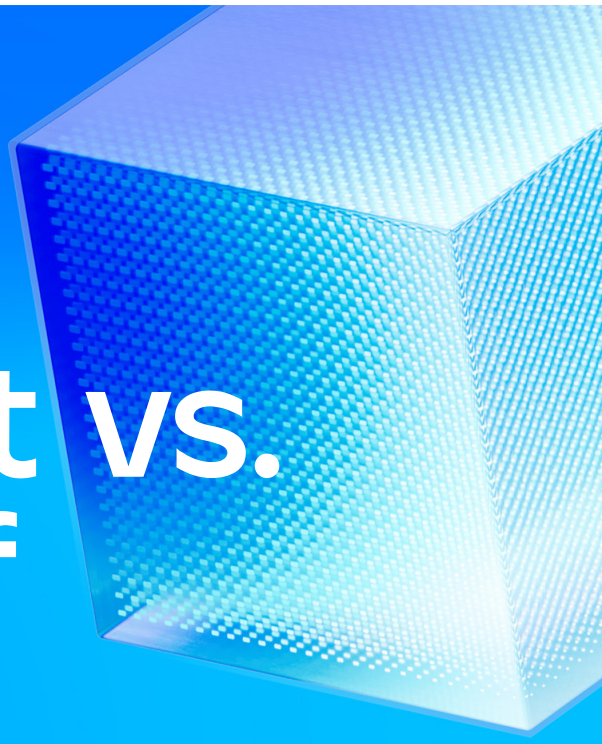
FIELD EFFECT

Field Effect vs. Arctic Wolf



Simple, powerful, and proactive cybersecurity—no add-ons required.

Arctic Wolf offers complex, siloed solutions that require trained cybersecurity professionals to manage. Originating as a SOC-as-a-service, Arctic Wolf uses a SIEM-based model that aggregates logs and telemetry data from a combination of third-party and acquired tools, creating noisy environments, management demands, and a higher total cost of ownership.

Why organizations choose Field Effect:

Single Pane of Glass

Streamline all the tools and services needed to deliver comprehensive cybersecurity in one, natively-built solution.

Crystal-Clear Alerts

Users of all technical backgrounds can act with confidence.

Noise Free

Receive only the information that matters and avoid alert fatigue.

Exceptional Value

Enterprise-grade cybersecurity accessible for organizations of any size.

Feature	Field Effect	Arctic Wolf
COVERAGE		
Packages	**Purpose-Built** Field Effect MDR Complete and MDR Core are purpose-built and right-priced to meet a range of cybersecurity needs—from lower-complexity clients to those with robust compliance and cyber insurance requirements. The flexible packages simplify security by consolidating essential tools and services into one solution, ensuring comprehensive protection for your clients' critical assets.	**Modular** Arctic Wolf offers complex, siloed services with frequent upsells, often leading to SKU confusion and difficulty achieving ROI.
Threat Detection	**Precision Detection** Field Effect stops both known and unknown threats early in the attack lifecycle to prevent disruption. Known threats and malicious behaviors are blocked in real time at the endpoint, while telemetry and logs are aggregated across the environment for contextual analysis and high-fidelity alerts. Proven results: Ranked #2 in Mean Time to Detect (MTTD) in the MITRE Engenuity ATT&CK® Evaluations: Managed Services – Round 2.	**Reactive** Arctic Wolf uses a SIEM-based approach, aggregating logs and telemetry from third-party tools and/or Aurora Endpoint Security. As a result, analysis and response mostly happens in the cloud–not the endpoint–leading to delays that could potentially lead to disruption. Arctic Wolf has not been publicly tested in a third-party security evaluation.

Feature	Field Effect	Arctic Wolf
COVERAGE		
Visibility	**Transparent** Field Effect's AROs (Actions, Recommendations, and Observations) surface only the most critical threat information—with a clear, actionable, and noise- free approach. Users who want deeper context can access the underlying alerts, offering transparency into the behaviors that triggered their precision detections.	**Black-Box Approach** Arctic Wolf lacks transparency into how alerts are generated, preventing users from accessing granular visibility when they need it.
Integration	**Natively Built** Field Effect was natively built to provide unified protection across endpoints, networks, and cloud services—analyzing and correlating data from your entire environment to deliver richer insights, reduced noise, and automated protection.	**Minimally Integrated** Arctic Wolf is minimally integrated into third-party tools and/or acquired technology, resulting in high alert volumes and increased labor costs.
24/7 SOC		
24/7 Monitoring and Threat Hunting	**Expert-Led** Field Effect's expert-led SOC monitors security alerts across your environment, investigating suspicious signs of attack that might otherwise go unnoticed, and delivering only the alerts that matter.	**Hindered** Arctic Wolf's cyber concierge monitors client environments 24/7, investigating and alerting on suspicious behavior. However, their effectiveness is hindered by the limited context provided by minimally integrated technology, making it difficult to eliminate alert noise.

Feature	Field Effect	Arctic Wolf
24/7 SOC		
Threat Disruption and Containment	**Rapid, Flexible & Fully Managed** Field Effect MDR stops threats early in the kill chain, blocking malware and ransomware, while neutralizing active attacks before they spread. Flexible response policies let you tailor actions by organization or user, balancing risk tolerance with business continuity. Whether automated or analyst-verified, Field Effect enables faster, smarter threat response aligned to your needs	**Manual & Incomplete** Arctic Wolf performs manual isolation through their Aurora Endpoint Security or third-party tools, with an all-or-nothing approach, forcing organizations to choose between risk management and business continuity. Arctic Wolf cannot isolate Microsoft 365 accounts or Google Workspace Accounts.
Remediation guidance	**Actionable** Jargon-free remediation instructions are shared as part of Field Effect's AROs to streamline resolution. Users can also access 24/7 support for further assistance.	**Complex** Complex instructions require support to effectively guide users through remediation.
USER FRIENDLINESS		
Alert volume	**Noise-Free** Sophisticated triaging and alert tuning ensure precise alerts with minimal noise.	**Noisy** Arctic Wolf generates a high volume of alerts, even after review from their Triage Security Team. This forces organizations to spend time triaging non-critical issues, increasing operational overhead and delaying response to real threats.

Feature	Field Effect	Arctic Wolf
USER FRIENDLINESS		
Usability	**Designed for SMEs & MSPs** Field Effect's AROs are clear and accessible to users of all technical backgrounds.	**Designed for Security Experts** Complex alerts require cybersecurity expertise to manage, triage, and action.
Onboarding	**Simple** Field Effect offers a plug-and-play appliance, simple click-to-enable cloud monitoring, and industry standard endpoint installers compatible with Mac, Linux, and Windows devices for rapid onboarding.	**Complex** Paid onboarding is time intensive and complex, while deployment requires heavy concierge involvement, often taking up to a month to install.
AVAILABLE FEATURES		
Vulnerability Management	**Included** Field Effect helps you understand and manage endpoints, cloud, and networks vulnerabilities that attackers can easily exploit. This includes out-of-date operating systems, misconfigurations, and required patches, as well as external threats like typo-squatting domains and exposed services.	**Available for Upsell** Arctic Wolf's Managed Risk offering/feature is available for a costly upgrade, making organizations choose between going over budget or leaving significant risk unmanaged.
Dark Web Monitoring	**Included** Field Effect identifies credentials, financial information, and personally identifiable information leaked on the dark web.	**Not Available**

Feature	Field Effect	Arctic Wolf
AVAILABLE FEATURES		
Email Analysis	**Included** Field Effect's Suspicious Email Analysis Service (SEAS) allows employees to flag suspicious emails with a single click for near-real-time expert review.	**Not Available**
DNS Firewall	**Included** Field Effect provides a DNS firewall to ensure safe web browsing by blocking access to known malicious sites and allowing for content filtering capabilities.	**Not Available**
Log Retention	**Flexible Storage Options** Field Effect MDR Complete includes a complimentary 90 days of Field Effect MDR log retention. Flexible and cost-effective storage options can retain log data for up to seven years to meet compliance frameworks and cyber insurance requirements.	**Available for Add-on** Log retention is available through a costly upgrade, making it expensive to comply with regulatory requirements.

Feature	Field Effect	Arctic Wolf
PRICING		
Pricing Structure	**Straightforward and Cost-effective** Field Effect MDR Complete and MDR Core are purchased on a per-user basis.	**Mixed and Expensive** Arctic Wolf offers a mixed pricing model, with multiple, expensive SKUs charging per endpoint, per server or per user account, for a comprehensive offering..
Value	**High Value** Field Effect MDR brings together essential security tools and services into a single, comprehensive solution—maximizing efficiency while delivering industry-leading protection and value with per-user pricing.	**Diminished Value** Complex, siloed solutions paired with high management fees increase total cost of ownership, making cybersecurity only affordable to mid to large enterprises.

Note: All information is deemed to be as accurate as possible, given available market information. Details may change regularly, and therefore may not be up-to-date based on latest product updates.

Profound simplicity, powerful cybersecurity.

FIELD EFFECT / MDR

About Field Effect

Every business deserves powerful protection from cyber threats.

Field Effect's cybersecurity solutions were purpose-built to prevent, detect and respond to threats for clients of all sizes. We take on the complexity behind the scenes and deliver a solution that's sophisticated where it matters, and simple everywhere else. Consolidate your tech and eliminate the noise while empowering users of all technical backgrounds to confidently navigate cybersecurity and avoid disruptions.

Complexity out, clarity in.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
+1 (800) 299-8986