

Why Are You Still Paying for Antivirus?



Executive Summary

The front lines of the cyber war have moved away from the perimeter and onto the endpoint. End user desktops and laptops are under fire from two types of security issues: **nuisance malware and advanced threats**.

Nuisance malware can damage productivity and consume IT time, but advanced threats can cripple a company. As advanced attacks increase in both sophistication and quantity, the potential risk and damage they pose to organizations has increased exponentially. While antivirus (AV) serves a role in mitigating nuisance malware, it does not stop advanced threats and it should not be a top endpoint security investment in 2015.

Organizations should minimize AV investments and reinvest those savings into next generation advanced endpoint threat protection solutions. Organizations that fail to shift endpoint security investments toward advanced threat security are alarmingly vulnerable to advanced attacks and the millions of dollars of damage they bring.

How can a security team get the benefits of both AV and an advanced endpoint security solution without paying for both?

The path taken by many companies who have invested in advanced endpoint security is to adopt Microsoft System Center Endpoint Protection as their AV solution for little or no cost, and shift their savings to best-of-breed endpoint threat prevention solutions such as Bit9 + Carbon Black. **In fact, over a third of enterprises are now considering adopting Microsoft System Center Endpoint Protection as their AV solution.**

Protecting over 100 million endpoints, Microsoft is the market share leader in the antivirus market with over 25% of the market. Bit9 + Carbon Black is the industry leader in advanced endpoint threat protection with over 1,000 deployments, including 25 of the Fortune 100.

Together, Microsoft and Bit9 + Carbon Black provide an industry-leading and cost effective endpoint security solution to stop both nuisance malware and advanced attacks.

Arm Your Endpoints.

Why are you still paying for antivirus?

The front lines of the cyber war have moved away from the perimeter and onto the endpoint. End user desktops and laptops are under fire from two types of security issues: nuisance malware and advanced threats.

You need to stop both, but as advanced attacks increase in both strength and volume, the traditional approach to endpoint security of relying on signature-based anti-virus software needs to be reexamined in terms of antivirus' decreasing efficacy and diminishing return on investment.

Simply put, many security teams are asking, **"Why am I still paying for AV?"**

Type 1: Nuisance Malware:

Widely distributed and opportunistic in nature, these attacks are often not overly damaging but can cause annoyance, affect system performance, and consume valuable IT time. Common examples include spyware, adware and ransomware.

Type 2: Advanced Threats:

Highly sophisticated attacks designed to control or destroy an infected system with the goal of stealing economic or strategically important information. Purpose-built to evade antivirus detection, this type of malware is typically undetected for months or even years resulting in millions of dollars in damage. Well known examples include Stuxnet, Backoff, Flame, Gauss and Reign.

The problem: endpoints only protected by AV are defenseless against advanced attacks.

120M+

the number of malware variants produced annually.
— 2014, Kaspersky Lab

\$5.9M

the average cost of a data breach in 2013.
— Ponemon Institute,
2014 Cost of a Data Breach Study

0

number of antivirus solutions that stopped the Flame advanced malware variant.
— 2012, Wired Magazine

"Reactive approaches are ineffective against advanced attacks"¹

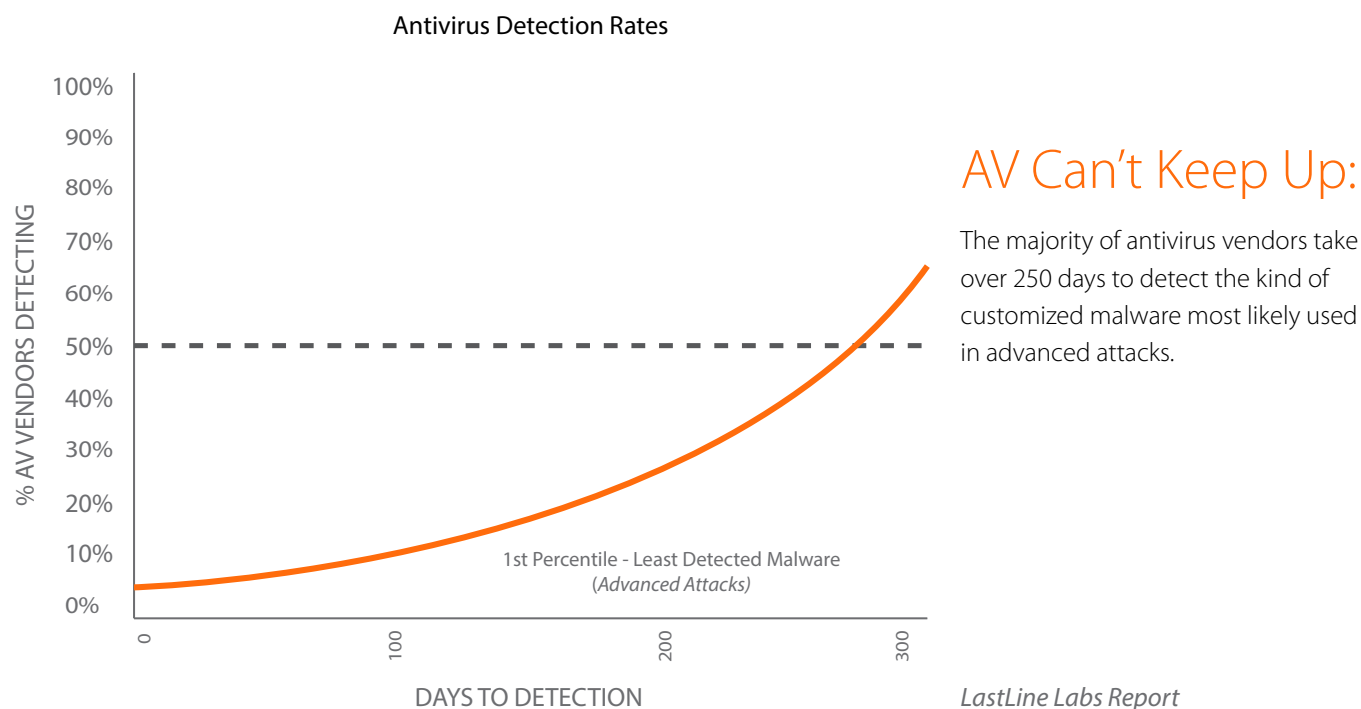
— Gartner

| | Nuisance Malware | Advanced Threats |
|------------------------|---------------------------|-------------------------------------|
| Scope | Broad and General | Narrow and Focused |
| Presence | Noisy | Quiet and Stealthy |
| Mode of Operation | Automated | Human Operated |
| Damage | User Impact | Corporate Impact |
| Detection & Prevention | Signature Protection | Requires a New Approach |
| Answer | Signature-Based Antivirus | Next-Generation Endpoint Protection |

¹ Gartner, "How to Successfully Deploy Application Control," Neil MacDonald, January 25, 2013

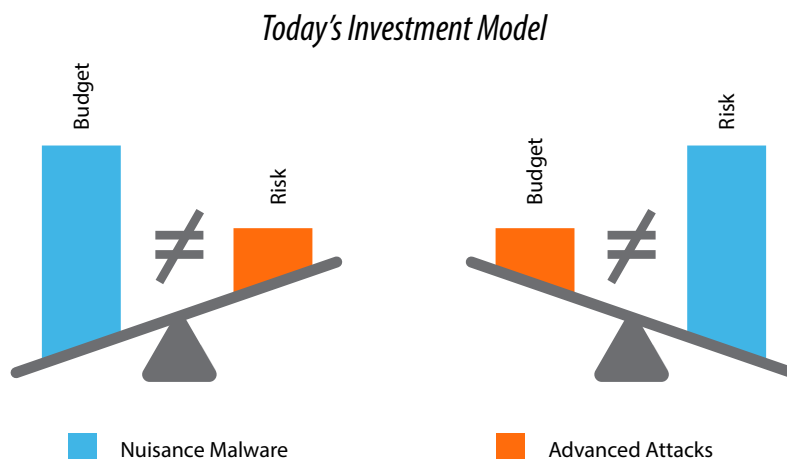
With more than 90% of corporate devices running antivirus software, it is by far the most widely deployed endpoint protection solution. While useful at stopping nuisance malware, antivirus is powerless against today's company-crippling advanced threats. The result is a huge gap in endpoint protection that has resulted in a wide range of advanced attacks against both large enterprises and SMB companies alike costing billions of dollars. Clearly the traditional approach to endpoint protection will not close the gap.

No matter how much organizations spend on traditional AV, the best signature-based cyber defenses will always fail to stop today's latest advanced attack.



Endpoint Investments Today

In 2013, cash-strapped IT organizations spent more than \$2.5 billion on antivirus software and less than \$1B on advanced endpoint threat protection. This investment model is upside down.



Endpoint Investments Tomorrow

To properly ensure the protection of corporate and customer data, organizations need to prioritize investment spending on solutions that address the strategic and economic risks of today's advanced attacks.

As advanced attacks grow to be the biggest financial threat to organizations' cyber security, it follows that advanced solutions should make up the majority of an organization's endpoint security budget. The market is catching on and Forrester predicts that the investment pendulum will switch in 2015 with adoption of proactive security tools designed to stop advanced threats outpacing signature-based anti-malware in 2015².

While some have gone so far to call "AV-dead"³, this is an incomplete view that fails to consider the role that antivirus can play in mitigating nuisance malware. But while AV isn't dead, it should not be a top endpoint security investment in 2015.

With rising threats and IT Security budgets expected to increase less than 9% in 2015, many organizations are forced to choose between investing in advanced endpoint threat protection solutions or continuing to pay for traditional AV solutions. This poses a major dilemma: how can an organization take the necessary steps to protect themselves from advanced attacks without paying for both AV and a next-generation endpoint protection solution?

Nuisance Malware Protection with the Right ROI

Microsoft System Center Endpoint Protection

Companies around the world have already done the math and are planning changes to their endpoint investments. In fact, 51% of organizations plan to replace their existing endpoint solutions in 2015 and most are switching to Microsoft's System Center Endpoint Protection, the clear leader.

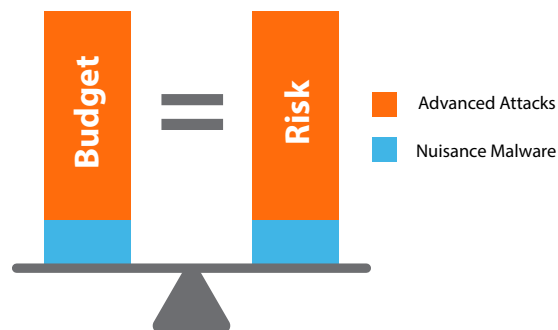
Microsoft System Center Endpoint Protection is an enterprise quality antivirus solution that provides solid nuisance malware protection at little or no cost. For organizations with a Microsoft enterprise license agreement (ELA), adopting SCEP can be a easy way to save money and further extend the value of existing ELA investments.

Are you getting the most out of your ELA?

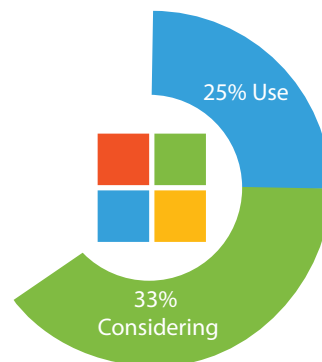
Protecting over 100 million endpoints⁴ and currently being considered by a third of all enterprises as a replacement to their existing AV solution, Microsoft is the market share leader in the antivirus market with over 25% of the market⁵. **If you're not looking at SCEP, you're missing an opportunity to improve your endpoint security while maximizing your ROI.**

Hundreds of leading organizations have already made the switch and are putting those AV dollars to work against advanced threats by investing in next-generation endpoint threat prevention, detection, and response solutions.

Tomorrow's Investment Model



"Approximately one-third of enterprise buyers have indicated that they are actively considering Microsoft"



² Forrester, [The State of Endpoint Security Adoption 2014 to 2015](#)

³ 2014, [Wall Street Journal](#)

⁴ 2014, [Edgile, System Center Endpoint Protection 2012 R2](#)

⁵ 2014, [Opswat, Market Share Analysis of Antivirus & Operation Systems, October 2014](#)

Advanced Threat Prevention, Detection, and Response

Bit9 + Carbon Black

Designed specifically to evade signature-based detection solutions, be they on or off network, advanced attacks represent a serious threat to the financial health and stability of any organization and are estimated to cost the global economy hundreds of billions of dollars each year⁶.

To stop the bleeding, you need broader protection on the endpoint and should adopt solutions that provide real time visibility and proactive detection, response, and prevention.

The Bit9 + Carbon Black solution consists of two industry-leading products and the threat intelligence cloud. Independently, each product is a leader in its category. When used together, their integrated capabilities provide unmatched endpoint threat prevention, detection, and response.

Bit9 + CARBON BLACK

“Adoption of proactive security tools will outpace signature-based anti-malware in 2015.”⁷

- Forrester

Why these capabilities are critical for advanced attacks:

| Challenge | | Solution |
|---|---|-----------------------------------|
| You're blind on your endpoints | Most malware does its damage within minutes and then morphs or deletes itself. Scans and snapshots aren't good enough. You need to know what's resident and running right now | Real-Time Visibility |
| You can't know what's bad ahead of time | You need to see and record everything, and use big data analytics combined with a threat intelligence to look for the indicators of advanced threats. | Rapid Detection |
| Incident response is too slow and expensive | You need to be able to instantly see the “kill chain” for any attack: where it started, what it did, where it is now, and what you should do about it. And once you have clearly identified the attack, you need to immediately contain and control it by blocking its execution on every computer at once. | Continuous Response |
| Traditional endpoint security doesn't stop advanced attacks | You need a proactive endpoint prevention solution that provides multiple forms of prevention to stop advanced attacks from infiltrating your organization. | Advanced Threat Prevention |
| Your network security doesn't integrate with your endpoint security. | When under attack, you need real time context and understanding. You need to be able to immediately correlate network alerts with endpoint data to know where the malware landed, what it did, how severe the threat is—and immediately stop it from executing. | Open API Integration |

⁶ 2014, Forrester, The State of Endpoint Security Adoption 2014 to 2015

⁷ 2014, National Association of Corporate Directors, Cyber-Risk Oversight Summary

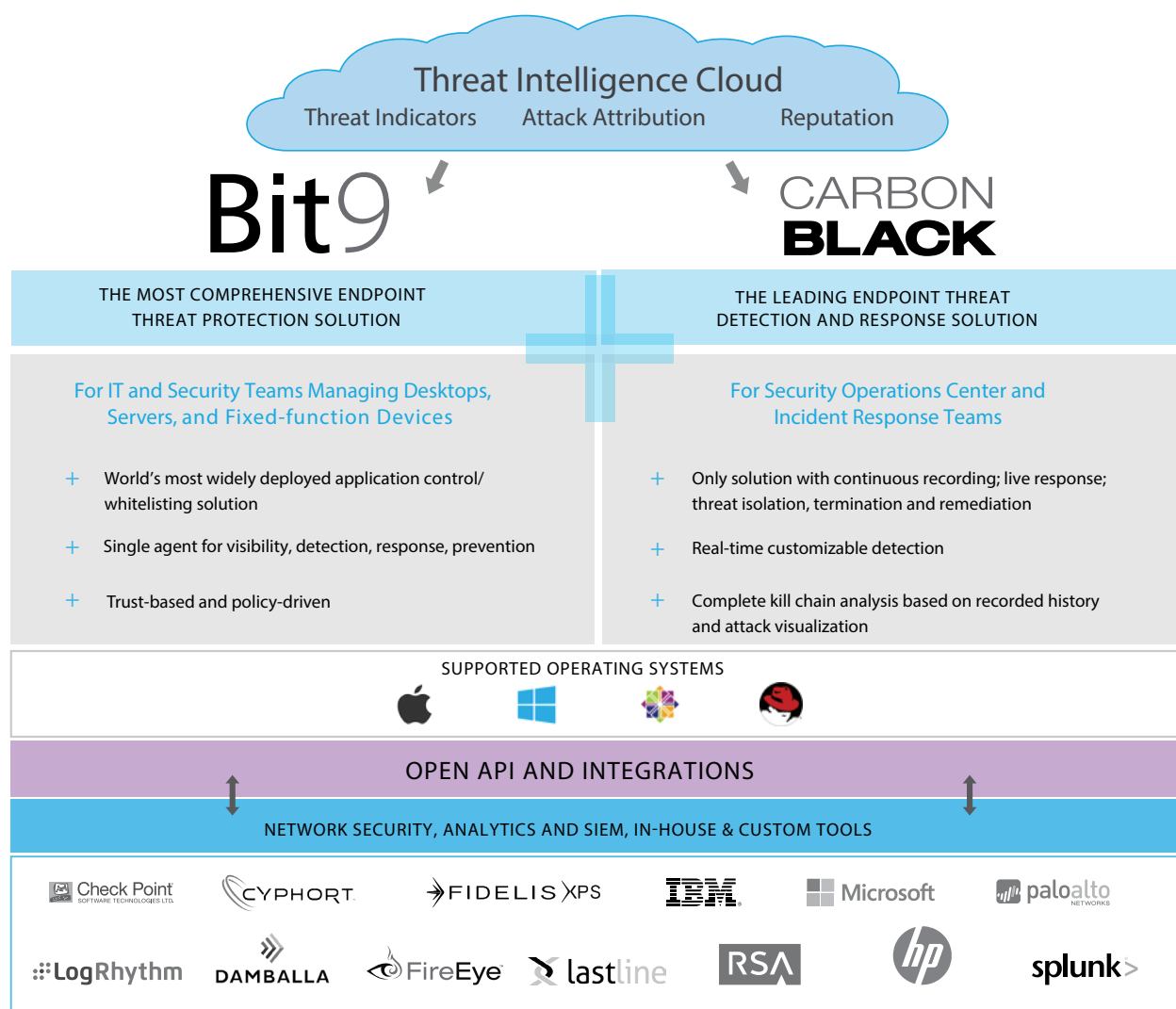
Bit9 Security Platform: Advanced Threat Prevention

The Bit9 Security Platform is the most comprehensive endpoint threat protection solution. By continuously monitoring and recording all endpoint activity, Bit9 can prevent, detect and respond to cyber threats that evade traditional security defenses. Bit9's real-time visibility, cloud-driven reputation, advanced threat indicators, and real-time enforcement engine provide organizations with immediate visibility and granular control over all endpoint activity. This allows Bit9 to deliver real-time signature-less detection of and protection against advanced threats.

Carbon Black: Incident Response in Seconds

Carbon Black is the industry's leading endpoint threat detection and response solution for SOC and IR teams. Carbon Black reduces the cost and complexity of traditional incident response by replacing "after-the-fact" manual data acquisition with continuous monitoring and recording of all activity on endpoints and servers. The powerful combination of Carbon Black's endpoint visibility with the Bit9 + Carbon Black Threat Intelligence Cloud enables organizations to prepare for a breach proactively hunt for threats, customize their detection, and respond in seconds. Top IR firms and MSSPs have made Carbon Black a core component of their detection and response services.


Together, Bit9 + Carbon Black provide organizations with the industry's most advanced endpoint threat prevention, detection, and response solution.



Conclusion

For better or worse, the choices enterprises make in 2015 around endpoint security will have a defining and lasting impact on the security and financial health of their organizations.

The combination of Microsoft SCEP and Bit9 + Carbon Black allows organizations to shift their endpoint security investments to where it is needed most – against advanced attacks – while maintaining a line of defense against nuisance malware.

| | Nuisance Malware | Advanced Threats |
|------------------------|---|-------------------------|
| Scope | Broad and General | Narrow and Focused |
| Presence | Noisy | Quiet and Stealthy |
| Mode of Operation | Automated | Human Operated |
| Damage | User Impact | Corporate Impact |
| Detection & Prevention | Signature Protection | Requires a New Approach |
| Answer |  Microsoft | Bit9+ CARBON BLACK |

Enterprises that move quickly to free up existing budget, by adopting Microsoft System Center Endpoint Protection and deploy next-generation solutions, such as Bit9 + Carbon Black, that prioritize real-time visibility, prevention, detection and response will be in the greatest positions to lead their industry's into 2016.

For more information on Bit9 + Carbon Black's comprehensive portfolio of advanced endpoint threat protection solutions, please visit www.bit9.com

For more information on Microsoft System Center Endpoint Protection, please visit www.microsoft.com

ABOUT BIT9 + CARBON BLACK

Bit9 + Carbon Black offers the most complete solution against the advanced threats that target your organization's endpoints and servers. This makes it easier for you to see—and immediately stop—those threats.

Carbon Black's lightweight endpoint sensor, which can be rapidly deployed with no configuration to enable detection and response in seconds, combined with Bit9's industry-leading prevention technology, delivers four key benefits:

- + Continuous, real-time visibility into what's happening on every computer
- + Real-time threat detection, without relying on signatures
- + Instant response by seeing the full "kill chain" of any attack
- + Prevention that is proactive and customizable

More than 1,000 organizations worldwide—from 25 Fortune 100 companies to small enterprises—use Bit9 + Carbon Black to increase security, reduce operational costs and improve compliance. Leading managed security service providers (MSSP) and incident response (IR) companies have made Bit9 + Carbon Black a core component of their detection and response services. With Bit9 + Carbon Black, you can arm your endpoints against advanced threats.

Bit9+ CARBON BLACK

266 Second Avenue
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com