

Sophos Appliance Integrity Monitoring

Detect signs of compromise. Understand what happened. Maintain trust in your appliance.

Linux-based appliances sit at the center of modern infrastructure. They control traffic, protect data, manage operations, and often operate with the level of trust attackers are looking for. When attackers gain access to an appliance, the impact extends beyond the device itself.

The challenge is that compromise rarely looks like compromise. Attackers who gain access to an appliance often use legitimate tools and expected processes to blend into normal operations. Individual file changes and log entries may appear routine even when they are part of a larger attack. File monitoring can tell you something changed. Logs can show that something happened. Neither tells you what it means.

Sophos Appliance Integrity Monitoring (AIM) was built to answer that question.

AIM is a dedicated solution that ensures the integrity of Linux-based appliances. It pairs lightweight kernel-level visibility with an appliance-focused detection model shaped by real-world attacks.

While generic tools surface events, AIM evaluates the surrounding activity to help determine whether those events reflect normal operation or signs of compromise. Guided customization from a Sophos Appliance Integrity Expert helps align the model to the way the appliance is expected to behave.

From defense to product: Built through real-world attacks

AIM emerged from a multi-year campaign to defend Sophos Firewall against coordinated, nation-state-level threat groups in what became one of the most documented appliance security investigations on record: Pacific Rim.

That experience required more than telemetry: Sophos had to distinguish legitimate appliance behavior from attacker activity deliberately designed to blend in.

What came out of that experience was a monitoring model that goes beyond surfacing events — one that understands what matters on an appliance, and why.

Why AIM is different

Context-rich visibility

AIM helps determine whether events warrant investigation by collecting the surrounding context and related activities.

Attack-informed detection rules

Built from real appliance attacks and years of appliance-security research, it identifies behaviors that matter in production compromises.

Built for resource-sensitive environments

Lightweight by design, with monitoring and context collection aligned to the appliance's requirements, helping balance detection value and operational impact.

Appliance-specific baseline

Aligned to how the system operates, AIM aids teams distinguish between expected behaviors and signals that may indicate compromise.

Refined through ongoing research

Ongoing Sophos investigations and appliance-security research help keep protections aligned with new attack techniques and evolving attacker behavior.

Guided by Appliance Integrity Experts

Sophos Appliance Integrity Experts help refine monitoring logic and detections around the product's architecture, workflows, and unique attack surface.

How AIM works

AIM combines Sophos's appliance-security experience with the vendor's knowledge of how the product should behave to create a product-specific monitoring model for detecting and investigating signs of compromise.

- 1 Establish an appliance-specific baseline**

The vendor contributes product knowledge. Sophos contributes detection content, sensor telemetry, and experience gained defending appliances under real attack. Guided customization helps optimize the detection model, refine existing rules, and develop appliance-specific detections based on how the product is expected to behave. This establishes the baseline that guides how activity is evaluated throughout the solution.
- 2 Capture meaningful behavior**

The Sophos Linux Sensor provides kernel-level visibility into activity occurring on the appliance, including behaviors that may not generate a meaningful file alert or obvious log entry. Visibility alone does not explain whether activity is expected, suspicious, or part of a larger sequence of events, but it provides the evidence needed for thorough investigation.
- 3 Surface anomalous activity**

AIM evaluates observed activity against detection content built around appliance compromise patterns. The appliance-specific baseline helps focus detections on behaviors that differ from expected operation, improving signal quality and reducing unnecessary investigation. Examples include unexpected use of legitimate utilities, persistence outside approved workflows, activity designed to conceal system behavior, and shell or network activity inconsistent with the appliance's intended role.
- 4 Investigate with full context**

When AIM identifies suspicious activity, it surfaces the context needed to understand what happened: the initiating process, related activity, affected files or system areas, timing, and whether the behavior aligned with an approved workflow. Rather than investigating isolated events, teams can evaluate activity as part of a broader sequence of behavior.

Where AIM delivers the greatest value

Protect trust in security-critical products

Security appliances, network infrastructure, storage platforms, and other systems often operate with elevated privileges and broad access. Their role within customer environments often makes them high-value targets for attackers.

Reduce brand and customer risk across large deployments

A compromise affecting a widely deployed appliance can quickly become a customer trust, support, and brand issue. Early visibility helps vendors identify and investigate suspicious behavior before incidents escalate.

Support integrity requirements in regulated environments

Healthcare, government, telecommunications, financial services, and industrial environments increasingly expect vendors to demonstrate how appliance integrity is monitored, investigated, and maintained over time.

Maintain confidence in long-lived deployed systems

Many appliances spend months or years in customer environments with limited visibility into system behaviors. Maintaining confidence in how the appliance operates becomes as critical as preventing compromise.

Explore whether AIM fits your appliance

Contact the Sophos OEM team at OEM@Sophos.com