Sophos Endpoint | Ransomware Defense

PRODUCT PROMISE

Proprietary technology that provides the most complete ransomware defense

CORE FFEATURE 1
Sophos CryptoGuard

By monitoring individual files and detecting signs of manipulation and encryption, CryptoGaurd can stop even the most determined attackers as well as ransomware attacks using new or novel techniques.

Why is this important?

- Nearly 60% of organization were hit with ransomware in the last year.[1]
- The median ransomware demand is $2M. [2]
- The average recovery cost is $2.73M. [3]

How is this differentiated?

Unlike most anti-ransomware technologies, CryptoGuard does not depend on indicators of breach, threat signatures, AI, or prior knowledge to be effective. Instead, it constantly monitors files to detect signs of manipulation and encryption, automatically stops malicious processes, and rolls back any affected files to their original state.

CORE FEATURE 2
Remote Ransomware Protection

Powered by CryptoGuard, Sophos Endpoint is uniquely able to stop remote ransomware, which is when attackers use a compromised and often unprotected device to encrypt data on other devices connected to the same network.

Why is this important?

- The majority (60%+) of human-led ransomware attacks now use malicious remote encryption. [4, 5]
- Remote Ransomware has grown in popularity among attackers because most endpoint security vendors are unable to detect or stop it.

How is this differentiated?

Because this type of attack involves encrypting files remotely, traditional anti-ransomware technologies don't "see" the malicious files or attacker activity, so they cannot provide protection. CryptoGuard, however, monitors for malicious encryption and provides real-time protection and rollback capabilities, even when the ransomware itself never appears on a protected device.

CORE FEATURE 3
Exploit Prevention

Sophos Endpoint includes more than 60 anti-exploitation capabilities that block the behaviors attackers use to exploit vulnerabilities, stopping both known vulnerabilities and zero-day threats ("zero-day" threats are those that take advantage of previously unknown security flaws).

Why is this important?

- Exploited vulnerabilities are the most common starting point in successful ransomware attacks. [6]
- Organizations whose attacks began with exploitation of a vulnerability have 4x higher attack recovery costs. [7]

How is this differentiated?

Most leading endpoint solutions have fewer anti-exploit mitigations and these mitigations are often disabled by default, requiring manual tuning. Sophos Endpoint includes over 60 proprietary and pre-configured exploit mitigations, with no training or tuning required. Sophos Endpoint's "Device Exposure" feature provides further insight into Windows and macOS devices with missing OS patches.

Sources

1. **Sophos, “The State of Ransomware 2024”**
   https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf
2. **Sophos, “The State of Ransomware 2024”**
   https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf
3. **Sophos, “The State of Ransomware 2024”**
   https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf
4. **Microsoft, “Microsoft Digital Defense Report”**
   https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
5. **Sophos, “CryptoGuard: An asymmetric approach to the ransomware battle”**
   https://news.sophos.com/en-us/2023/12/20/cryptoguard-an-asymmetric-approach-to-the-ransomware-battle/
   - **Sophos News, “Sophos Endpoint: Industry-leading protection against remote ransomware attacks”**
     https://news.sophos.com/en-us/2023/12/07/sophos-endpoint-industry-leading-protection-against-remote-ransomware-attacks/
6. **Sophos, “The State of Ransomware 2024”**
   https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf
   - **Sophos News, “Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector”**
     https://news.sophos.com/en-us/2024/04/03/unpatched-vulnerabilities-the-most-brutal-ransomware-attack-vector/
7. **Sophos, “The State of Ransomware 2024”**
   https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf