SOPHOS

Cybersecurity Guide for Finance and Banking Organizations

Cybersecurity that detects, responds to, and resolves threats faster with AI-driven, human-led 24x7 threat intelligence.

The finance and banking sector is on a fast path to digital transformation. By leveraging cloud apps, open banking, Fintech, and third-party suppliers, the sector's offering to its customers is increasing– but so is its attack surface. With a massive database of critically sensitive PII, corporate, and financial data in its possession, finance and banking continues to be an attractive target for cyber attackers.

Sophos secures finance and banking institutions 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 organizations to optimize their defenses and frees up IT teams to focus on the business.

A Sophos Whitepaper. February 2023

Cybersecurity Challenges in Finance and Banking

The challenge facing defenders in finance and banking continues to grow as cyber threats increase in both volume and complexity.

A 2022 Sophos survey of 444 IT professionals working in financial services revealed that 55% of organizations were hit by ransomware in 2021 – a 62% increase over the previous year. Moreover, the average cost for mid-sized financial services providers to remediate a ransomware attack came in at $1.59M.

It's not just ransomware. The overall IT environment in financial services has become even more challenging: 55% of organizations reported an increase in attack volume over the last year, 64% reported an increase in attack complexity, and 55% reported an increase in the impact of attacks.

55%
of financial services organizations were hit with ransomware in 2021

64%
of IT pros observed an increase in the complexity of attacks

$1.59M
average cost to remediate following an attack on financial services

63%
of data recovered by financial services organizations after paying the ransom

>1 Month
12% of financial services organizations took over a month to recover following an attack

54%
of attacks on financial services resulted in data being encrypted

91%
of organizations hit by ransomware said it impacted their ability to operate

10%
of financial services recovered ALL data after paying the ransom

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

Behind these statistics are a number of 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 in an attempt 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. Finance and banking also need to contend with insider threats (both malicious and accidental), strict regulatory compliance requirements, third-party vendor risks, and legacy infrastructure that is hard to keep up to date, amongst other challenges.

Sophos Security for Finance and Banking

Sophos delivers advanced cybersecurity solutions that enable finance and banking 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.

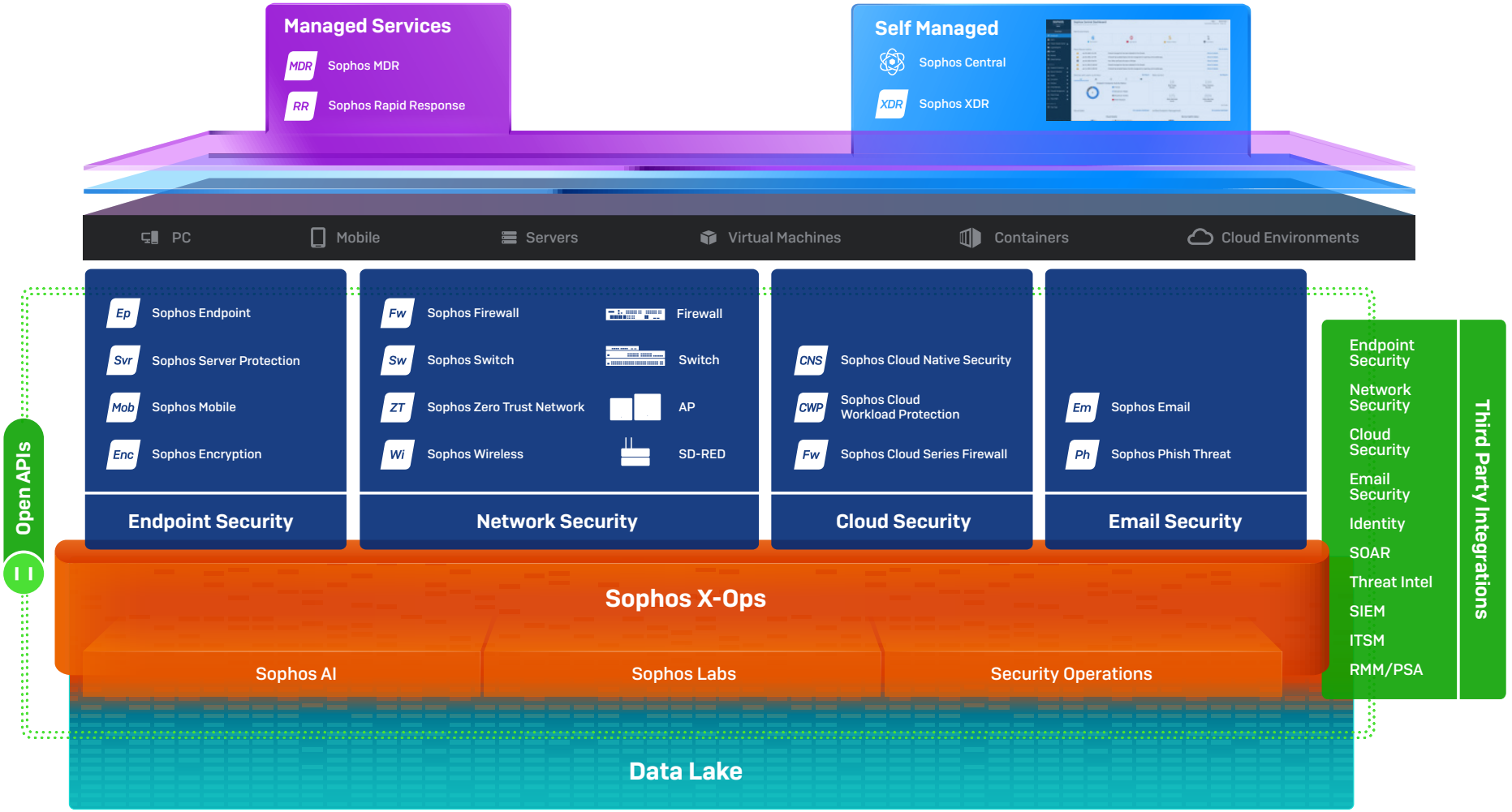
Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally.

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 finance and banking 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.

"The IT team has saved at least 40 hours a week that would otherwise have been spent on security operations tasks."

AAVAS Financiers Limited

"Sophos MDR helped us keep up with the growing volume and sophistication of cyberthreats without ramping up our security operations team."

Tourism Finance Corporation of India Limited

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 finance sector. Leveraging this extensive telemetry, we can generate 'community immunity', applying learnings from defending one finance and banking organization to all other customers in the sector, 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 Your Devices

Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution.

With cybersecurity, there is no silver bullet, no single protection capability that will stop every threat. Each attack combines a different set of tactics, techniques, and procedures (TTPs), and as a result, there is no 'one size fits all' protection 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 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.

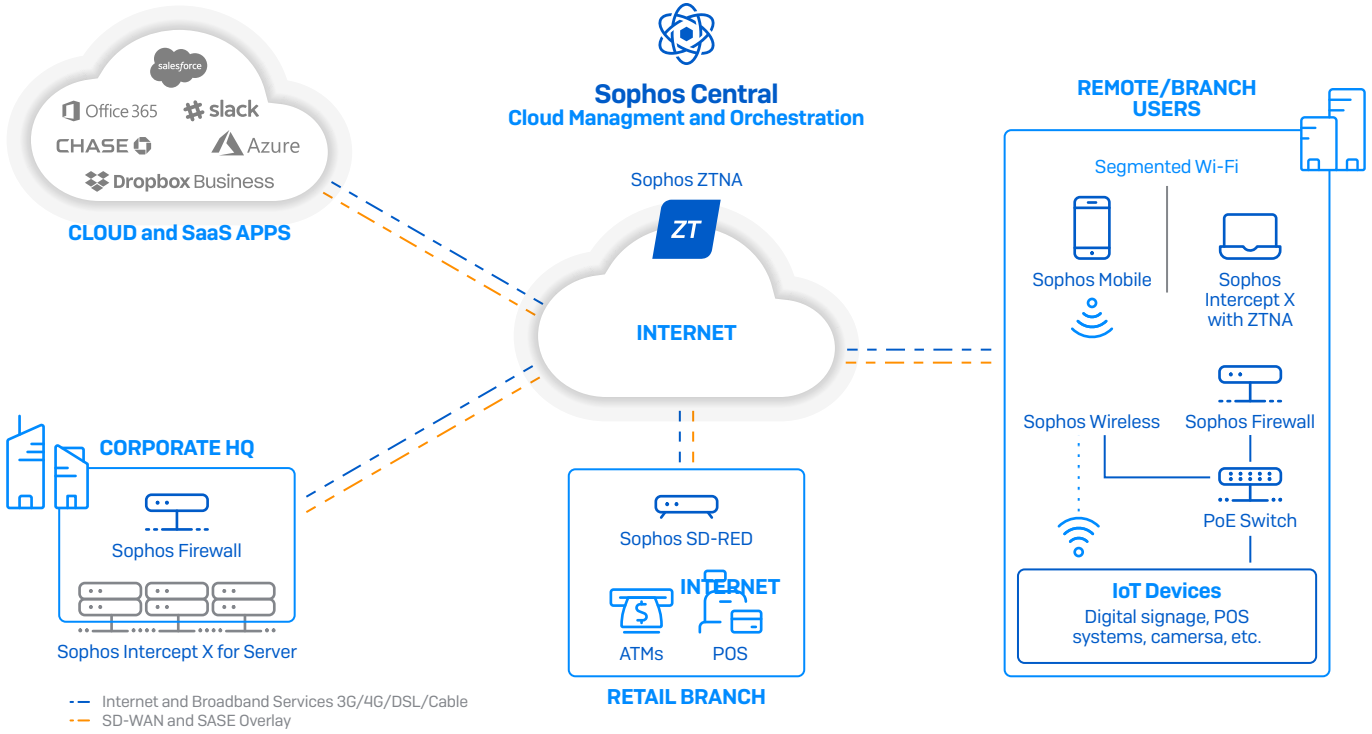
Network segmentation is an effective way by which finance and banking organizations can reduce their cyber-risk exposure and return to business as usual faster after a security breach. Sophos Firewall offers flexible and powerful segmentation options via zones and VLANs. This provides ways to separate 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.

Securing Branch Offices

Many firms need to connect their local, state, and national branch sites that share large amounts of sensitive information every day. They must protect personal and corporate data and financial transactions from cyber threats while keeping up with the continued growth of connected IoT devices such as ATMs and security cameras. Digitization plans include enabling new technologies and applications on the network, such as mobile banking, e-signatures, digital signage, and videos – while complying with PSD2, PCI DSS, and GDPR regulatory mandates.

Financial institutions can connect remote and branch sites, deliver critical cloud and SaaS applications, and share data and information with Sophos Secure Access portfolio. It includes Sophos ZTNA to support secure access to applications, Sophos SD-RED remote Ethernet devices to safely extend your network to branch offices and remote devices, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch for secure access on the LAN. Everything is managed through a single cloud-based security platform – Sophos Central.



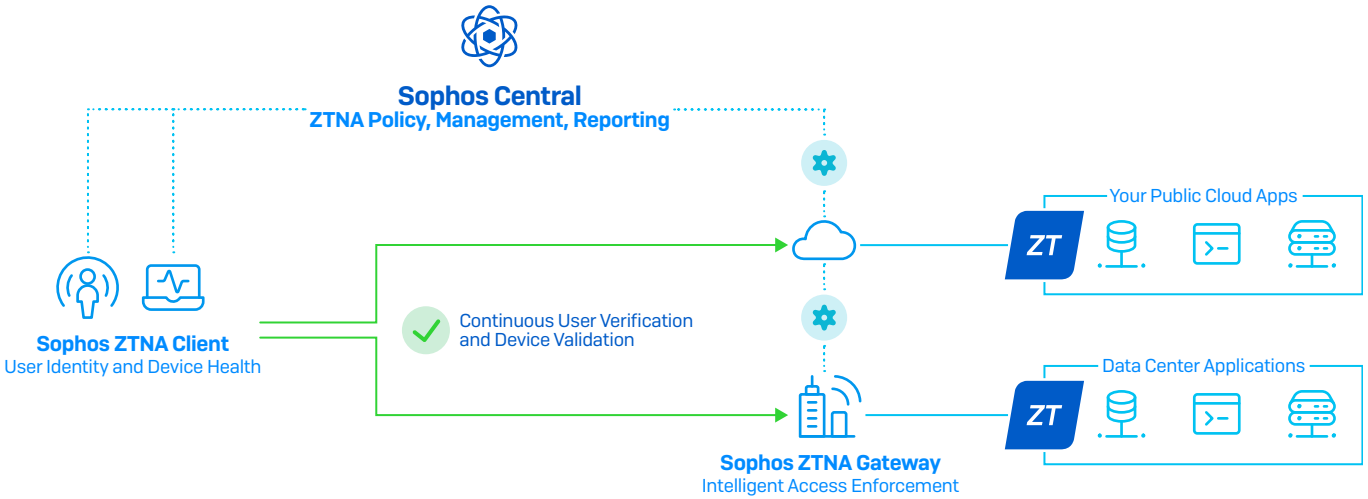
Providing Secure Remote Access

The hybrid and remote workspace accelerated by the pandemic has put pressure on the finance and banking sector to set up a secure way for employees to connect to their work network using any device. Sophos solutions enable your staff to connect securely from any location – without worrying about potential security breaches.

Sophos ZTNA eliminates vulnerable VPN clients, enabling you to offer secure and seamless access to resources for your remote workers defined by policies. By removing implicit trust in your environment's applications, users, and devices, ZTNA allows segmented access to your systems and resources to just those who need it.

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 financial and corporate data is safe and the employee's personal information is private. Now you can allow secure remote access to 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.



Encrypting Sensitive Data to Meet Regulatory Requirements

The finance and banking sector faces strict data security requirements by regulations and standards such as ISO/IEC 27001, GLBA, GDPR, SOX, and PCI DSS due to the vast private and sensitive data it holds. Ensuring encryption of critical financial 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.

In recent years, mobile devices have become ubiquitous in the finance and banking industry thanks to the productivity and efficiency gains they offer. 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 financial and customer data held by banks and financial 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 finance and banking 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. 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.

Reducing Third-Party Vendor Risks

Finance and banking organizations have a vast ecosystem of third-party vendors to support their critical day-to-day operations and facilitate innovative solutions for their customers. However, third-party vendors also expose organizations to cyber risks and vulnerabilities.

Third-party vendors often require remote access to critical resources, systems, and data. 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.

Cybersecurity incidents in your vendor's IT ecosystem can seriously disrupt your operations and the availability of your network and systems. Additionally, in cases when a vendor is breached, banks and financial institutions must conduct security audits and forensic investigations in their own networks and systems. To help you defend against malicious threats that can get in via third-party suppliers and to keep you ahead on audits and forensics, Sophos provides you with a comprehensive solution:

- Sophos Endpoint uses AI, exploit prevention, behavioral protection, anti-ransomware, and more to stop advanced, never-before-seen threats.
- Sophos XDR enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your environment.
- Sophos Managed Detection and Response (MDR) provides 24/7 expert support with over 500 specialists working around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.

Conclusion:

Cyberattacks like ransomware, exploits, and phishing can have severe business and reputational consequences for finance and banking institutions. 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 finance and banking organizations and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-02-28 EN-WP (DD)

SOPHOS