Sophos Compromise Assessment

Uncover evidence of a breach before it can impact your business

Last year, enterprises spent a median of 37 days and a mean of $2.4 million to find and recover from security breaches. Delivered by an expert team of incident response specialists, the Sophos Compromise Assessment, is the fastest, most effective means of identifying ongoing or past attacker activity in your environment, enabling your organization to take swift, decisive action.

Identify Active or Recent Attacker Activity

Delivered by an expert team of threat hunters and incident response experts, the Sophos Compromise Assessment rapidly identifies if an attacker has breached your defenses, quantifies the level of risk to your organization, and provides detailed guidance on what actions need to be taken to eliminate the threat.

Extensive experience responding to today's most advanced threats enables the Sophos Incident Response (IR) Services team to identify indicators of compromise (IoCs) through a targeted investigation of potentially compromised assets. The result is a fast, thorough assessment that helps your organization manage risk and compliance while maintaining operational efficiency.

Sophos Compromise Assessment Methodology

The Sophos IR Services team maintains direct communication with your organization through each phase of the Compromise Assessment, providing clarity on the threat, risk exposure, and actions to be taken to resolve the incident and address the root cause.

1. **Initial Coordination Cal**l – the assessment begins with the efficient exchange of information about the potential threat, identification of key points of contact, and confirmation of the deployment scope and investigation process to be followed.
2. **Deployment of Investigation Tools** – guided installation of the award-winning, clouddelivered Sophos platform ensures data on designated devices is captured immediately, enabling the Sophos IR Services team to conduct a thorough assessment of device health.
3. **Threat Investigation and Risk Assessment** – if an active threat is confirmed, the Sophos IR Services team will conduct an immediate Active Threat Call with your key points of contact to discuss the risk of a widespread security incident and urgent actions to be taken.
4. **Summary Call and Written Report** –receive technical documentation and a non-technical executive summary detailing evidence of attacker activity, risk exposure, and guidance on eliminating the threat and addressing the root cause.

All four phases of the Sophos Compromise Assessment are typically completed within 7 days of the Initial Coordination Call.

Highlights

- Rapidly identify if an attacker is operating undetected in your environment
- Quantify the potential risk of a widespread security incident
- Communicate directly with an expert team of threat hunters and incident response specialists throughout each stage of the investigation
- Receive a comprehensive analysis of attacker activity, risk exposure, and guidance on eliminating the threat and addressing the root cause
- Support risk management and compliance initiatives, as well as due diligence efforts associated with mergers and acquisitions activity

Fast, Thorough Investigation

The Sophos Compromise Assessment investigates and identifies a complete spectrum of attacker activities, including:

- Suspicious network activity
- Lateral movement
- Anomalous or malicious files
- Automated malware execution
- Unauthorized access
- Privilege escalation
- Defense evasion
- Credential theft
- Data exfiltration
- Unverified scripts

After the Assessment

If the Sophos IR Services team confirms that an attacker has breached your defenses, compromising your data and business, there is an option for priority onboarding to Sophos Rapid Response. This full-scale incident response service will triage, contain, and neutralize the active threat across your entire IT environment. An expert team of 24/7, remote incident responders will quickly act to eject the adversary from your environment and recommend real-time preventative actions to address the root cause.

If no signs of a breach are found, Sophos Managed Detection and Response (MDR) can arm your organization with ongoing 24/7 detection and response services. Our round-the-clock team of threat hunters and response experts proactively hunt for and validate potential threats and incidents. The team continually takes actions to disrupt, contain, and neutralize evolving threats, and provides actionable advice to address the root cause of incidents and improve your security hygiene.

Experiencing an Active Breach?

Sophos Rapid Response gets you out of the danger zone fast with our 24/7 team of remote incident responders, threat analysts, and threat hunters. Onboarding starts within hours, and the majority of customers are triaged in 48 hours. If you are in the middle of an active threat, call your regional number below at any time to speak with one of our Incident Advisors.

If you are in the middle of an active threat, email the Rapid Response team at rapidresponse@sophos.com or call your regional number below:

Australia: +61 272084454

Austria: +43 73265575520

Canada: +1 7785897255

France: +33 186539880

Germany: +49 61171186766

Italy: +39 02 947 52897

Netherlands: +31 162708600

Spain: +34 913758065

Sweden: +46 858400610

Switzerland: +41 445152286

United Kingdom: +44 1235635329

USA: +1 4087461064

Experiencing an Active Breach?

Get lightning-fast support from
Sophos Rapid 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

SOPHOS