unified cloud-based management console, Sophos Central, which allows real-time information sharing between products, centralized management, automated incident response, and deeper insights – all of which, working together, further elevates your protection while enhancing the efficiency of your IT team.

To learn more about how Sophos secures government agencies and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-04-21 EN-WP (NP)

SOPHOS