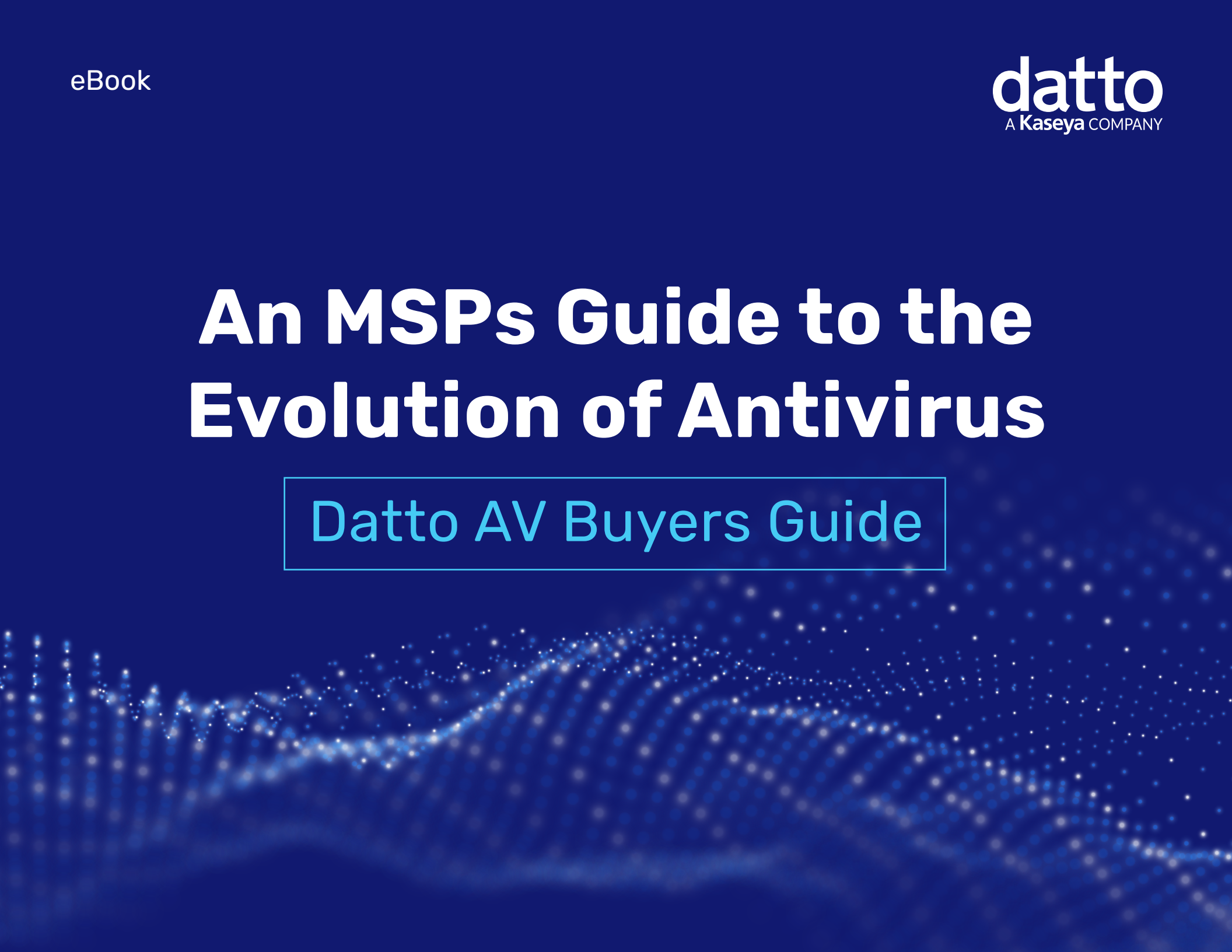
eBook

datto
A Kaseya COMPANY

An MSPs Guide to the Evolution of Antivirus

Datto AV Buyers Guide



Introduction

In the realm of cybersecurity, malicious actors pose a persistent challenge for managed service providers (MSPs) and the customers they serve. The advent of generative AI has enabled cybercriminals to quickly craft and deploy more malware than ever before at scale.

This eBook focuses on the critical role antivirus (AV) plays in helping MSPs protect endpoints and strengthen their customers' first line of defense against rapidly evolving cybersecurity threats. Exploring the current threat landscape that businesses face, and learning more about how advances in technology have launched a new generation of AV solutions, can give MSPs insights into choosing the right AV solution for their customers and their business.

The escalating threat landscape

Every day, MSPs grapple with the threat posed by malware to their customers. Unfortunately, the rise of generative AI has enabled bad actors to create new malware at a rate not seen before.

To understand the gravity of the situation, consider the following statistics:

Statistic	Implication
75% of security professionals report a surge in attacks that most feel can be attributed to the rise of generative AI.	Reflects the escalating intensity of cyberthreats in the past year, necessitating enhanced cybersecurity measures. Generative AI has helped escalate the pace, severity and sophistication of cyberthreats, necessitating investment in cybersecurity solutions that can handle the complexity and intensity of those threats.
In 2007, over 8 million types of malware were in existence, which has exponentially increased to over 1 billion in 2024.	New malware is created daily, so MSPs must help their clients protect their endpoints with an AV solution that can protect against known threats and new and unknown malware.
60% of small businesses face closure after a successful cyberattack.	Underscores the severe consequences businesses may endure, emphasizing the critical role of cybersecurity in overall business resilience. With the right security buildout, MSPs can help their customers avoid the dire consequences that businesses face in the wake of a successful cyberattack.

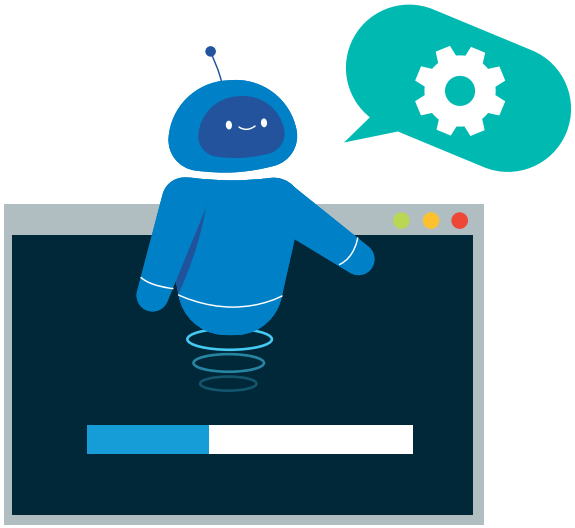
Signature-based antivirus solutions don’t do enough

Historically, IT professionals have relied on the signature-based models used by traditional AV solutions to mitigate virus risk. This conventional approach, rooted in identifying known threats through established signatures, now faces substantial shortcomings as the threat landscape undergoes exponential growth, with new dangers emerging every day.

A historical signature-based model

- Limited to detecting only known threats
- Requires tech time to update and adjust
- Can’t keep up with the pace of constantly emerging threats

However, it is easy to see that traditional AV solutions fall short in today’s fast-moving cybersecurity landscape, especially when addressing the increased intricacies of modern cyberthreats. That’s why MSPs and other IT professionals have increasingly gravitated toward next-gen AV solutions.



The new standard, next-generation antivirus

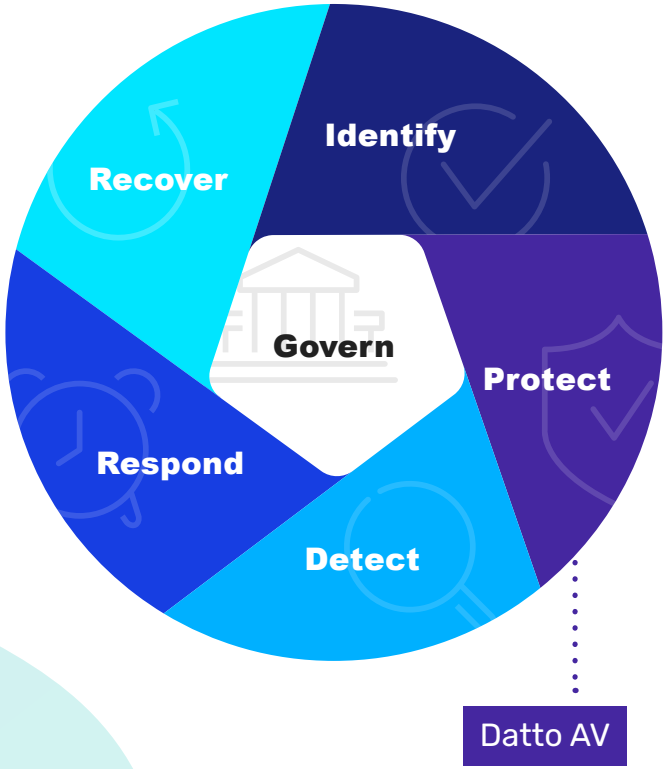
Next-gen AV solutions are designed to transcend the constraints of traditional signature-only-based protection methods, offering a more comprehensive protection against both known and unknown threats.

- Utilizes AI, machine learning and heuristic analysis to maximize performance and minimize maintenance.
- Can effectively defend against both known and unknown threats.
- Is future-ready and affordable for both MSPs and their customers.

Next-gen AI offers MSPs and their customers an array of benefits, including powerful real-time protection from known threats while stopping unknown threats proactively.

Distinctions between signature-based and next-gen antivirus technologies

Capabilities	Signature-Based AV	Next-Generation AV
Signature-based detection	✓	✓
Protection against known threats	✓	✓
Can be updated when new threats are discovered	✓	✓
Real-time protection	✓	✓
Scans on a schedule you determine	✓	✓
AI-based detection	✗	✓
Machine learning	✗	✓
Heuristic analysis	✗	✓
Protects against zero-day threats	✗	✓
Cloud-based, real-time updates	✗	✓
Allows for deep integration and data feeds	✗	✓



NIST Cybersecurity Framework Protection in Depth

The NIST framework consists of five key areas representing the cybersecurity risk lifecycle:

Identify: Understanding and managing cybersecurity risks to systems, assets, data, and capabilities.

Protect: Implementing safeguards to ensure the delivery of critical infrastructure services.

Detect: Developing and implementing activities to identify the occurrence of cybersecurity events.

Respond: Taking action regarding a detected cybersecurity event to mitigate its impact.

Recover: Planning for resilience and restoring any capabilities or services impaired during a cybersecurity event.

NIST emphasizes the importance of a multilayered cybersecurity strategy. Datto AV and antivirus software align with the Protect category, providing a foundational layer within the NIST framework. Datto AV offers robust protection against zero-day attacks, malware, potentially unwanted applications (PUAs), scripts, and more, ensuring comprehensive security coverage.

Core antivirus features to consider

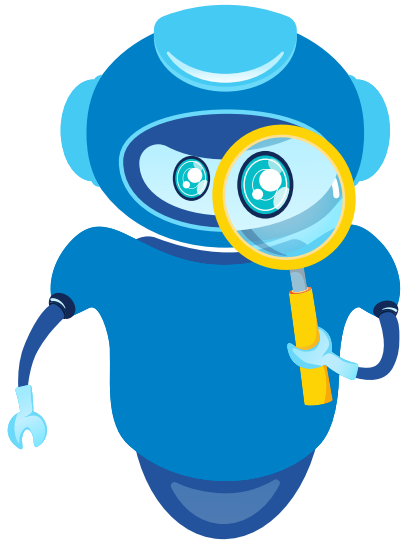
Feature	Why it matters	What to look for
Real-time protection	Real-time protection is like having a vigilant guard standing watch over your digital assets. It ensures immediate detection and response to any malicious activity, safeguarding your systems and data from potential threats.	Seek antivirus solutions that offer robust real-time protection capabilities, capable of proactively identifying and blocking threats in real-time without impacting system performance.
Malware detection and removal	The core function of any antivirus solution is to detect and remove malware from a system or network. Effective malware detection and removal capabilities are critical for maintaining a secure environment and preventing potential data breaches or system compromises.	Look for smart antivirus software with advanced malware detection techniques that make the most of machine learning, heuristic analysis and AI. Ensure that the antivirus can effectively identify and remove both known and emerging malware threats.
Updates and database maintenance.	Cyberthreats are constantly evolving, with new malware variants and vulnerabilities emerging regularly. Regular updates and database maintenance are needed to keep your antivirus software equipped to detect and mitigate the latest threats effectively.	Prioritize antivirus solutions that offer frequent updates and timely database maintenance. Look for features such as automatic updates and cloud-based threat intelligence to ensure that your antivirus stays up to date with the latest malware signatures and security patches without a technician's intervention.

Purchasing considerations beyond protection

For MSPs, selecting the right AV solution involves balancing security features with ease of use, performance, and cost. Key considerations include integration with existing security tools for unified alerts and improved threat management.

Features to look for:

- **Customizable scanning:** Allows tailored security checks and comprehensive scans as needed.
- **Anti-tamper technology:** Prevents malware from disabling or altering the antivirus.
- **Lightweight agent and seamless, quick deployment:** Ensures minimal CPU impact and high user satisfaction.
- **Mark content non-malicious:** Reduces false positives by allowing admins to whitelist content.
- **Affordable price point:** Offers comprehensive protection at a cost-effective price for your profitability
- **Deep integrations:** Reduces tech time and simplifies cybersecurity management through integration with existing tools.



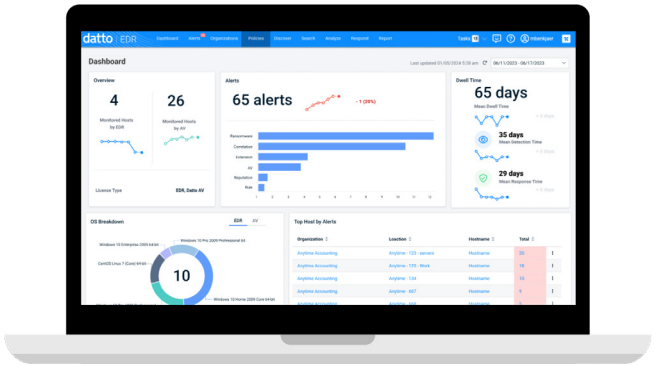
Datto AV – Next-generation antivirus protection for MSPs

Tailored for today's MSP, Datto AV is an affordable, easy-to-use, manage-and-deploy antivirus solution powered by a next-generation engine to protect against today's advanced threats. Datto AV provides top value for MSPs that want the latest antivirus protection while providing unparalleled integration with Datto EDR and Kaseya's IT Complete platform.

Benefits of the Datto AV Solution

- **Next-generation antivirus engine:** Available today and built for tomorrow's threats, Datto AV's next-generation antivirus engine protects against known and unknown threats. Boasting a lightweight AI engine, machine learning and heuristic analysis, Datto AV offers thick, powerful layers of protection.
- **Real-time advanced protection:** Cyberthreats are multiplying daily. With Datto AV, you get automatic quarantine and remediation with the ability to protect against zero-day attacks, malware, potentially unwanted applications (PUA) and scripts — all with minimal user intervention.

- **Anti-tampering technology:** Datto AV employs anti-tamper technology to safeguard against unauthorized modifications to its processes, registry keys and files. Our specialized protection drivers further reinforce this defense, permitting access to Datto AV's components only for verified, trusted applications.
- **Cloud security connection for global intelligence:** All endpoints equipped with Datto AV maintain a seamless connection to a cloud-based infrastructure, ensuring consistent updates with real-time global threat intelligence. This process is designed to be non-disruptive to performance, providing up-to-date protection without impacting system efficiency.
- **AMSI integration for script-based threats:** Seamlessly integrates with applications supporting the Antimalware Scan Interface (AMSI) to protect against dynamic script-based malware, including Microsoft Office VBA macros, PowerShell, JavaScript and VBScript.
- **Minimal impact on system resources:** Optimized for high-performance protection with a small memory footprint, using less than 1GB of disk space, keeping users protected without sacrificing performance.



Delivering the powerful combination of AV and EDR

Many MSPs' customers need the endpoint protection of both an AV and an endpoint detection and response (EDR) software. Datto AV was built to integrate seamlessly with Datto EDR to empower MSPs to manage both easily via the same interface. For MSPs that want a multi-layered security posture using both Datto AV and EDR gives benefits over using an AV and EDR from two different vendors such as:

- Seamless integration for simplicity and ease of use
- Streamlined management through a unified interface
- Enhanced analytics for greater visibility
- Cost effectiveness and value

Connect with us

To request a demo visit