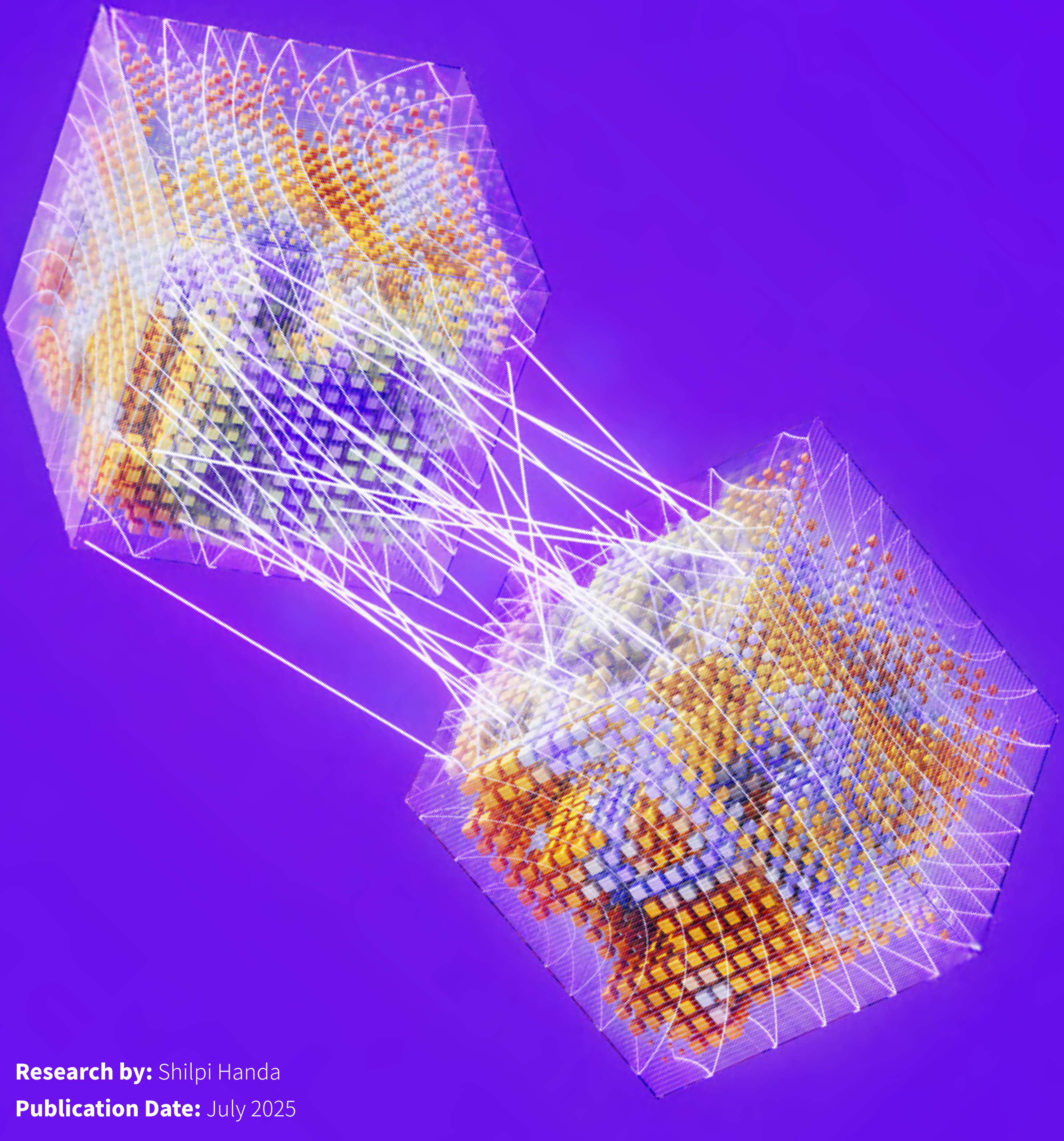
An IDC whitepaper, sponsored by:

Endpoint Security in the Age of AI
Resilience by Design, Intelligence by AI



Research by: Shilpi Handa

Publication Date: July 2025

Table of Contents

As AI-driven threats push the boundaries of cyberattacks, the security of every endpoint within the organization becomes paramount. Each unsecured or inadequately secured endpoint isn't just a weak link — it's an open door, expanding the attack surface and leaving critical assets exposed. The era of relying on traditional security measures is over; modern challenges demand sophisticated, innovative solutions to stay ahead of evolving threats.

The most secure endpoints are secure by design, equipped from the outset with a purpose-built security platform that seamlessly integrates with the wider contextual telemetry. This integrated approach minimizes vulnerabilities and establishes a robust defense against advanced cyberattacks.

Investing in such advanced security isn't just about protection — it's also about ROI. Endpoint security platforms deliver tangible value by automating processes, reducing dependence on inexperienced analysts, consolidating tools, and significantly accelerating resolution and reporting. If these investments involve the right vendor, they often pay for themselves several times over.

The game changer in selecting an efficiency-driven provider is the seamless integration of AI at the core of its security strategy. AI isn’ t just a tool — it’ s the engine powering transformation. It's essential to choose AI-driven security agents that operate in perfect harmony with endpoints, delivering powerful on-device protection that doesn’ t rely on connectivity. These are continuously refined by cloud-based intelligence and offer dynamic, adaptive defense, equipping organizations with a resilient and ever-evolving shield against modern threats.

Secure your organization's future with a strategy that goes beyond risk mitigation to deliver tangible business value. Transform every endpoint into a pillar of resilience with AI-driven solutions that maximize protection and ROI.

Take the first step toward smarter security today — empower your organization with AI-driven defense.
Smarter technology for all
Lenovo

From Component to Cloud: The State of Endpoint Security

Comprehensive Security: From OS to Cloud

As businesses race headlong into the digital age, the very definition of an “endpoint” has exploded — from the traditional desktop PC to an ever-widening array of devices and workloads. Endpoints have continuously expanded from the early days of desktop PCs and laptops to include servers, mobile devices, IoT sensors, operational technology machines, and even human interfaces, and now, with AI-driven agents and models residing on devices and in the cloud, endpoints encompass intelligent workloads themselves. Each new endpoint introduces potential vulnerabilities and new complexities for cybersecurity professionals.

Security has always been in a race to keep up, and many believe it has managed to evolve alongside technology. Initially, during the antivirus (AV) era, early PCs depended on signature-based AV software to scan disks and memory for known malware patterns. As new threats, such as trojans, spyware, and complex email-borne malware, appeared, security vendors responded by creating “endpoint suites” that combined firewalls, antispyware, and patch management tools. With the advent of cloud computing and containerization, the concept of endpoints expanded to include multitenant infrastructures. The proliferation of IoT devices and the increase in remote work further amplified the number of unmanaged and often underprotected endpoints. In response, extended detection and response (XDR) platforms emerged. These platforms integrate telemetry from various sources, including endpoints, networks, emails, and identity systems, into a unified “data lake” for comprehensive security management.

While security technology has kept pace with the proliferation of endpoint devices, adoption has lagged. **IDC’ s Worldwide Endpoint Security Survey reveals that the top 2 endpoint security solutions in use globally are traditional antivirus/antimalware software and cloud-based endpoint security solutions.**

Worldwide Adoption of Endpoint Security Solutions

Question: What type of endpoint protection solution is your organization currently utilizing?

75%
Cloud-based endpoint security solutions

75%
Antivirus/antimalware software

73%
Endpoint detection and response (EDR)

72%
Endpoint protection platform (EPP)

60%
Zero trust network access for endpoints

54%
Mobile device management

54%
Extended detection and response

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

This revelation is hardly surprising; it highlights a long-standing issue — the reliance on disparate point solutions for on-premises endpoint security and separate solutions for cloud security, which inadvertently expand the threat surface by creating vulnerabilities. On-premises security continues to rely on traditional antivirus solutions that are four decades old, while cloud-based security solutions protect cloud endpoints. These isolated systems contribute to security gaps, making endpoints one of the most significant threat vectors. **Among the more startling findings from the survey is that 81% of the financial industry worldwide, the most regulated and frequently targeted sector, still relies on traditional AV solutions.** Moreover, the adoption of advanced, uniform, telemetry-based XDR solutions remain notably low across the world.

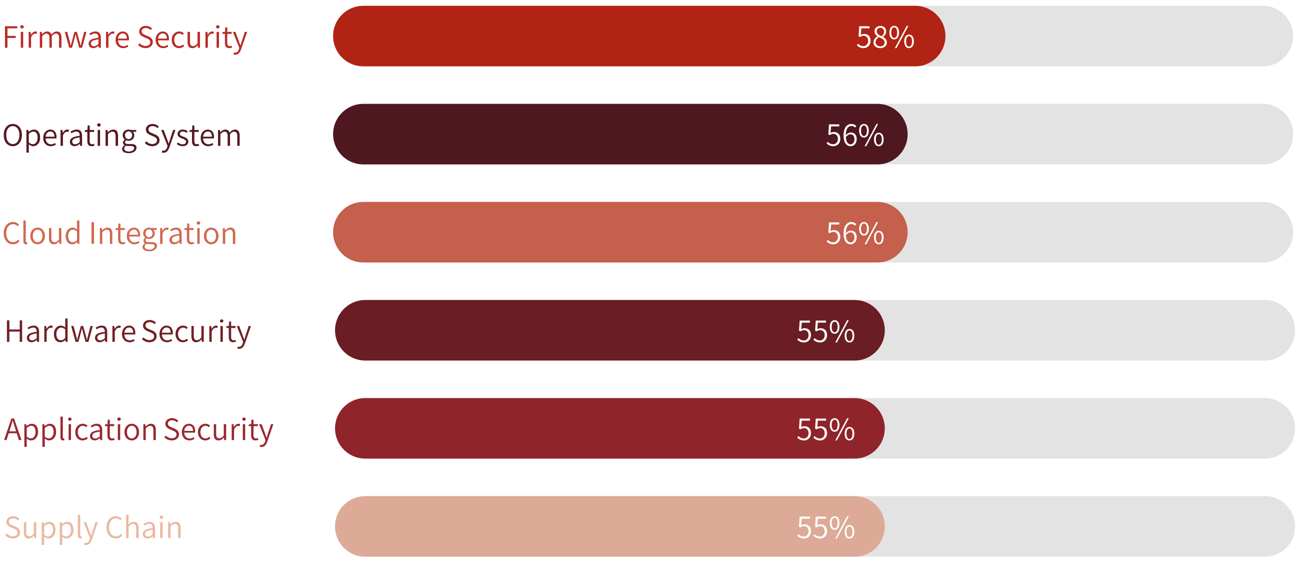
Layered Defense: Securing Every Level

The uniformity issue in security solutions runs deeper than it appears on the surface. Security uniformity should extend beyond on-premises and cloud infrastructure. While many security solutions emphasize hybrid infrastructure coverage, which is crucial, they often overlook the granular aspects of security. Effective endpoint security must encompass multiple layers, including firmware, hardware, OSs, applications, and supply chain security. A standardized, layered approach to endpoint security is essential, yet modern solutions often fall short.

IDC’ s Worldwide Endpoint Security Survey uncovers significant insights: over half of the surveyed security professionals express dissatisfaction with their current endpoint security providers, citing shortcomings across multiple aspects of endpoint security.

The widespread dissatisfaction spans across all key areas, such as firmware, supply chain, hardware, application, OS, and cloud security.

Question: How well do you rate your current endpoint security provider addressing each of the following security areas?



Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

Current endpoint security solutions do not fully address any single area. When analyzing data across industries, it becomes evident that critical industry use cases remain unmet. For instance, in the retail sector, application security is largely suboptimal, with nearly 66% of respondents expressing dissatisfaction. **In the energy and utility sector, where hardware security is paramount, 62% are dissatisfied with the security solutions of their endpoint providers.**

Endpoint hardware security features, including Trusted Platform Modules (TPMs), encrypted storage, and secure enclaves, are pivotal in establishing a robust hardware root of trust that effectively resists tampering and theft of cryptographic keys. TPMs provide secure key storage and attestation, encrypted storage ensures data remains protected even in compromised devices, and secure enclaves isolate sensitive computations from potential breaches. These features form a tamper-resistant foundation critical for protecting sensitive data and maintaining device integrity.

Complementing this, OS security plays a vital role by enforcing stringent user permissions, deploying advanced security agents, such as AV and EDR systems, and mediating access to resources. These agents monitor and neutralize threats in real time while ensuring secure resource allocation and policy enforcement. This dynamic OS layer is essential for implementing adaptive, real-time defenses that can respond swiftly to emerging threats. Together, these hardware and OS security measures form a comprehensive defense strategy and should be a primary focus for endpoint security solution providers.

In the financial services industry, firmware security falls short for 62% of organizations. Firmware security is vital for the sector, as it faces the highest number of advanced threats that bypass traditional defenses. Firmware security is important for all sectors, not just the financial segment, and it is where the maximum gap exists in today' s endpoint security solutions, with 58% of professionals indicating insufficient coverage. Modern threats increasingly target firmware because code at this level can subvert Secure Boot, conceal rootkits below OS visibility, and persist across reboots and OS reinstalls. Unlike application or OS patches, firmware updates have historically been rare and challenging, leaving devices exposed for extended periods. Without firmware integrity, hardware may misreport its state, and OS protections (AV, EDR) can be bypassed from below, granting attackers full system control with minimal detection risk.

Firmware security, which is often neglected and is currently largely unaddressed by the most modern endpoint security providers, is critical because it underpins and validates both the hardware root of trust and the OS. If firmware is compromised, hardware protections can be disabled or spoofed, and the OS can be loaded with malicious code, rendering higher-level defenses ineffective.

Superficial endpoint security solutions prevent effective modern threat management; depth at every layer is crucial. A holistic endpoint security strategy must standardize protections across firmware, hardware, and OSs to close the gaps that adversaries frequently exploit. **Unfortunately, survey findings indicate that current solutions may not sufficiently address the complex and evolving nature of cyberthreats, highlighting the need for a reevaluation of security practices and technologies.** Therefore, it is essential to assess solutions layer by layer for comprehensive coverage.

Supply Chain Security: Safeguarding Every Link

Another essential aspect of endpoint security is safeguarding the links — software supply chain security that underpins all endpoint components and has become a prime target for attackers. High-profile breaches, such as the 2020 SolarWinds hack and the 2021 Kaseya compromise, have demonstrated how the insertion of malicious code into a vendor' s software can proliferate across thousands of endpoints. The dependency on third-party services, as in the case of CrowdStrike, also poses significant risks to productivity. In an era of tariff wars, securing the supply chain is fundamental to operational and cyber-resilience.

A single-point failure within a supply chain, such as a critical vendor, can have widespread repercussions, affecting multiple organizations. Overreliance on external services can introduce systemic risks if those services experience failure or downtime. **According to IDC, 61% of organizations reported experiencing a third-party data breach in the past 12 months, underscoring the vulnerabilities inherent in extended supply chains.**

This "weakest link" risk necessitates that endpoint security cannot overlook vendor trust. Organizations must operate under the assumption that any third-party component could be compromised. Practically, this requires implementing comprehensive end-to-end controls, including code signing, software bills of materials, vendor security assessments, and continuous monitoring. The supply chain forms the foundation of endpoint security resilience; if the chain is insecure, every endpoint built on it is vulnerable.

AI Protection for an AI Landscape

Beyond comprehensive, layered, and interconnected endpoint security, security intelligence plays a crucial role in elevating the effectiveness of modern endpoint solutions. The power of AI, particularly through neural networks in endpoint security, should not be underestimated. Neural networks excel at analyzing vast amounts of telemetry data to identify patterns and anomalies that traditional methods might miss. This capability enhances the capacity to detect sophisticated threats, such as zero-day attacks, and automate responses to minimize damage. Neural networks feed the AI engine, allowing it to learn from vast amounts of data and continuously improve its threat detection capabilities. This intelligence is an important defense against AI-driven threats.

Modern endpoint security solutions must leverage neural network-based intelligence that is robust, responsive, and capable of anticipating and countering new attack vectors. **Like endpoint security, threat intelligence should be comprehensive, offering seamless, standardized protection across on-premises and cloud environments. This includes integrating on-device and cloud-based analytics to create a unified security framework that addresses diverse and evolving attack surfaces.**

Superior Intelligence: Unified and Dynamic AI

AI-driven threat intelligence is non-negotiable for modern defense. Standardizing it on-device and in the cloud represents a strategic defense approach that can be a game changer in modern defense.

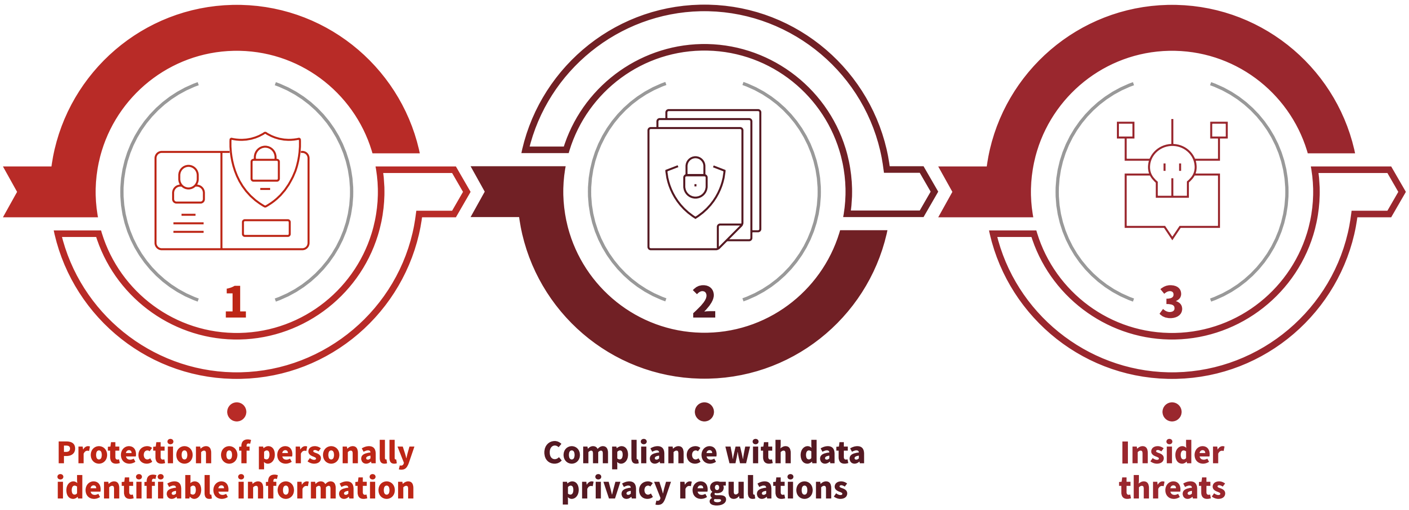
On-device intelligence typically manifests as a static AI engine, which utilizes machine learning models to scrutinize files, scripts, or binaries for malicious attributes without executing them, thereby enabling pre-execution threat detection. This method involves comparing file characteristics — such as byte sequences, header metadata, and embedded code structures — against patterns derived from extensive data sets of known malicious and benign samples.

AI agents that perform real-time data analysis allow for immediate threat detection and response. This reduces the latency associated with sending data to a centralized server for analysis, facilitating quicker mitigation of potential security breaches. Static AI engines operating locally on devices can offer several key advantages for endpoint security. They can minimize bandwidth usage by reducing data transfer across networks, which is particularly beneficial in environments with limited connectivity. These engines can enhance scalability, enabling each device to independently analyze and respond to threats, thereby simplifying the management of large networks. They can provide customization and flexibility, allowing for tailored security measures based on individual risk profiles. Local AI engines ensure resilience against network disruptions, maintaining security operations even during outages. They enhance threat intelligence by continuously learning from locally processed data, aiding in the identification of new threats.

While there are numerous benefits to using local AI agents, the most critical case for security professionals globally is maintaining user privacy. By processing data locally, sensitive information does not need to be transmitted over the network, reducing the risk of exposure during data transfer and ensuring compliance with privacy regulations. **According to IDC's Worldwide Endpoint Security Survey, 57% of professionals globally believe that endpoint security solutions need to prioritize the protection of personally identifiable information (PII), making it the top security concern associated with such solutions.** Compliance with data protection requirements ranks as the second most important concern.

Concerns with current endpoint security solutions

Question: What additional security concerns should endpoint protection platforms help mitigate?


1
Protection of personally identifiable information
2
Compliance with data privacy regulations
3
Insider threats

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

Compliance with privacy protection laws and regulations often necessitates on-premises analysis for certain critical servers or endpoints. In such scenarios, an endpoint platform that leverages behavioral AI engines can be invaluable. Endpoint security platforms generally leverage various types of engines to provide comprehensive protection, such as:

Behavior-based:

Identifies threats by analyzing deviations from normal user or system behavior, detecting unknown attacks based on suspicious activity patterns

Telemetry-based anomaly detection:

Collects and analyzes endpoint data (e.g., network traffic, file access) to flag anomalies that deviate from expected behavior

Predictive:

Uses machine learning to predict potential threats by analyzing historical and real-time data, enabling proactive defense before an attack occurs

Reinforcement learning for response:

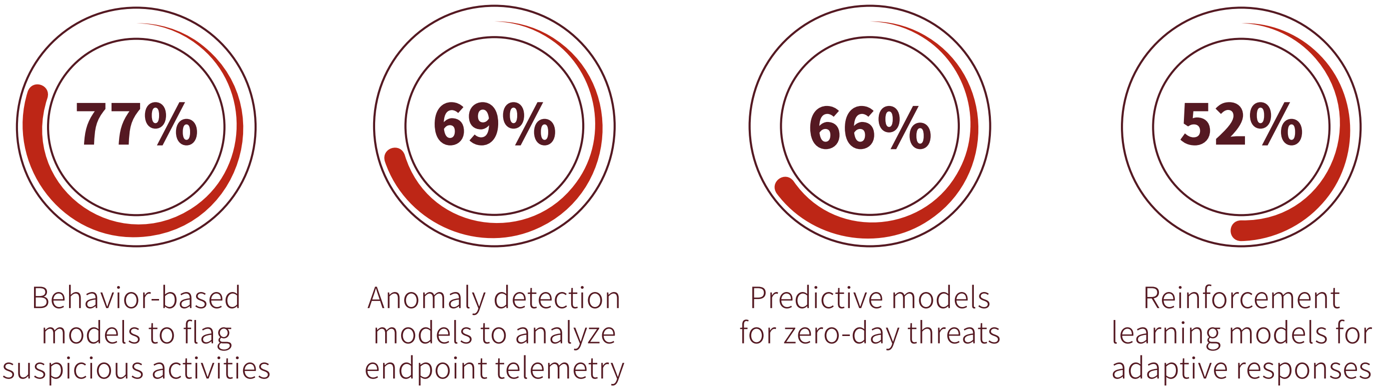
Trains AI systems to optimize responses by learning from outcomes, improving automated threat containment and remediation over time

Of these, behavioral AI engines monitor live system activity, observing processes, scripts, and memory for suspicious tactics, such as code injection or anomalous behavior. They are particularly effective in identifying fileless or zero-day attacks that static analysis might overlook. By correlating process activity in real time, behavioral engines can detect deep memory exploits, such as memory-resident attacks, and promptly flag them.

Behavioral AI engines provide a dynamic layer of security by continuously learning and adapting to new threat patterns. This adaptability is essential for both on-device and cloud environments. The on-device capability ensures that protection is immediate and continuous, maintaining vigilance and monitoring every activity in real time, even when the device is offline. **According to IDC' s Worldwide Endpoint Security Survey, 77% of respondents favor behavior-based learning models for identifying suspicious activities, highlighting the increasing dependence on these advanced technologies to bolster endpoint security. In the Middle East and Africa, as well as North America, the preference for behavior-based models is even more pronounced, with up to 81% of organizations expressing a proclivity for these models.**

Preference for Machine Learning Models

Question: What types of machine learning models do you prefer endpoint protection platforms to leverage?



Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

Cloud Neural Networks Fueling Device AI

While on-device AI offers immediate local defense, cloud-based AI provides a broader global context, making it indispensable for endpoint security. Cloud-based AI agents are crucial due to their scalability, flexibility, and centralized management capabilities, allowing organizations to efficiently extend security measures across numerous endpoints, ensuring consistent protection regardless of device location.

Cloud-based neural networks play a pivotal role in fueling on-device AI agents within endpoint security frameworks. These networks provide the computational power and expansive data resources necessary for training sophisticated AI models for deployment on individual devices. By leveraging the cloud, AI agents on devices can access vast amounts of data and advanced algorithms, enabling them to learn from diverse threat patterns and continuously improve their detection capabilities.

The integration of cloud-based neural networks allows on-device AI agents to benefit from real-time updates and insights derived from global threat intelligence. This ensures that the AI models remain current and effective against emerging cyberthreats. The efficiency of scaling this analysis across various endpoints can vary significantly depending on the provider. However, cloud-based solutions significantly alleviate the computational burden on individual devices, ensuring that they maintain optimal performance without sacrificing security. By offloading intensive processing tasks to the cloud, these solutions free up local resources, allowing devices to operate efficiently while still benefiting from robust security measures. Additionally, cloud-based platforms foster collaboration and threat intelligence sharing across various sectors, thereby enhancing defenses against increasingly sophisticated cyberthreats.

Prioritizing Advanced Threats Is Critical

The two-tier model, combining local and cloud AI, ensures that each device benefits from fleetwide learning capabilities. When it detects novel malware on one device, it can swiftly classify and block the intrusion across the entire network.

A significant advantage of on-device AI is its ability to provide continuous protection. Endpoint agents remain effective without requiring constant connectivity, allowing security measures to persist, even in disconnected or "air gapped" scenarios. Modern solutions must function in air-gapped environments, enabling "protective actions even in the case of disconnected operations.” This capability allows enterprises to securely manage endpoints that occasionally lose cloud connectivity, ensuring that protection is always active, whether online or offline.

Modern endpoint security solutions can handle the most elusive threats that bypass traditional defenses — such as malware, phishing, advanced persistent threats (APTs), and insider threats. Yet, instead of utilizing such solutions, many customers remain focused on combating day-to-day malware. This tendency stems from the relative familiarity and simplicity of these threats. However, this misplaced prioritization often results in the oversight of critical, complex risks, including zero-day vulnerabilities and supply chain attacks, leaving organizations exposed to significant security gaps.

While less frequent, these advanced threats carry far more devastating consequences, yet they often rank lower on customers' priority lists due to a lack of awareness, technical expertise, or a clear understanding of their potential impact. This imbalance in threat management leaves organizations vulnerable, exposing them to risks that can severely disrupt operations, damage reputations, and result in significant financial losses.

Endpoint Security Solutions Fail to Provide Protection Against Many Threats

Question: What types of attacks do your endpoint security solution fail to provide protection against?

48%	Malware
44%	Phishing attacks
43%	Advanced Persistent Threats (APTs)
41%	Insider threats
38%	Denial-of-service (DoS)/ Distributed denial-of-service (DDoS)
35%	Fileless malware
34%	Credential theft
31%	Ransomware
30%	Zero-day attacks
30%	Supply chain attacks

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

End-To-End Visibility

A possible reason for these misplaced priorities is that implementing effective endpoint security is a challenging task. While technological depth across various layers is crucial, the breadth of coverage is paramount to prevent threats from slipping through the cracks. This complexity makes the solution intricate, and scaling it across an organization becomes a formidable endeavor. The vast array of devices, from traditional desktops to mobile devices and IoT sensors, further complicates the maintenance of robust security protocols throughout the network.

No Silos — One Platform for All Tools

Not every solution provider is equipped to harmonize endpoint security across such a diverse landscape. This gap leads to numerous challenges for IT professionals. According to **IDC' s Worldwide Endpoint Security Survey, three primary concerns stand out: the difficulty in managing and updating endpoint agents, insufficient integration, and limited visibility into endpoint activity across the network.** These issues underscore the need for comprehensive solutions that can seamlessly integrate and manage security protocols across varied devices and environments.

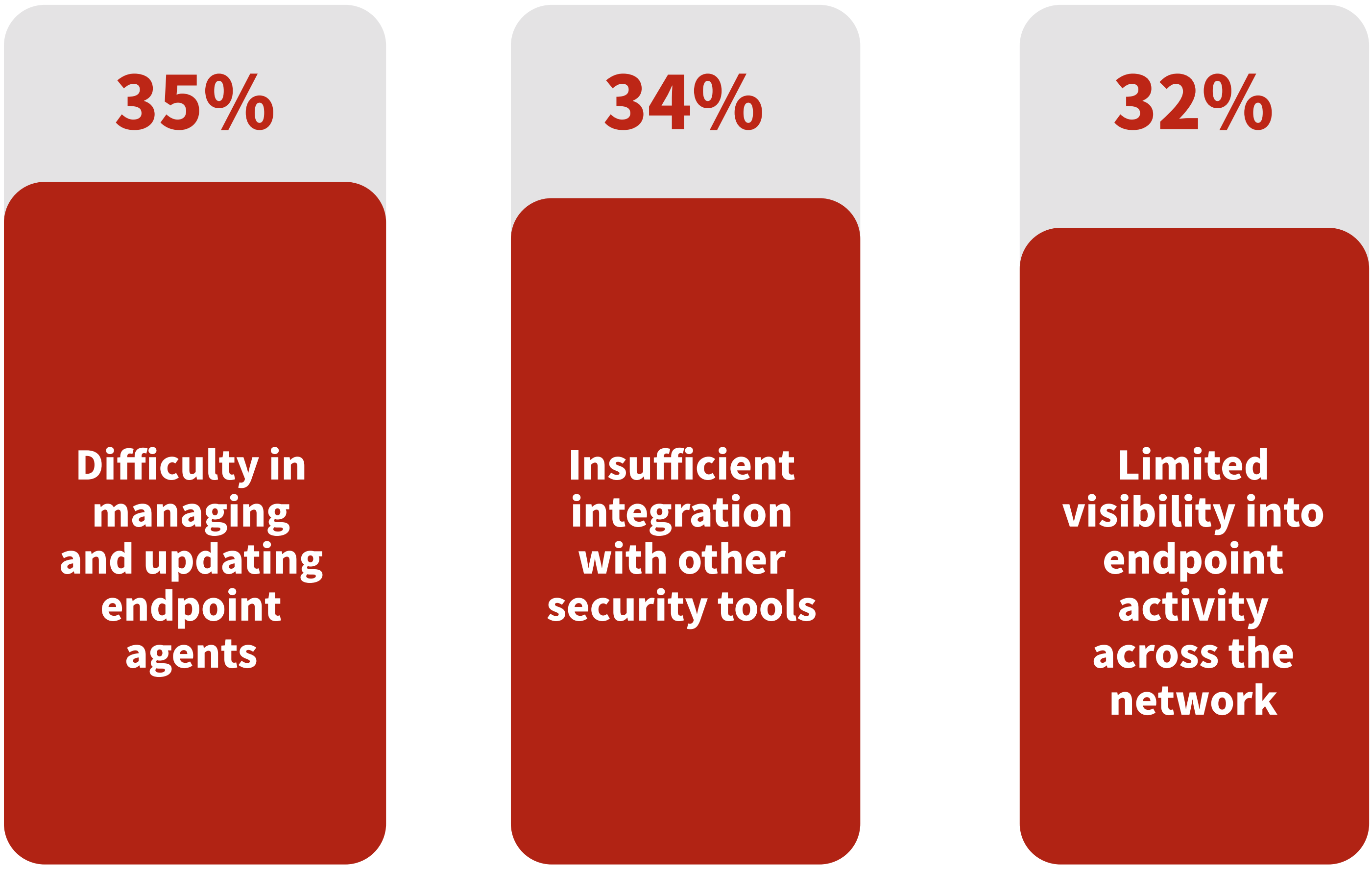
Managing and updating endpoint agents is a daunting task, as it requires consistent oversight and coordination to ensure that all devices have the latest security patches and configurations. The diverse range of OSs and device types within an organization further complicates this process.

Insufficient integration poses a significant hurdle, as many security solutions operate in silos, preventing seamless communication and collaboration between different systems. This lack of integration can lead to gaps in security coverage, making it difficult to implement a cohesive defense strategy across the entire network.

Limited visibility into endpoint activity is the most critical challenge, as it hampers the ability to detect and respond to threats in real time. Without comprehensive visibility, security teams struggle to identify suspicious behavior and potential vulnerabilities, leaving the organization exposed to cyberattacks.

Top Three Challenges with Current Endpoint Solution

Question: What are the top 3 challenges your organization faces with its current endpoint protection solution?



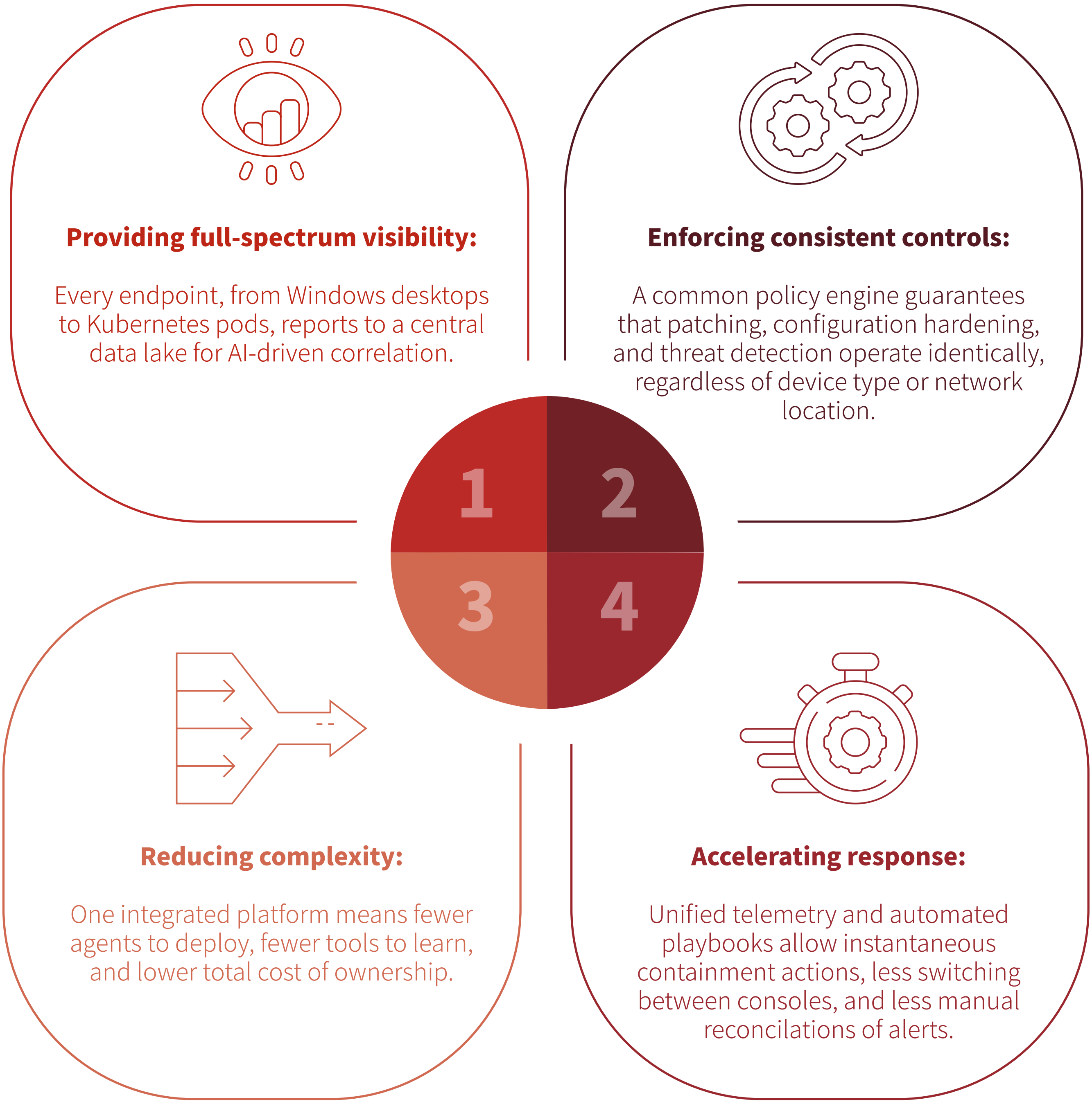
Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

All-Encompassing Platform Coverage

A truly effective security platform transcends the limitations of a single system with restricted coverage. By employing advanced analytics, it extends across diverse environments to address the myriad challenges users encounter. The platform performs extensive data crunching at machine scale and automates processes, ensuring comprehensive and efficient security management.

According to IDC' s Worldwide Endpoint Security Survey, many modern tools fall short of providing comprehensive solutions, resulting in issues such as inconsistent protection across various OSs, complexity in managing EPP solutions across hybrid environments (cloud and on-premises), and high operational overhead for managing multiple device types and environments.

Addressing these challenges requires a strategic approach that emphasizes unified security management, enhanced integration, and improved visibility. A truly uniform endpoint security solution — one agent, one console, one policy framework across OS to the cloud — closes these gaps by:



Providing full-spectrum visibility:

Every endpoint, from Windows desktops to Kubernetes pods, reports to a central data lake for AI-driven correlation.

Enforcing consistent controls:

A common policy engine guarantees that patching, configuration hardening, and threat detection operate identically, regardless of device type or network location.

Reducing complexity:

One integrated platform means fewer agents to deploy, fewer tools to learn, and lower total cost of ownership.

Accelerating response:

Unified telemetry and automated playbooks allow instantaneous containment actions, less switching between consoles, and less manual reconcilations of alerts.

XDR Data Lake: The Heartbeat of AI Analysis

Security is a data game, and at the core of an AI-driven platform, there should be a data lake, a centralized repository often referred to as the “single source of truth.” This repository stores and normalizes every log, including endpoint process records, network flows, application events, and identity changes. Mastering security requires focus and dedication, akin to becoming a chess grandmaster, or a ninth-dan professional. Just as mastering multiple games is unrealistic, managing numerous disparate security platforms and application data sources can be overwhelming. Instead, focus on one platform and master that “game” to effectively lead security efforts.

Therefore, most organizations strive to achieve full-spectrum visibility, reduce alert noise, and enhance AI-driven correlation across their entire digital landscape. **According to IDC' s Worldwide Endpoint Security Survey, professionals favor solutions with AI-driven data lakes that enhance AI model training by accessing large volumes of diverse data and improve threat detection through real-time data correlation across endpoints and environments.** This comprehensive approach ensures robust security and resilience in the face of evolving cyberthreats.

Preference of an AI-driven Data Lake for Various Benefits

Question: What benefits do you feel a centralized data lake should bring to AI-driven endpoint cybersecurity detection, management, and response?

Enhanced AI model training with access to large volumes of diverse data

Improved threat detection through real-time data correlation across endpoints and environments

Automated and accurate response to incidents through AI-powered insights

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

The data lake requires meticulous crafting using a security-first approach and should be capable of ingesting raw data from a comprehensive array of sources to enrich it with contextual insights. This means achieving the widest possible coverage to ensure no telemetry is overlooked, as any missing data could become a weak link in the security chain. Given the diverse nature of threat vectors, it is crucial to capture and analyze data from every conceivable source to maintain a robust defense.

In the context of modern cybersecurity, telemetry plays a vital role because it provides real-time data that can help detect, analyze, and mitigate threats. Security professionals face an increasing array of attack vectors, many of which evolve rapidly, making it challenging to pinpoint the most critical types of telemetry. The endpoint security survey underscores this challenge, where no single telemetry type stood out as universally more important than others. This variability reflects the complexity of modern threats, requiring a multifaceted approach to security.

Given the variety and sophistication of these threats, relying on a narrow set of data inputs can leave significant blind spots. Adopting a broad telemetry strategy ensures comprehensive coverage of potential attack surfaces, from user behavior analytics and application logs to network traffic and system performance metrics. The more data points, the better the chances of detecting anomalies and threats early in the attack life cycle.

Thus, even though it's difficult to prioritize one form of telemetry over another, the need for a holistic, integrated view of all security-relevant data becomes clear. Broad telemetry coverage enables security professionals to respond proactively to threats, adapt to new attack methods, and fine-tune their defenses.

Telemetry Important for Threat Detection

Question: What types of telemetry should Endpoint Protection Platform (EPP) ingest for analysis and threat detection?

- Identity and access telemetry
- User behavior analytics
- Cloud environment telemetry
- Network traffic data
- Endpoint activity logs
- Application-level telemetry
- Threat intelligence feeds
- System-level telemetry
- Mobile device telemetry

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

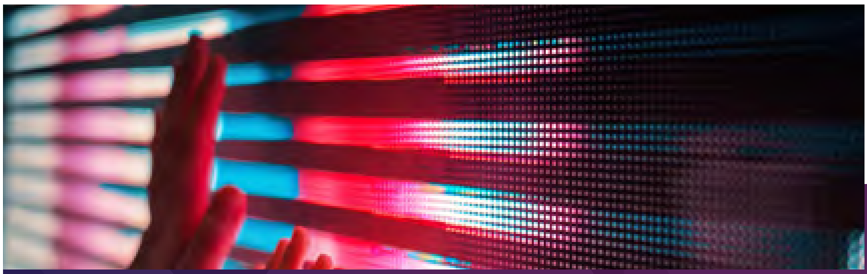
These telemetry sources require continuous and automatic monitoring to ensure comprehensive security coverage. Automated monitoring systems tirelessly mine this data, offering anomaly detection through real-time correlation and sophisticated pattern recognition rather than relying on the labor-intensive process of manually scanning endless logs. Security professionals actively seek this capability worldwide, as it enhances threat detection efficiency and effectiveness.

According to recent surveys, 65% of security professionals emphasize the importance of models that can automatically adapt to new threats in real time. Organizations globally advocate for systems that are continuously updated with real-time threat intelligence, ensuring that defenses remain agile and responsive. **The data lake serves as the powerhouse that drives AI-driven visibility and response throughout the enterprise.**

AI Productivity and User Experience (a Paradigm Shift for Analysts)

Security operations at organizations are experiencing significant transformation through the integration of AI-powered platforms. These platforms automate routine tasks, providing analysts with intuitive interfaces that allow them to interact using everyday language rather than complex query codes. For instance, a SOC analyst can simply type queries such as "List devices running outdated software," and the AI system will parse the request, search the data lake, and deliver results instantly. This innovation eliminates the need for memorizing search syntax and data schemas. This democratization of security data exploration enables junior analysts or non-specialists to access insights without extensive training in query languages. Following an initial query or alert, the user interface often provides "suggested next questions" or action buttons, effectively crowd-sourcing best practices.

AI also automates reporting, generating written executive summaries of incidents or daily/weekly threat reports automatically. By automating routine tasks and reducing false positives, AI significantly alleviates analysts' workloads, enabling them to concentrate on genuine threats rather than being inundated with alerts. This focused approach reduces frustration and burnout, as the system can manage routine actions, such as quarantining an endpoint or blocking an IP, freeing analysts from repetitive tasks.



According to the IDC endpoint security survey, the top 2 benefits that security professionals derive from AI are the generation of AI-driven automated summary reports for quick insights and the ability to provide high-level intelligence that enables automated remediation.

Smarter technology for all

Lenovo

Organizations report that adopting AI-driven tools has markedly reduced alert fatigue and stress, empowering analysts to become proactive detectives with AI support rather than overwhelmed firefighters.

AI-Driven Security: Next-Level Protection and Outcomes

While this paper has discussed the numerous benefits of data lake-driven and AI-powered endpoint security platforms, it's important to recognize that many solution providers often market these as fully realized advantages when they may be only partially developed. Sometimes, these marketed features do not align with what security professionals truly seek in terms of creating tangible, outcome-based improvements in security operations. According to the IDC WW Endpoint security survey IDC survey, from a containment perspective, professionals rate certain features and use cases as essential, underscoring the gap between marketed capabilities and actual needs.

Features

Per IDC’ s Worldwide Endpoint Security Survey, the top 2 features that endpoint security solutions should offer center around advanced AI capabilities, reflecting the evolving needs of security professionals. **Firstly, AI models require continuous training to minimize false positives and negatives, leveraging historical data and feedback to refine their accuracy. This feature, which 63% of professionals favor, underscores the importance of precision in threat detection, ensuring that security teams can focus on genuine threats without distraction from erroneous alerts.**

Secondly, adaptive learning capabilities are crucial, with 64% of professionals emphasizing their importance. These capabilities allow AI systems to automatically adjust thresholds in response to changing environments and threat landscapes. Adaptive learning ensures that security measures remain effective, even as new vulnerabilities and attack vectors emerge. This feature empowers security teams to stay ahead of potential threats, fostering a proactive approach to cybersecurity.

Threat Response

Threat response capabilities are among the most diverse and varied across vendors today, reflecting the dynamic nature of cybersecurity solutions. **According to IDC’ s Worldwide Endpoint Security Survey, security professionals place a high value on automated processes that can swiftly isolate endpoints and block malware or applications in real time.** These workflows are crucial for reducing the time to respond to threats, significantly enhancing an organization’ s overall security posture.

Overall, all the response functions had a high rating, which indicates the growing skill gap in cybersecurity, the increasing complexity of threats, and the need for cost-effective, automated solutions. Automated functions, such as isolating infected endpoints, blocking malicious processes, and rolling back changes, reduce the reliance on manual intervention, which can be slow and error-prone, especially in high-pressure situations.

To fight growing threats, a multidimensional response that addresses various stages of the attack life cycle is essential for ensuring faster, more efficient remediation. Automated, broad-spectrum security responses are becoming vital, as they streamline detection and containment and ensure that organizations stay ahead of increasingly sophisticated attacks, reducing human error and accelerating recovery.

Top response actions that endpoint security solutions should offer for efficiency

Question: What types of response actions and containment options should AI-driven endpoint security solutions offer to reduce the time to respond?

Blocking malicious processes or applications in real time 1

Quarantining suspicious files for further analysis 2

Automated isolation of infected endpoints from the network 3

Source: IDC AI Security Survey, May 2025, n=546 organizations globally, large organizations 1,000+ employees.

Compliance

Endpoint security solutions must go beyond offering robust features and rapid response capabilities; they must also address customers' compliance needs. Some 62% of security professionals increasingly favor solutions that provide mechanisms to obtain explicit consent for data usage, as mandated by data protection regulations. This ensures that organizations can adhere to legal requirements while maintaining their users' trust.

Sixty-one percent of professionals want these solutions to guarantee transparency in data usage, offering clear insights into data collection, processing, and storage methods. Transparency is crucial for building confidence among stakeholders, as it allows them to understand the security measures in place and how their data is being handled. By providing detailed information on data management practices, security solution providers can demonstrate their commitment to privacy and compliance, fostering a culture of accountability and trust.

AI Security

In the realm of AI security within endpoint solutions, ensuring the integrity and confidentiality of data for AI training and analysis is paramount. Recent survey results highlight several critical processes and practices that security professionals prioritize to safeguard data:

- Processes to sanitize large data sets: With 68% of professionals emphasizing this need, robust processes are essential for sanitizing large data sets for AI training.

- Encryption and anonymization: A significant 73% of respondents prioritize the encryption and anonymization of sensitive data during AI training and analysis.

- Regular audits and validations: Ensuring secure data handling is a continuous process, with 64% of professionals advocating for regular audits and validations.

- Automatic PII detection and removal: With 66% of respondents supporting this capability, the automatic detection and removal of personally identifiable information from data sets is a critical feature.

Incorporating these practices into AI security strategies within endpoint solutions enhances data protection and builds trust with stakeholders by demonstrating a commitment to privacy and compliance.

ROI

An important aspect that the conversation about AI-powered and data lake-driven endpoint security platforms often overlooks is the critical need for organizations to choose an ROI-driven vendor solution. The right solution will reduce manual intervention through automation, enabling faster detection, response, and reporting while lowering operational costs. Consolidating tools into a unified platform simplifies operations, cuts licensing expenses, and reduces the need for expensive top-tier SOC analysts, allowing organizations to scale efficiently. It's important that the chosen solution aligns with business goals, offering benefits such as compliance support, risk management, and scalability. By prioritizing vendors that deliver tangible, outcome-based results, organizations can bridge the gap between promises and performance, turning cybersecurity into a strategic growth enabler.

Key Takeaways and Recommendations

To achieve robust endpoint security, take decisive action by implementing layered endpoint security that covers every aspect of your digital infrastructure. Actively evaluate the provided AI capabilities, both online and offline, to ensure they deliver comprehensive threat detection and response. Scrutinize the behavioral analysis component to confirm its effectiveness in monitoring and responding to suspicious activities. Thoroughly examine the data lake’ s coverage depth to guarantee it captures and analyzes a broad spectrum of telemetry for precise threat intelligence. Assess the AI tools’ response capabilities, focusing on their ability to automate and streamline remediation processes efficiently. Prioritize solutions that address critical use cases, such as compliance, and include essential remediation features. Finally, rigorously evaluate the safety and reliability of the provider’ s AI, ensuring it meets security standards and safeguards sensitive data.

1. **Secure every layer:** Proactively protect firmware, hardware, software, and the entire supply chain to eliminate vulnerabilities.

2. **Adopt two-fold AI:** Implement both on-device and cloud-based AI for comprehensive behavioral monitoring, enhancing threat detection and response.

3. **Centralize data:** Streamline operations by consolidating data management for efficient analysis and decision-making.

4. **Embrace automation:** Boost operational efficiency and accelerate response times by integrating automation into security processes.

5. **Consolidate your stack:** Integrate diverse security tools into a unified infrastructure to reduce complexity and improve effectiveness.

6. **Seek output-based solutions:** Focus on solutions that deliver measurable outcomes in compliance, response, feature robustness, and AI security.

7. **Foster vendor collaboration:** Partner with vendors offering integrated hardware and software security solutions to foster a cohesive and comprehensive security strategy.

About Lenovo

Lenovo is a US$57 billion revenue global technology powerhouse, ranked #248 in the Fortune Global 500, and serving millions of customers every day in 180 markets. Focused on a bold vision to deliver Smarter Technology for All, Lenovo has built on its success as the world' s largest PC company with a full-stack portfolio of AI-enabled, AI-ready, and AI-optimized devices (PCs, workstations, smartphones, tablets), infrastructure (server, storage, edge, high performance computing and software defined infrastructure), software, solutions, and services. Lenovo' s continued investment in world-changing innovation is building a more equitable, trustworthy, and smarter future for everyone, everywhere. Lenovo is listed on the Hong Kong stock exchange under Lenovo Group Limited (HKSE: 992) (ADR: LNVGY).

To find out more visit https://www.lenovo.com, and read about the latest news via our StoryHub.

Lenovo and SentinelOne Alliance

Lenovo' s strategic alliance with SentinelOne ensures that customers can have security from the component level all the way to the cloud. In addition to bringing leading devices to customers, Lenovo delivers expertise in security below the operating system. As a leading security company from the operating system to the cloud, SentinelOne perfectly complements the Lenovo portfolio with its AI-driven platform.

Lenovo ThinkShield is Lenovo' s comprehensive cybersecurity solution portfolio that encompasses hardware, software, and services.

Visit Lenovo ThinkShield

Lenovo
ThinkShield

Smarter
technology
for all

Lenovo

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC

IDC Middle East/Africa

Level 15, Thuraya Tower 1
Dubai Media City
P.O. Box 500615
Dubai, United Arab Emirates
+971.4.3912741
www.idc.com

#META53614125