**Arctic Wolf’s Response to the FireEye Cyberattack**

The threat detection and response capabilities of the Arctic Wolf® Platform and the security operations expertise of our Concierge Security® Team have prepared Arctic Wolf to deal with targeted and advanced threats.

All of the vulnerabilities named in the FireEye toolkit were previously disclosed by the various impacted vendors, and Arctic Wolf had already updated our Managed Detection and Response and Managed Risk detections accordingly. Our Concierge Security Team proactively notified all customers with the known vulnerabilities still in their environments.

Using the indicators of compromise (IOCs) shared by FireEye, Arctic Wolf has updated our detections, which apply to the Arctic Wolf Sensor, the Arctic Wolf® Agent, and various EDR/EPP integrations. We will continue to add more detections should FireEye disclose additional details.

These updated detections come in addition to the steps we take daily to ensure the systems of Arctic Wolf, our partners, and our customers are never compromised, which include:

* Continuous 24x7 monitoring of Arctic Wolf's entire infrastructure, including partner and customer data, by the full suite of Arctic Wolf security operations solutions and the Arctic Wolf Concierge Security Team
* The implementation of strict data access policies and multi-factor authentication tools for all Arctic Wolf systems
* Regular external audits and risk assessments conducted by both third parties and the Arctic Wolf Concierge Security Team

Want to know more? We invite you to learn about how Arctic Wolf obsesses over data protection by reading the complete [**Arctic Wolf Information Security Policy**](https://arcticwolf.com/informationsecurity/) on our website.