ARCTIC WOLF

ENDPOINT SECURITY BUYER'S GUIDE:

From Feature Checklists to Security Operations

01
Executive Summary

Endpoint security is foundational, but most buyers think they already know what an EDR does. That assumption can make the buying decision feel smaller than it is. Organizations know the standard checklist: prevention, detection, response, coverage, and performance. Those criteria still matter, yet, these criteria aren't addressing the entirety of the problem considering the rate of breaches continue to grow.

The threat landscape has changed. Cyber risk has accelerated from human-speed attacks to machine-scale exploitation. Attackers' breakout time is dropping dramatically and with the emergence of frontier AI models from organizations like Open AI, Anthropic, and Google, attackers may soon be able to discover and exploit weaknesses faster than organizations can patch them. Identity compromise, SaaS breaches, supply chain attacks and ransomware have already proven that one gap can quickly become a business-wide crisis. While the threat landscape has accelerated, so too has modern cybersecurity architecture. Getting the right endpoint security in this modern era of AI-powered threats and agentic security platforms is more important than it may initially appear.

Most credible endpoint vendors can check the traditional boxes. **What matters is how endpoint security is integrated into a broader cyber security platform and how it fits into your security operations model:** how it adds context, supports response across the attack chain, preserves flexibility, stays ahead of novel threats, and helps organizations operationalize security through platform-centric, agentic workflows.

Now is the time to ensure your endpoint security is integrated into a broader security operations approach, because the pressure is real and mounting:

44%

of Aurora® Incident Response cases involved ransomware.

33%

Endpoint volume continues to grow with IoT devices, and 33% of assets are missing at least one critical security control.

75%

Cybersecurity budget growth has slowed by 75% since 2022, according to World Economic Forum.

$20 billion

The FBI IC3 reported more than 1 million complaints of suspected internet crime in 2025 and reported losses exceeding $20 billion (USD).

Endpoint telemetry is too important to treat as a siloed tool output. Endpoint data is reviewed in nearly 95% of Arctic Wolf SOC investigations, and attackers are continuing to bombard the endpoint as an entry point. Last year, we prevented hundreds of attacks per customer while maintaining a 99% true-positive rate, but attack volumes are likely only going to increase. Nevertheless, even though the traditional criteria are still fundamental, the buying conversation must expand beyond the baseline.

This guide moves from traditional endpoint feature evaluation to security operations impact analysis. Standard endpoint criteria remain baseline gates. The real decision is what determines long-term security outcomes.

This is more than a traditional buyer's guide. It provides a framework for how endpoint security should be evaluated in the AI era.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

02

Why Endpoint Buying Criteria Need to Evolve

Endpoint security remains one of the most important controls in the security stack, but organizations are no longer choosing only a point product. They are making a security operations decision.

The traditional criteria for an endpoint solution was: Can it provide malware prevention, detection of suspicious behavior, containment of threats, and support for EDR workflows across the estate, in imperfect conditions, and with minimal resource constraints? Those are still necessary questions today, but they no longer account for the full evaluation.

The real-world challenge is often not whether the tool has the most cutting-edge features. It is whether the organization can use those features correctly and operationalize them. A tool that is not fully deployed, tuned, configured, and monitored according to traditional check-box, market-driven criteria creates a false sense of security.

That matters because attackers do not respect product boundaries. Ransomware, credential theft, malicious scripts, living-off-the-land activity, unsafe networks, risky applications, and phishing all intersect with endpoints in different ways. The Cybersecurity and Infrastructure Security Agency (CISA) continues to publish alerts and add actively exploited vulnerabilities to its catalog faster than ever before (with year-over-year growth hitting 20% in 2025), reinforcing the need for fast, threat-informed prioritization and stronger endpoint controls.

At the same time, standard prevention, detection, and response capabilities are not enough. The NIST Cybersecurity Framework 2.0 defines cybersecurity across Govern, Identify, Protect, Detect, Respond, and Recover. Endpoint security should permeate throughout that lifecycle, not operate as a disconnected tool that only blocks actions or alerts at arbitrary steps.

Modern endpoint evaluation must move beyond "does the tool work?" to "can this solution help my analysts and security program work better?" Baseline capabilities get a vendor on the shortlist. Operational outcomes should determine the decision.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

03

The Standard Endpoint Checklist Is Necessary, but Not Sufficient

The standard endpoint checklist still matters. Organizations should not treat prevention, detection, response, coverage, and performance as optional. These are the baseline gates every serious endpoint solution must clear.

A modern endpoint security solution checklist typically encompasses:

- *AI- or machine learning-based prevention*
- *Behavioral detection*
- *Endpoint detection and response*
- *Threat hunting support*
- *MITRE ATT&CK mapping*
- *Response actions*
- *Device control*
- *Application control*
- *Script and memory protection*
- *Support for a wide-range of operating systems*
- *Mobile device coverage where needed*
- *Low endpoint-performance impact*
- *Clear management and reporting*

Aurora Endpoint Security is designed to maximize the value customers get from endpoint security while helping them achieve broader security outcomes:

- **Aurora Protect** delivers lightweight, AI-powered prevention.
- **Aurora Endpoint Defense** adds EDR capabilities for investigation and response.
- **Aurora Managed Endpoint Defense** delivers these capabilities via the Aurora Agentic SOC to reduce noise and operational burden.
- **Aurora Mobile Threat Defens**e extends protection to iOS and Android.

Our portfolio is designed to deliver the core capabilities organizations need, but more importantly, it gives them a scalable path to reduce cyber risk, improve price-to-performance ratio, to maximize security budget, and integrate with a broader security operations approach.

Protection is table stakes. Operationalization is where outcomes are won or lost.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

04 The New Endpoint Security Buying Criteria

Open architecture and future flexibility	Security platform and agentic workflows	Tuning and configuration aligned to operational reality
Endpoint telemetry in context	Cross-domain response	Defense in depth includes business resilience

Open architecture and future flexibility

Endpoint decisions shape the future of your security program. A closed endpoint-led ecosystem may simplify some decisions today, but it can also make future changes harder.

An open-XDR foundation keeps the security operations platform constant, even as organizations change tools across network, SaaS, cloud, infrastructure, and endpoint. Endpoint should strengthen and complement security operations without forcing a closed, all-or-nothing stack that benefits a vendor over a security operations leader.

Endpoint telemetry in context

Endpoint telemetry is valuable because both user and attacker activity happen at the endpoint. Processes launch, scripts run, credentials are used, files are accessed, and network connections are made. That activity can reveal meaningful differences between expected behavior, unusual behavior, and possible compromise.

But endpoint activity only becomes useful signal when it is analyzed in context. A script may be expected for one user but suspicious for another. A login may look normal until it is paired with unusual device activity, cloud access, privilege changes, known exposure, or activity from another part of the environment. The endpoint shows what happened. Context helps explain whether it matters.

That context rarely comes from the endpoint alone. It comes from connecting endpoint telemetry with identity, cloud, network, email, SaaS, mobile, vulnerability, asset, and business signals. Endpoint telemetry is reviewed in nearly 95% of Arctic Wolf SOC investigations, which reinforces how important endpoint activity is when it is connected to the broader security operations picture.

Organizations should evaluate whether the solution can ingest and correlate signals across the environment, not just collect endpoint events. The goal is to turn endpoint activity into clear, prioritized, and actionable context that helps teams understand what happened, why it matters, and what should happen next.

Security platform and agentic workflows

Context creates the foundation. Agentic workflows determine how quickly teams can act on it.

Agentic AI should help teams move faster through triage, investigation, response, and remediation. It should summarize what happened, enrich alerts with current threat intelligence, identify likely attack paths, recommend next steps, and support response actions with appropriate guardrails and human oversight. The value is not "AI" as a feature. The value is faster, more consistent execution when time matters.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

Agentic security operations should not become another implementation project for constrained teams. If organizations have to prepare data, build agents, design workflows, test automations, manage model behavior, monitor usage costs, and govern AI decisions themselves, they have added work instead of reducing it. The stronger buying question is simple: Who does the work?

Organizations should evaluate whether agentic workflows are delivered as part of the operating model from day one. At the very least, a solution should help triage alerts, investigate activity, prioritize what matters, support intelligent response actions, and guide remediation without requiring the customer to build the AI operating model. The goal is to shorten time to response, improve decision quality, and keep humans in the loop for judgment, validation, and escalation.



Cross-domain response

Beyond the value of evaluating endpoint telemetry in context, attackers do not start or stop at the endpoint. Threat actors exploit the gaps between attack surfaces and point tools because organizations often have blind spots in these in-between spaces.

If endpoint activity indicates credential theft, response should extend to identity controls such as revoking sessions, resetting credentials, and blocking suspicious access.

Endpoint response should be evaluated as part of an attack chain workflow, not just a device workflow. Basic containment still matters, but containment alone is not enough when attacker activity crosses into identity, cloud, SaaS, email, or network environments.



Tuning and configuration aligned to operational reality

Even the very best endpoint tools can fail to secure organizations from threats. But it is not always the tool; it is often the operations that fall short. Tools are only effective when they are fully deployed, configured, tuned, and maintained correctly.

That makes tuning and configuration support a core buying criterion. Endpoint policies need to reflect how the organization actually works: users, workflows, business constraints, risk tolerance, and operational dependencies. Too much friction can disrupt productivity. Too little control can leave gaps.

Endpoint effectiveness depends on keeping policies, controls, and coverage aligned to real-world conditions, not just enabling features on paper. A strong endpoint program should adapt as users, devices, applications, policies, threats, and business requirements change, which means that teams need to evaluate if they have the resources on hand to optimize their endpoints regularly or if they need additional support from a vendor.



Defense in depth includes business resilience

Security teams are used to thinking about defense in depth in terms of controls: layered prevention, detection, and response across the environment. But defense in depth should also extend beyond technology to the business itself.

No endpoint tool prevents every attack. Skilled security teams using effectively tuned and capable tools and strategies can mitigate the risks posed by these attacks. Those strategies need to include additional layers of resilience and contingencies. Organizations should operate from the position that their security controls will fail and plan for what happens next. In adopting this mindset, the question can't solely be focused on "how do we prevent a breach?" but must also include "how do we protect our business when a breach occurs?"

Thinking about how endpoint security fits into a broader security operations program and incident response framework also means evaluating it in the context of business resilience. That includes how it supports incident response execution, security operations warranties, and cyber insurability.

This shift changes how organizations should think about risk transfer and financial resilience. Endpoint security now plays a role in supporting incident response readiness, helping organizations qualify for security operations warranties, and improving cyber insurability. Organizations should evaluate whether their endpoint solution helps meet the operational requirements behind these programs, including consistent detection, reliable response workflows, and the ability to contain and recover from real-world attacks.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

05 Baseline Criteria vs. the New Standards

STANDARD CRITERIA	WHY IT STILL MATTERS	WHAT ELSE MATTERS NOW
Prevention efficacy	Endpoint security still needs to stop known and unknown threats before they execute. Aurora Protect blocked hundreds of malicious files per customer on average last year, with a reported 99% true-positive rate.	Prevention is the entry point, not the full decision. Organizations also need to evaluate what happens when prevention fails.
EDR and behavioral detection	Detection and response are required when prevention does not stop suspicious activity.	Detection should connect endpoint activity to identity, cloud, network, SaaS, email, mobile, and business context.
Telemetry and alerting	Endpoint telemetry is reviewed in nearly 95% of Arctic Wolf SOC investigations.	The question is not whether the endpoint produces data. The question is whether that data becomes clear, prioritized signal that gets used.
Response actions	Containment, remediation, and response actions help limit damage.	Response should follow the attack chain, not just the device.
Deployment and management	Fast deployment improves time to value.	Organizations should ask who validates coverage, tunes policies, identifies drift, and keeps controls aligned over time.
AI features	AI can support faster triage, investigation, and prioritization.	AI should arrive as an operational outcome with guardrails and human oversight, not as a customer-built project.
Managed support	Many teams need help operating endpoint security effectively.	The buying question is whether the solution closes the gap between owning controls and getting outcomes.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

06 Evaluation Framework for Endpoint Security Vendors

EVALUATION AREA	BEST-PRACTICE BENCHMARK	WHY IT MATTERS
Baseline endpoint protection	Strong prevention, EDR, behavioral detection, response actions, OS coverage, mobile support, efficient performance, and independent validation (from customers and analysts).	The endpoint still needs to do the job: prevent, detect, respond, and support coverage across the estate.
Open architecture	Open ingestion, agnostic response, third-party integrations, and the ability to preserve tool choice over time.	Endpoint decisions can shape future security operations architecture and switching costs.
AI foundation	AI grounded in security operations data, validated workflows, customer context, human oversight, and clear control boundaries.	AI without context and guardrails can create more work and more risk.
Contextual signal	Endpoint, identity, cloud, network, email, SaaS, mobile, asset, vulnerability, and business context combined into prioritized signal.	Endpoint activity is most useful when analyzed alongside other signals.
Agentic outcomes	Agentic workflows delivered as part of the operating model from day one, with humans in the loop for judgment and escalation.	Security teams do not need another AI implementation project.
Cross-domain response	Coordinated response across endpoint, identity, network, cloud, email, SaaS, and other workflows.	Modern attacks move across attack surfaces and exploit the gaps between point tools.
Operational execution	Deployment validation, configuration support, policy tuning, drift detection, endpoint health checks, and ongoing operational guidance.	Tools fail when they are not deployed, configured, tuned, or maintained correctly.
Business resilience	Consistent detection, reliable response workflows, containment, recovery, and alignment with incident response and resilience plans.	Endpoint security can support incident response readiness, cyber insurability, and risk transfer outcomes.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

07
Final Thoughts

Endpoint security is no longer a tool decision. It is a security operations decision.

Prevention, detection, and response still matter, but they do not determine long-term outcomes on their own. The real decision is whether endpoint security can be deployed, tuned, operated, and continuously improved as part of a broader security operations model.

The new buying criteria lead to a simple conclusion: endpoint security delivers value only when it is operationalized. That means connecting endpoint telemetry with broader context, reducing noise, prioritizing what matters, responding across the attack chain, and keeping policies aligned to how the organization actually operates.

Aurora Endpoint Security is designed for that model. Built on the Aurora Superintelligence Platform, it brings endpoint telemetry into a broader security operations foundation that connects activity across identity, cloud, network, email, SaaS, and mobile environments. This moves organizations from isolated alerts to coordinated detection and response.

The Aurora Agentic SOC delivers agentic workflows as part of that operating model, helping triage, investigate, and prioritize alerts with current threat intelligence and customer context. Teams do not need to build or manage AI workflows. The system is designed to deliver outcomes from day one, with human oversight built in.

This approach improves operational consistency and reduces alert burden. **Arctic Wolf triaged, investigated, and actioned 96.5% of endpoint alerts on behalf of customers last year,** helping teams focus on what matters most.

At the same time, endpoint protection remains strong. Aurora Protect blocked hundreds of files per customer on average last year with a reported **99% true-positive rate, while operating with approximately 27% lower resource consumption than the industry composite.** These outcomes are sustained through continuous tuning, policy alignment, and operational workflows that adapt as environments and threats evolve.

Endpoint activity also plays a central role in security operations. **Endpoint telemetry is reviewed in nearly 95% of Arctic Wolf SOC investigations,** reinforcing its value when analyzed in context and connected to broader response workflows.

The result is an endpoint security model that goes beyond protection alone. It connects prevention, detection, investigation, response, and continuous improvement into a single operating model that helps organizations reduce risk, reduce noise, and respond with confidence.

The right endpoint decision does more than protect devices. It turns endpoint security into a security operations advantage.

©2026 Arctic Wolf Networks, Inc. All rights reserved. | Public

About Arctic Wolf

Arctic Wolf is the cybersecurity and AI company that ends cyber risk by transforming it into business resilience. Powered by the Aurora® Superintelligence Platform, Arctic Wolf delivers modern security operations built on proprietary AI and decades of real-world expertise. By combining AI-driven automation with expert validated precision, Arctic Wolf helps organizations confidently manage cyber risk — so organizations can operate with control and the freedom to innovate.

To learn more about Arctic Wolf, visit **arcticwolf.com**.

REFERENCES

FBI IC3, 2025 Internet Crime Report

CISA, Known Exploited Vulnerabilities Catalog and Cybersecurity Alerts and Advisories

NIST, Cybersecurity Framework 2.0

World Economic Forum, Center for Cybersecurity

ARCTIC WOLF RESOURCES

Aurora Endpoint Security

Arctic Wolf Security Operations Bundles

Arctic Wolf Security Operations Warranty

©2026 Arctic Wolf Networks, Inc., All Rights Reserved. Arctic Wolf, Arctic Wolf Platform, Arctic Wolf Security Operations Cloud, Arctic Wolf Managed Detection and Response, Arctic Wolf Managed Risk, Arctic Wolf Managed Security Awareness, Arctic Wolf Incident Response, and Arctic Wolf Concierge Security Team are either trademarks or registered trademarks of Arctic Wolf Networks, Inc. or Arctic Wolf Networks Canada, Inc. and any subsidiaries in Canada, the United States, and/or other countries.

AW_G_EDR BUYERS_0826