Better together: ScienceLogic with CrowdStrike

ScienceLogic is committed to employing security best practices to deliver solutions that you can trust. As another layer of security and compliance, we have partnered with CrowdStrike to complete validation and testing of CrowdStrike sensors on ScienceLogic appliances and Restorepoint agents.

Enhance IT monitoring and operations protection

Cyber-attacks are rising in frequency, sophistication, and extent of damage they can inflict upon your operations, reputation, or worse, your customers. As a result, most organizations have a cybersecurity program that includes an endpoint security management policy to ensure all the endpoint devices in their network maintain certain levels of security and safety. This requirement extends to your IT operations environment as well: The ScienceLogic and Restorepoint agents and appliances that you use for monitoring and change management are seen as endpoints in your IT environment.

Secure SL1 and Restorepoint endpoints with CrowdStrike Falcon®

ScienceLogic has partnered with CrowdStrike to offer additional security on SL1 with the CrowdStrike Falcon Prevent and Insights services. Assisted by CrowdStrike Endpoint Detection and Response (EDR) technology, ScienceLogic continues to maintain security vigilance and regularly evaluate vulnerabilities to ensure a robust security posture.

The CrowdStrike Falcon platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry to automatically detect attacker activity and grants your security team real-time visibility across the environment. Visibility into the ScienceLogic on-premises architecture allows your team to identify and track the source of malicious activity reported on your edge-deployed SL1 platform instances and related components, in addition to human-initiated activity, to proactively identify, investigate, and remediate threats.

With the use of CrowdStrike Falcon Endpoint Detection and Response capabilities with ScienceLogic and Restorepoint on-premises endpoints, you can:

- Increase endpoint visibility across your IT estate
- Secure on-premises ScienceLogic SL1 and Restorepoint endpoints
- Satisfy compliance guidelines
- Uncover and respond immediately to security threats

Because the Falcon platform treats normal IT operations functions like other software processes running on the endpoints, your security team gains an additional layer of protection and enhanced remediation actions. CrowdStrike's accurate and swift remediation actions, enabled from within its single console, allow your team to quarantine compromised collectors without impacting broader ScienceLogic operations, ensuring business continuity in the event of an incident.

With the CrowdStrike Falcon platform and the ScienceLogic SL1 platform, you can ensure your organization is equipped with fortified protection and enhanced visibility for your dispersed AIOps environment to thwart attackers before damage is done.

Supported versions and components

ScienceLogic successfully completed testing of CrowdStrike Falcon Insight Endpoint Detection and Response (EDR) and Falcon Prevent Next-Generation Antivirus (NGAV) for the following ScienceLogic product versions and components:

- **SL1 Eiffel (11.2):** All on-premises SL1 appliances, including collectors, agents, PowerFlow, co-resident, and high availability/disaster recovery locations

- **SL1 Duomo (11.1.1.2):** SL1 on-premises collectors

- **Restorepoint 5.4:** Agents

Learn how you can take advantage of this new capability by contacting your ScienceLogic or CrowdStrike representative.

Commitment to security

With validation of CrowdStrike Falcon support for SL1 and Restorepoint endpoints, ScienceLogic adds another proof point to our commitment to our customers' security requirements.

To learn more about managing your hybrid cloud estate while establishing a secure foundation to automate and modernize your IT operations, please visit our ScienceLogic Trust Center.

About ScienceLogic

ScienceLogic enables companies to digitally transform themselves by removing the difficulty of managing complex, distributed IT services. Our IT infrastructure monitoring and AIOps platform (SL1) provides modern IT operations with actionable insights to predict and resolve problems faster in a digital, ephemeral world. The SL1 platform sees everything across cloud and distributed architectures, contextualizes data through relationship mapping, and acts on this insight through integration and automation. SL1 solves the challenges and complexities of today and provides the flexibility to face the IT monitoring and management needs of tomorrow. Trusted by thousands of organizations, ScienceLogic's technology was designed for the rigorous security requirements of United States Department of Defense, proven for scale by the world's largest service providers, and optimized for the needs of large enterprises.