Solution Brochure

SOPHOS

Sophos Emergency Incident Response

Comprehensive full-service assistance — from investigation to recovery

Immediate response to active threats

Every second counts when your business is under attack. When an incident occurs, you need speed, efficiency, and cross-discipline security skills and expertise. You also need visibility into and knowledge of the ever-evolving global threat landscape and the latest threat actor tactics and techniques.

Sophos Emergency Incident Response is there for you when a cyber emergency strikes, working quickly to assess, contain, understand, and remediate. Our team of cross-functional experts apply their years of experience and learnings to rapidly triage, contain, and neutralize active threats, and eject adversaries to prevent additional damage. Sophos leverages what we've learned through performing thousands of engagements to guide recommended improvements and preventative actions that don't just address the root cause of the incident, but help elevate your resiliency against future strikes.

Proactively strengthen defenses and security posture

Sophos Emergency Incident Response employs a collaborative and interactive approach, working with your team to quickly assess the situation, contain and eliminate the threat as needed, and deliver actionable guidance for recovery. Our team provides digital forensics, malware analysis, threat hunting and threat intelligence from the Sophos X-Ops and Counter Threat Unit research teams to find and eliminate threats. We use cross-disciplinary subject matter experts (such as penetration testers and threat researchers) to ensure comprehensive risk mitigation and recovery.

Detect and investigate

Initial contact and investigation

To ensure the fastest response possible, Sophos is laser-focused on immediate distribution of agents to discoverable assets. This remote incident response assistance enables the capture of forensics data to support initial analysis, develop appropriate containment actions, and determine the need for additional technology to quickly expand visibility throughout your engagement.

Deepen investigation

Data Capture: Assets, services affected, business impact, other attack vectors.

Iterative Forensics & Threat Analysis: Researchers, hunters, penetration testers and analysts help gain a full understanding of the threat.

Remediation Planning: Start planning for remediation, in parallel and in concert with the investigation.

Customer benefits

- Extend your team with cross-functional digital forensics and incident response capabilities and expertise.
- Reduce the impact of an incident and the risk of recurrence with a complete understanding of the threat.
- Expand visibility, obtain facts and determine answers fast to determine the right actions.

Attack Surface Reduction: Sophos can provide interactive threat actor insight to validate controls and identify additional reentry points for comprehensive risk mitigation.

Ransom Negotiation: Experienced ransomware negotiators leverage deep knowledge of ransomware threat actors to ease negotiation and offer guidance to recover data safely and in a cost-effective manner from ransomware actors.

Remediate

Secure and validate

Focused Security Hardening: The IR team guides and supports tactical security control hardening efforts that will prevent reentry by the threat actor.

Containment: Cutting off the threat actor's command-and-control.

Threat Actor Eviction: Evicting the adversary from a contained network requires the orchestrated elimination of their tradecraft and resetting of compromised domains.

Recover

System and Data Recovery: To help rebuild systems, sanitize data and put systems back into production, the Sophos IR team works with trusted partners to provide recovery services seamlessly and securely.

Host Validation: Using our industry-leading agent technology, we help ensure that restored hosts are ready for production.

Follow-up

Improve

Sophos leverages lessons learned through the thousands of engagements we have performed to guide recommended response process improvements as well as strategic recommendations to help drive a security transformation roadmap. At the end of the engagement, we can provide you with a formal incident report of our investigation, detailing the actions taken, the discoveries we made, and long-term recommendations on how to mitigate the recurrence of similar threats in the future.

Why Sophos for incident response?

Sophos brings extensive experience to every cybersecurity emergency engagement. We deliver full-service incident response assistance to a wide range of organizations, across verticals and incident types — from small, single compromised system concerns to enterprise-wide crisis situations that significantly disrupt or impede business operations.

Our seasoned incident response team leverages expertise and backgrounds spanning national, military, organizational Computer Security Incident Response Teams (CSIRTs), law enforcement and intelligence agencies. They combine hands-on understanding of key cybersecurity practices with front-line incident response, threat intelligence from our X-Ops and Counter Threat Unit research teams, findings from security testing and assessment engagements, and security analytics to accelerate investigations and recover with confidence.

Service features

- Rapid identification and neutralization of active threats.
- Quick deployment of technologies.
- Capture and analysis of digital forensics data to identify indicators of compromise and track adversary activity.
- Threat hunting to identify related threat actor activity.
- Remote and onsite technical, incident command and advisory capability.
- Seasoned and accredited global incident response team experienced in common and uncommon cyber threat scenarios.
- Incident-specific threat intelligence and insights into current adversary tradecraft.
- Expert ransom negotiation.
- Post-incident report detailing actions taken, discoveries, and recommendations.

Experiencing an active breach?

Call your regional number below at any time to speak with one of our Incident Advisors.

Australia: +61 272084454

Austria: +43 73265575520

Canada: +1 7785897255

France: +33 186539880

Germany: +49 61171186766

Italy: +39 02 94752 897

Switzerland: +41 445152286

United Kingdom: +44 1235635329

USA: +1 4087461064

If all the Incident Advisors are busy, please leave a message and someone will get back to you as quickly as possible.

Email: EmergencyIR@sophos.com

To learn more, visit
sophos.com/emergency-response

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2025-06-04 BREN (MP)

SOPHOS