JANUARY 2022

Forbes INDIA

SOPHOS

Proactive Protection Against Known and Unknown Cyber Threats

sophos.com/en-us.aspx

FORBES INDIA MARQUEE

A special marketing presentation complimentary with Forbes India. Not for Sale.

Network 18

Sophos stops ransomware.

SOPHOS

Cybersecurity evolved.

Proactive protection against known and unknown cyber threats

Sunil Sharma, Managing Director- Sales(India & SAARC), talks about how companies need to recognise that security lies not just with management and how Sophos is helping organizations of all sizes with a strong combination of prevention, detection and response to combat cyberthreats.

In 2021, data security emerged as a vital component for companies of all sizes to consider more closely. As a business leader, what is your take on who shoulders the responsibility to ensure adequate security is in place at your company? Are the cyber defenses at your organization up-to-date and current enough to protect against modern and future cyberattacks? Do you think cybersecurity should be left only in the hands of the IT department?

Cybersecurity, in the simplest terms, means an approach through which organizations defend themselves against cybercriminals. Hence, it is logical to understand attacker behaviors to best develop a concrete cybersecurity strategy, in which everyone across an entire organization needs to participate.

Attackers are known to go after three areas of weakness to gain entry into an organization: people, technology and processes. This is why defense-in-depth is important, and while IT can "own" a cybersecurity strategy, the master plan must reach all facets of the business, from phishing awareness

DISCLAIMER: The views and opinions expressed in this supplement are not endorsed by Network 18 Media and Investments Limited. This is a marketing initiative and Forbes India journalists were not involved in producing this supplement.

to regularly patching and applying updates to secure software vulnerabilities.

Even today, companies still view cybersecurity as a business hurdle, especially smaller companies that do not have the resources to build their own security operations. What advice would you give to such companies?

On the contrary, we are seeing more businesses becoming better aware of cybersecurity and they no longer see it as a hurdle. Companies are aware that cybercrime has not been kind to any size or type of organization. At Sophos, we have been witnessing cyberattacks on all types of organizations, across verticals and sizes. However, we agree that the awareness and preparedness needed for cybersecurity is somewhat less likely when it comes to small businesses. Smaller companies can no longer continue to think that they will never be attacked because they are too small and don't have anything substantial that adversaries would want to target. In fact, there are many reasons why adversaries target small and also medium sized organizations. One is that these companies could serve an entry point to bigger organizations – this is also known as a supply chain attack. Some attackers design ransomware, for instance, specifically for small businesses and charge a four figure ransom demands, but on a much frequent basis.

If small to mid-sized businesses have limited resources to apply cybersecurity, they should outsource it to Managed Service Providers (MSPs) who specialize in this area and can work on a tighter budget.

Cybercrime is no longer about whether an organization is big or small – it is about when and how.

What security solutions and services does Sophos offer?

Today's threat landscape demands a strong combination of prevention, detection, and response. Sophos provides a complete ecosystem of security solutions that combines the best protection with efficient detection and response, providing organizations with better security outcomes.

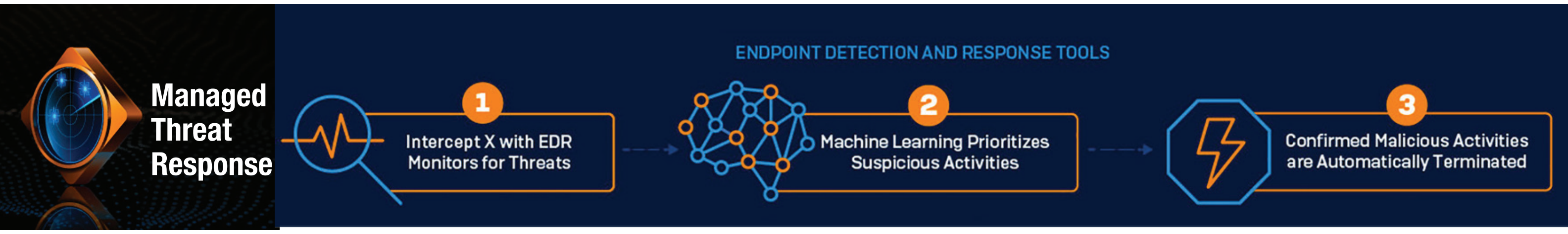
Sophos Firewall protects an organization's perimeter. Many companies have embraced remote working, and Sophos Firewall provides Secure Access Service Edge (SASE) and Zero Trust Network Architecture (ZTNA) capabilities to help secure remote connectivity. Sophos Intercept X optimizes the protection for endpoints and servers. By reducing the attack surface and preventing attacks from running, Intercept X removes opportunities for attackers to penetrate an organization.

Sophos XDR

Sophos Intercept X with XDR (extended detection and response) combines the world's best endpoint protection with the ability to detect and investigate threats across endpoints, servers, firewalls, and other data sources. See the bigger picture so you never miss a thing.

However, attackers can also break into organizations using open internet facing ports, stolen credentials, and unpatched or unprotected systems. If a cybercriminal is able to infiltrate an organization, Sophos XDR can minimize the time to detect and respond to the attack.

Sophos XDR ensures that even the earliest of indicators are made visible, easily investigated, and resolved. Powerful AI-guided detections and investigation capabilities enable organizations to hunt for threats across a cloud-based data lake with the ability to pivot to a device to see real-time state and up to 90 days of rich historical data. Native integrations with endpoint,


Managed Threat Response

ENDPOINT DETECTION AND RESPONSE TOOLS

1 Intercept X with EDR Monitors for Threats

2 Machine Learning Prioritizes Suspicious Activities

3 Confirmed Malicious Activities are Automatically Terminated

server, firewall, email, and cloud security provides a holistic view of an organization's environment. With this comprehensive and integrated approach, Sophos XDR provides the richest data set and deep analysis for threat detection, investigation and response.

Organizations need security analysts to use an XDR solution for threat-hunting. Not every company can afford to employ dedicated, skilled individuals. Alternatively, an organization may have the skills, but not the time to threat-hunt. Organizations can augment their security efforts with the Sophos Managed Threat Response (MTR) service. Expert security analysts monitor an organization's environment 24/7, and proactively hunt for threats, and if threats are found, remediate them.

Please tell us more about Sophos' Adaptive Cybersecurity Ecosystem

With cyberattacks growing in volume, sophistication, and speed, organizations cannot afford to have a security blind spot. Organizations need a security ecosystem that proactively shares threat intelligence and works together for a coordinated response. The Sophos Adaptive Cybersecurity Ecosystem (ACE) brings together the power of Sophos' threat intelligence, advanced product technologies, data lake, APIs, and Sophos Central management platform to create an ecosystem that constantly learns and improves. Sophos ACE is an open platform. From the native integration of Sophos products spanning endpoint, cloud, messaging, and network security to third party integration and open APIs, it is a system that will grow with an organization.

Can a good XDR platform stop most of the threats?

There's a classic saying in security: "Prevention is ideal, but detection is a must." Some XDR vendors focus more on detection than protection, which leads to more work, time and cost. The reality is that organizations require both prevention and detection for the best possible security outcomes. Sophos Intercept X will automatically block 99.98% of threats. Sophos XDR enables security analysts to focus their limited, valuable time on the detections where they will have the biggest impact and minimize their time to detect, investigate and respond.

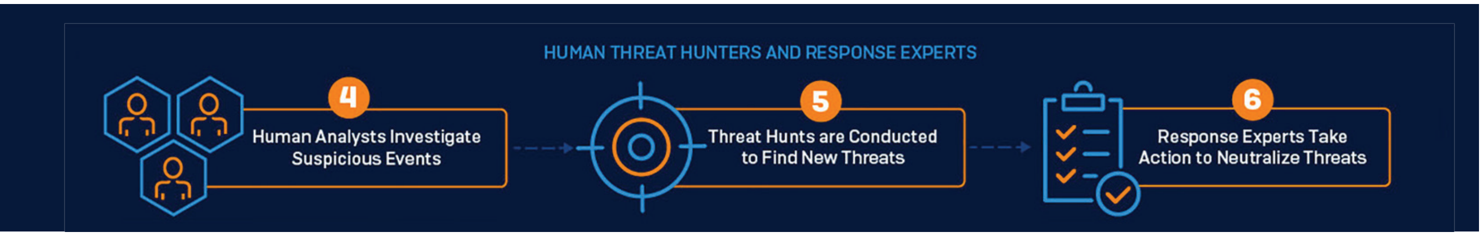
Sophos Email

Sophos Email is cloud email security delivered simply through Sophos Central's easy-to-use single management console. Protect sensitive data – and your users – from unwanted and malicious email threats with the latest artificial intelligence.

What is the biggest form of cybersecurity threat right now?

For many companies, ransomware is one of the biggest cybersecurity concerns. But ransomware attacks are changing all the time. The recently published Sophos 2022 Threat Report highlights the evolution of ransomware as attacks become more service-based and targeted and the attackers turn to additional extortion methods, such as stealing data and threatening to publish or sell it or making aggressive calls to employees, to put pressure on victims to pay.

According to Sophos researchers, over the coming year, a greater proportion of ransomware attacks will be based on ransomware-as-a-service (RaaS) offerings, with specialist ransomware developers focused on creating and then leasing their malicious code and infrastructure to third-party affiliates. Some of the most high-profile ransomware attacks of 2021 involved RaaS, such as the attack on Colonial Pipeline


HUMAN THREAT HUNTERS AND RESPONSE EXPERTS
4
Human Analysts Investigate Suspicious Events
5
Threat Hunts are Conducted to Find New Threats
6
Response Experts Take Action to Neutralize Threats

Cloud Optix

Cloud Optix delivers the continuous analysis and visibility organizations need to detect, respond to and prevent security and compliance gaps while finding ways to optimize cloud spend.

in the US. Ransomware operators can then turn to other cybercriminal services to buy access to hacked victims or use malware delivery platforms to find and target potential victims. These platforms also deliver commodity malware, adware or spam, threats that are less dangerous and disruptive.

What this means for business IT security teams, among other things, is that ransomware attacks are increasingly within range of cybercriminals regardless of their skill levels, as they can just rent or buy what they need; that any infection, for instance, with adware, can lead to every infection, including ransomware, once a target is compromised, so no suspicious signals should be overlooked; and that ransomware attackers will target people as well as technology. Defense-in-depth and human-led threat hunting are two vital protection measures against the rapidly evolving, ruthless threat of ransomware.

What best practices does Sophos recommend to combat ransomware?

In the light of the survey findings in The State of Ransomware 2021 report, Sophos experts recommend the following best practices for all organizations across all sectors:

1. Assume the organization will be hit. Ransomware remains highly prevalent. No sector, country, or organization size is immune from the risk. It's better to be prepared and not be hit than the other way round.

2. Make frequent backups. Routine backups are the number one method organizations used to get their data back after an attack. Even if organizations pay the ransom, attackers rarely return all of the data, so backups are essential either way. Aim for an approach that involves at least three different copies, using at least two different backup systems, and with at least one copy stored offline and preferably offsite.

3. Deploy layered protection. In the face of the considerable increase in extortion-based attacks, it is more important than ever to keep the adversaries out of the network in the first place. Use layered protection to block attackers at as many points as possible across an entire estate.

4. Combine human experts and anti-ransomware technology. The key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting. Technology provides scale and automation, while human experts are best able to detect the telltale tactics, techniques and procedures that indicate when a skilled attacker is attempting to break in. To bolster in-house skills, enlist the support of a specialist cybersecurity company. Security Operations Centers (SOCs) are now realistic options for organizations of all sizes.

5. Don't pay the ransom, if this is an option. Independent of any ethical considerations, paying the ransom is an ineffective way to get data back. Sophos research shows that after a ransom is paid adversaries will restore, on average, only two-thirds of the encrypted files.

Integrated Endpoint Protection for Desktops and Servers

Intercept X with intelligent Endpoint Detection and Response (EDR) for desktops, servers and mobile devices delivers the world's best protection, integrated perfectly with Sophos Firewall.

6. Have a malware recovery plan and continuously test and update it. The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Organizations that fall victim to an attack often realize they could have avoided a lot of cost, pain and disruption, if they had an incident response plan in place.

In your opinion, what percentage of budgets should be earmarked for cybersecurity?

Organizations need to view cybersecurity as their own budget line item and not as a sub department of IT. Cyberattacks impact each and every department of an organization, plus the organization as a whole in terms of company reputation.

Every organization should consider designing the best possible defense in depth strategy according to their business vertical and size of the business. Then they should decide on cybersecurity solutions, processes and best practices needed to implement the designed strategy, and the budget should commensurate with the strategy.

There has been an acceleration of digital transformation in India and in the coming years this will only expand. What challenges does this pose to cybersecurity as more data is created, stored, and utilized as well as more systems and processes within facilities become automated and move online?

Digital transformation means that you are taking analog or manual processes and digitizing and/or automating them. This naturally means that some or all of the old processes will have a new digital dimension. These new processes may require Indian organizations to adopt new technologies, which in turn demands a rethink on security to better protect against sophisticated cyberattacks.

What are the key factors to consider for organizations to make their digital transformation more secure?

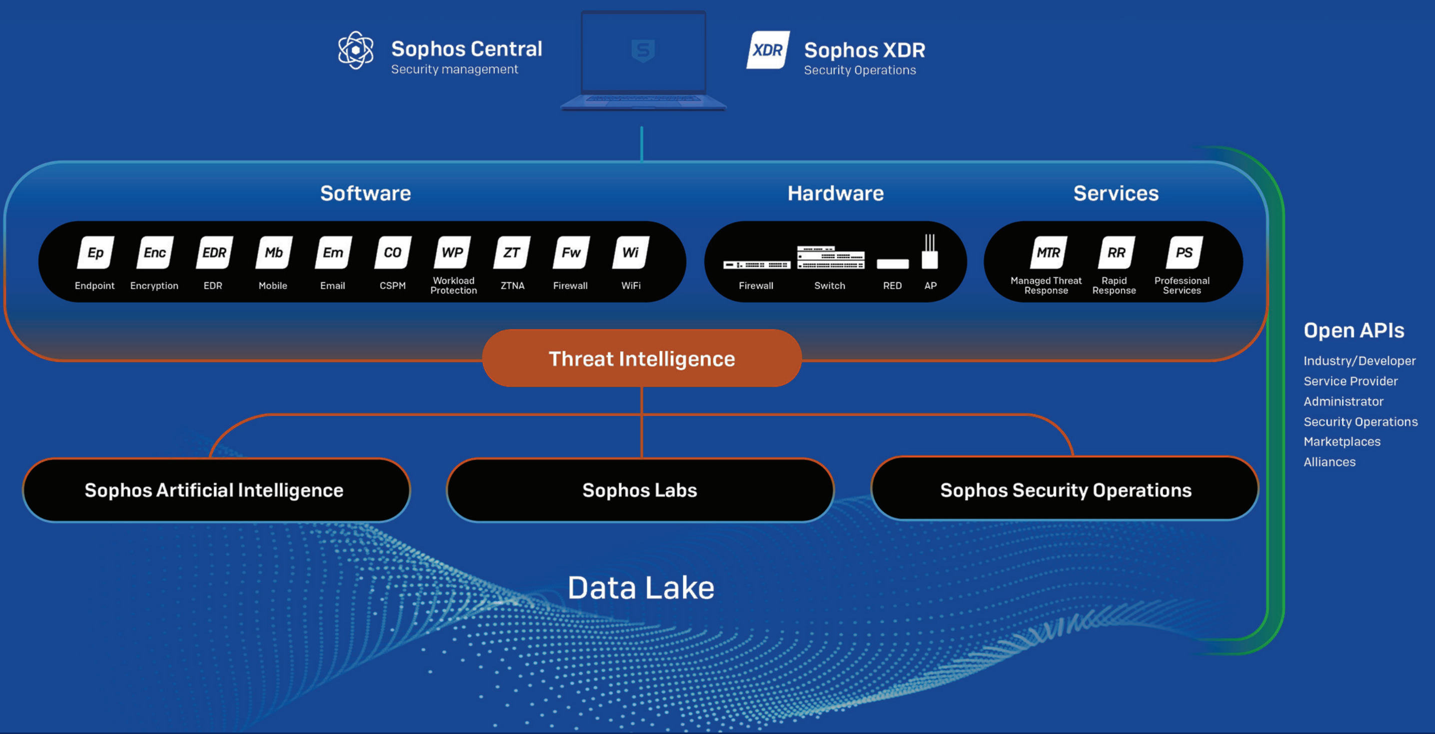
Digital transformation has brought increased speed and agility to business, but in this process, security often remains on the backburner. That is to say, when organizations are moving their infrastructure, applications, data and users into the cloud/digital environment, security also needs to go along with the new technology landscape.

Organizations thus need to evaluate the current state of security critically in their respective organizations, and work to immediately resolve the largest problems, and then incrementally improve in all areas of concern. They need to set up a cybersecurity posture including solutions, services, processes, and people aligned to their area of business and the way they interact internally and with the external world. Collectively all departments should work to improve their digital immune system by raising the bar for cybercriminals.

What can companies do to overcome privacy challenges?

The simple answer is that businesses should only collect as much data as is necessary to deliver their goods or services. The next step is to secure this data in accordance with current best practices and regional data privacy regulations.

SOPHOS



Sophos Central
Security management

Sophos XDR
Security Operations

Software

Ep Endpoint, Enc Encryption, EDR EDR, Mb Mobile, Em Email, CO CSPM, WP Workload Protection, ZT ZTNA, Fw Firewall, Wi WiFi

Hardware

Firewall, Switch, RED, AP

Services

MTR Managed Threat Response, RR Rapid Response, PS Professional Services

Threat Intelligence

Sophos Artificial Intelligence

Sophos Labs

Sophos Security Operations

Data Lake

Open APIs

Industry/Developer
Service Provider
Administrator
Security Operations
Marketplaces
Alliances

https://www.sophos.com/en-us.aspx