SOPHOS

Cybersecurity Guide for Retail

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

Retail holds the personal and financial information of customers, making it a popular target for cyberattacks such as phishing, credential stuffing, attacks on IoT devices, ransomware and DDoS attacks, and supply chain attacks. Point-of-sale systems are an increasingly popular point of attack for acquiring transaction data and for entry into more critical systems connected to the POS, such as billing, inventory, etc. Such attacks on retailers can lead to heavy penalties for non-compliance with regulatory mandates like PCI DSS and GDPR, and data, financial, and reputational losses.

Sophos secures retail organizations 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 retailers to optimize their defenses and frees IT teams to focus on the business.

A Sophos Whitepaper. March 2023

Cybersecurity Challenges in Retail

The cybersecurity challenges for the retail sector continue to grow with increased digitization and integration of IoT devices to enhance customers' buying experience. Besides this, cyber threats in this sector continue to grow in both volume and complexity.

A 2022 Sophos survey of 422 IT professionals working in the retail sector revealed that 77% of organizations were hit by ransomware in 2021 – a massive 75% increase in the rate of ransomware attacks over the previous year. Moreover, the average cost for mid-sized retail organizations to remediate a ransomware attack came in at $1.27M.

It's not just ransomware. The overall IT environment in retail has become even more challenging: 55% of organizations reported an increase in attack volume and complexity over the last year, and 51% reported an increase in the impact of attacks.

77%
of retail organizations hit with ransomware in 2021

$1.27M
average cost to remediate following an attack

>1 Month
17% of retail organizations took over a month to recover following an attack

92%
of retail organizations hit by ransomware said it impacted their ability to operate

55%
of IT pros in retail sector observed an increase in the complexity of attacks

62%
data recovered by retail organizations after paying the ransom

68%
of attacks on retail resulted in data being encrypted

5%
of retail organizations recovered ALL data after paying the ransom

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

Behind these statistics are several changes in the threat landscape:

The professionalization of cybercrime

Over the last year, one of the most significant developments 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. Retail organizations 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 Retail Sector

Sophos delivers advanced cybersecurity solutions that enable retail organizations 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.

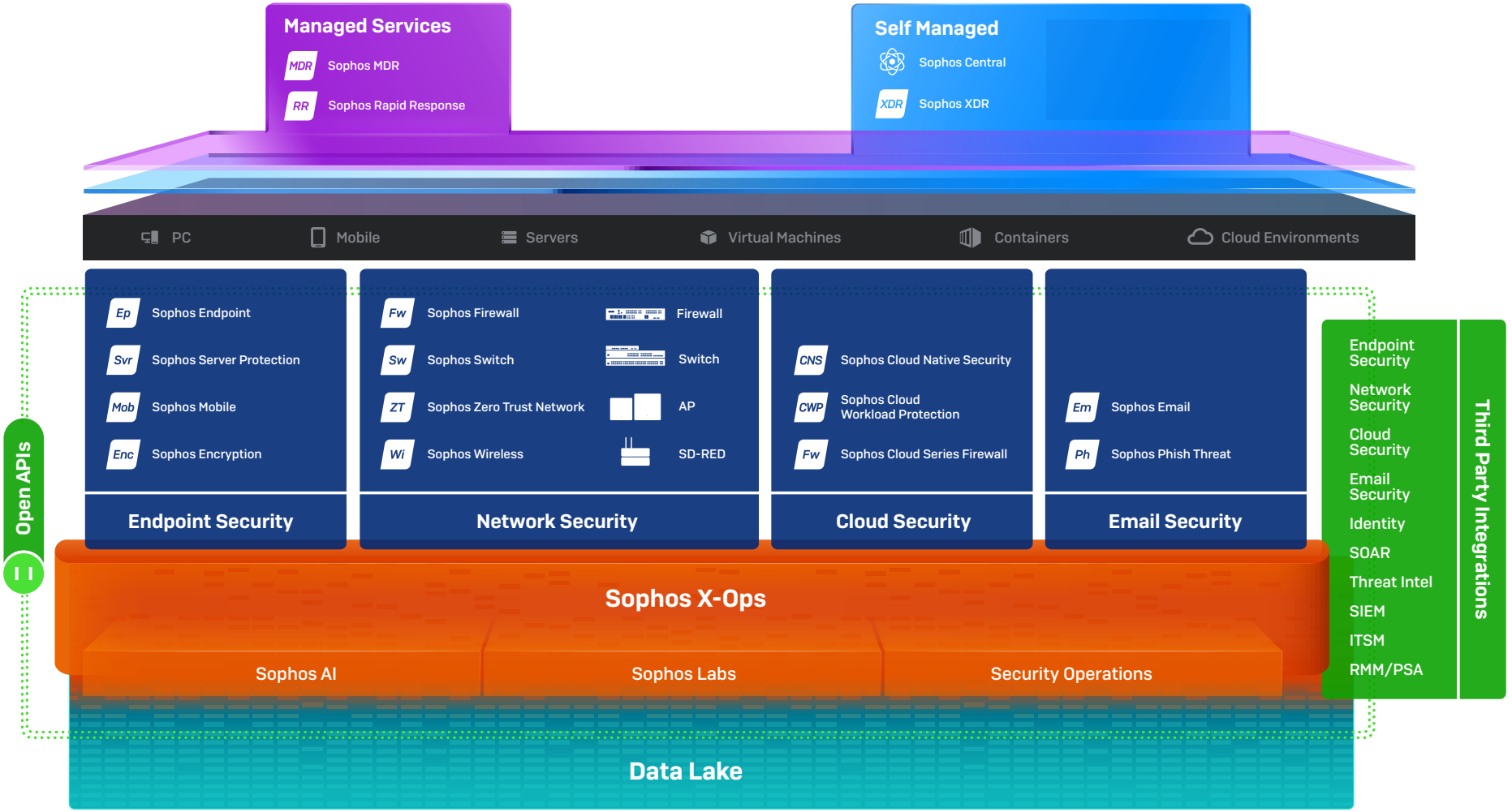
Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally.

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 retail organizations.

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.

"Because Sophos MDR is there, we can prop up and mature other areas of the organization like vulnerability management, patching, and security awareness."

The Fresh Market, U.S.

"We appreciate that Sophos keeps on top of the latest activity and threats, so we can focus on delivering a secure, world-class service for customers and artists."

CD Baby, U.S.

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 retail sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one retail 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 Scams

Phishing attacks are one of the easiest ways for scamsters to gain access to your system and valuable credit card and payment information.

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 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.

Securing Against POS System Attacks

A point-of-sale (POS) system combines hardware and software that work together to enable organizations to process payment transactions, record sales, manage inventory and customers, etc. POS systems are increasingly becoming a popular point of attack in retail organizations to hack transactional data and give access to valuable information like credit card data and PINs to cybercriminals.

Tighten your POS security by stopping hackers from exploiting vulnerabilities in applications and operating systems with the exploit prevention capabilities in Sophos Endpoint Protection. Sophos' Server Workload Protection automatically scans your system for known good applications, whitelisting only those applications and blocking unauthorized applications from running in the system. For security of your cloud POS systems, Sophos Cloud Optix continually monitors your multi-cloud environments to detect unsanctioned activity, vulnerabilities, and misconfigurations and provides detailed threat remediation steps.

Retail organizations must keep their POS and server endpoints updated with regular patch management as they are easy targets for malware attacks. Sophos XDR gives you the most complete view of your cybersecurity posture by pulling in rich data from your network, email, cloud, and mobile data sources and helping you locate systems and devices that are unpatched or have out-of-date software.

POS systems and their data can be kept secure by monitoring the retail environments for any anomalous activity and indicators of threats. Sophos Managed Detection and Response (MDR) continuously monitors signals from across your security environment to help you detect potential cybersecurity events quickly and accurately. We detect, investigate, and correlate anomalous behaviors and code use to identify malicious activities and quickly neutralize the event.

Securing your network

Sophos Firewall offers powerful protection from the latest 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.

Network segmentation is an effective way by which retail organizations can reduce their cyber-risk exposure and return to business as usual faster after a security breach. Sophos Firewall 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. For example, databases and servers are often 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.

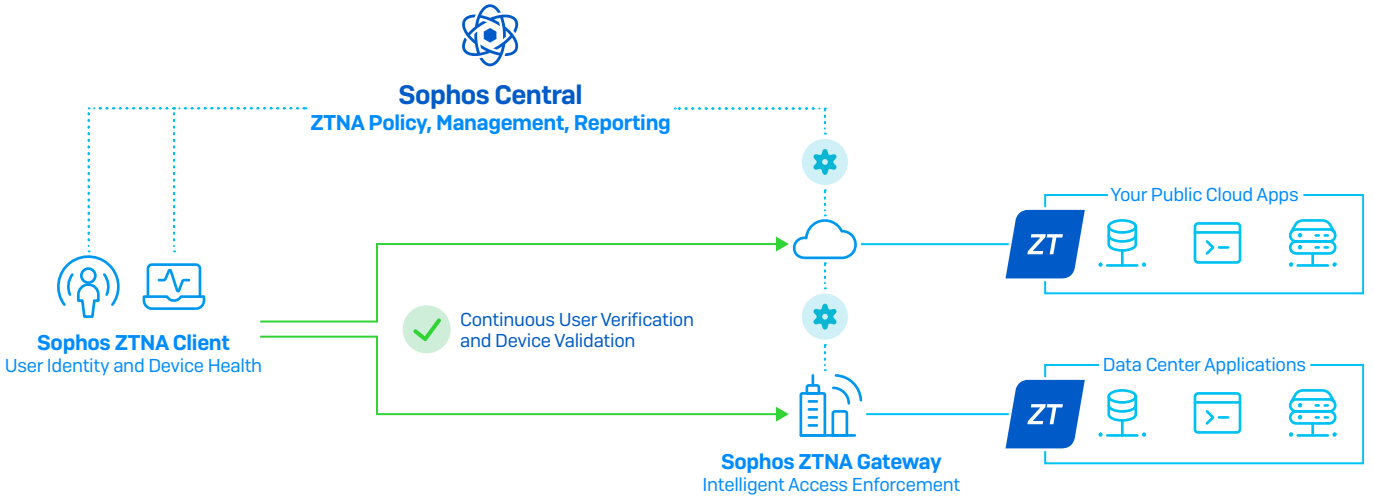
You can also segregate your traffic at the switch level with Sophos Switch, which allows you to configure VLANs to segment your internal traffic and reduce the attack surface in case of a security breach or infection.

Reducing Supply Chain Risks

Retailers rely on a vast supply chain network to keep their business and stock moving. A retailer's supply chain network will consist of a network of third-party vendors who often require remote access to critical resources, systems, and data in order to support different aspects of the business. This increases the risk of misuse of access privileges which may lead to credential and data theft.

Sophos ZTNA safeguards your organization against supply chain attacks that rely on supplier access to your systems via very granular access controls. It removes implicit trust by validating user identity, device health, and compliance before granting access to resources. It only connects users to very specific applications or systems, not the entire network. The unique integration of Sophos Endpoint and Sophos ZTNA allows them to share status and health information to automatically prevent compromised hosts from connecting to networked resources preventing threats from moving laterally and getting a foothold on your network.

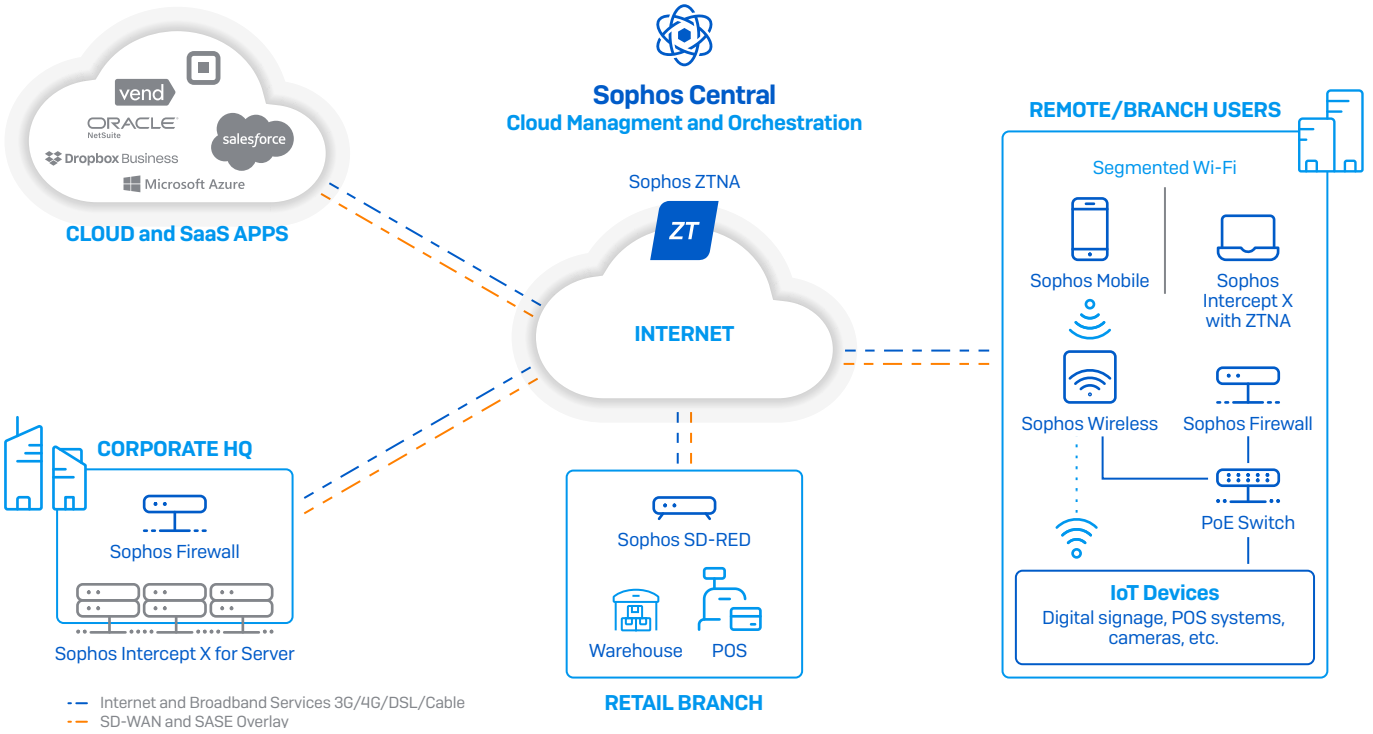
Sophos Mobile supports the BYOD environment in your setup by ensuring sensitive company and customer data is safe. Ensure secure remote access for your employees accessing the corporate network from any device with Sophos Mobile's Enterprise Mobility and security management capabilities. Stay assured with flexible compliance rules that monitor device health and flag deviation from desired settings.



Securing Distributed and Diverse Retail Environments

Retailers have a vast network of people, technologies, and software to manage different aspects of business, including vendor access, logistics, inventory, and cardholder data management. They must secure distributed sites that use multiple devices, platforms, and customer-facing web and mobile applications to ensure positive customer experiences and operational efficiencies in all stores. What most retailers need is a robust and reliable network infrastructure with superior application performance, segmentation to separate their guest and corporate Wi-Fi networks, secure connectivity with warehouses to ensure optimal inventory and with central headquarters to access marketing and financial data, etc.

The Sophos Secure Access portfolio connects your remote and branch sites, delivers your critical cloud and SaaS applications, and lets you securely share data and information. It consists of Sophos ZTNA to secure access to your applications, Sophos SD-RED remote Ethernet devices to safely extend your network to your remote and branch sites, Sophos Wireless access points for easy and secure 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.



Securing Against Business Email Compromise (BEC) Scams

Business email compromise (BEC) scams targeting senior management executives, HR departments, or third-party vendors are on the rise in retail organizations. In such scams, cybercriminals use social engineering skills to impersonate someone the recipients trust and trick them into payroll frauds, providing sensitive company information, sending money, etc.

Sophos Email uses advanced Natural Language Processing (NLP) machine learning to block these targeted impersonation and Business Email Compromise attacks. For added protection, Sophos Email also includes a setup assistant that integrates with AD Sync to automatically identify the individuals within an organization who are most likely to be impersonated. It scans all inbound mail for display name variations associated with those users, further extending protection against phishing imposters.

Meeting Regulatory Requirements

Retailers face strict data security requirements by regulations and standards such as PCI DSS, GDPR, HIPAA, and SOC2 due to the vast private and sensitive data they hold.

Ensuring encryption of critical corporate and customer records and transactions, PII, and other sensitive data can mean the difference between a safe harbor and the need for public breach notification. Sophos Device Encryption protects your devices and data with full disk encryption for Windows and macOS that helps you to verify device encryption status and demonstrate compliance.

Sophos Cloud Optix helps you eliminate compliance gaps with a single view of your compliance posture across AWS, Azure, and Google Cloud environments. Continuously monitor compliance with custom or out-of-the-box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2.

In recent years, mobile devices have become ubiquitous and employees are constantly connected to the company database and other corporate resources using smartphones, tablets, or laptops. However, easy access to critical business data on mobile devices threatens the security of sensitive corporate and customer data held by retail organizations. Sophos Mobile ensures the integrity of your sensitive data on mobile devices by enforcing device encryption and denying access to email, network, and other resources if a device is not compliant with the company policy.

Securing Resources in the Cloud

The cloud is integral to the successful day-to-day operations of almost all retail organizations. It offers greater speed and flexibility than traditional on-premises resources, as well as the opportunity to move from one-off capital expenses to distributed operating costs. 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, exploits, and phishing can have severe business and reputational consequences for retail organizations. 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 retail organizations and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-03-23 EN-WP (NP)

SOPHOS