5 WAYS SOPHOS CAN HELP YOU TAKE A PREVENTION-FIRST APPROACH TO SECURITY

Every attack that gets through drains time, budget, and trust — disrupting lean teams and stretching even the most mature security operations. Prevention-first cybersecurity helps catch threats earlier, reduce noise, and keep teams focused on what matters.

Here are five practical ways to put prevention first using Sophos solutions — no matter your size, structure, or team.

1. Stop ransomware before it starts

Ransomware is evolving — from smash-and-grab to stealthy, remote encryption.

- **Sophos Endpoint** blocks threats before they impact your systems using deep-learning AI, anti-exploitation, and behavior-based detection.
  - Add **Sophos Endpoint Detection and Response (EDR)** for deep visibility into suspicious activity on computers and servers, or expand to **Sophos XDR** to defend against multi-stage, multi-vector attacks.

2. Shut down network threats fast

Attackers often use valid credentials to move laterally — especially in hybrid environments.

- **Sophos Firewall** with integrated **ZTNA** and **NDR** can enforce MFA access to all applications and systems to prevent attacks from credential theft. It can also detect active attackers operating on the network and automatically isolate compromised systems to prevent lateral movement.
- **Sophos Network Detection and Response (NDR)** adds additional deep traffic inspection to detect stealthy movement deep within the network.

3. Block phishing and BEC before the inbox

Phishing and business email compromise (BEC) drive over **90%** of successful cyber attacks — and now account for **37%** of ransomware entry points.

- **Sophos Email** proactively stops threats before they reach users with AI-powered detection. It seamlessly enhances Microsoft 365 and Google Workspace, while integrating with the full Sophos ecosystem.

of successful cyber attacks driven by phishing and BEC

of incidents by attackers use stolen legitimate credentials

4. Stop identity abuse in its tracks

Using stolen legitimate credentials is now the top entry point for attackers — used in **56%** of incidents.

- **Sophos Identity Threat Detection and Response (ITDR)** delivers real-time credential misuse detection, highlights identity posture weaknesses, and enables rapid response to identity threats.

5. Find and fix gaps before attackers do

65% of ransomware victims say a known or unknown gap led to the compromise.

- **Sophos Advisory Services** help you uncover and close those gaps with:
  - Internal and External Penetration Testing.
  - Wireless Network Penetration Testing.
  - Web Application Security Assessments.
- **Sophos Managed Risk** powered by **Tenable** uncovers critical vulnerabilities in hardware and software before adversaries can.

of ransomware victims say a known or unknown gap led to the compromise

Stop attacks before they spread. Catch what others miss. Close gaps before attackers exploit them — with smarter tech and experts who never stop watching.

Start your prevention-first journey at **sophos.com/prevention**.

SOPHOS