Traditional AV vs. Next-Generation Attacks

How Antivirus Leaves Businesses Exposed

Both traditional antivirus and next-generation antivirus are designed to block file-based malware. They work by scanning files on disk and quarantining malicious executables. Today, most attacks have evolved to bypass antivirus protection through new, fileless delivery techniques. Exploits, scripts, and macros are some of the vectors hackers use to execute malicious payloads undetected. In fact, 70% of infections detected used powershell scripts (Wired). With antivirus protection alone, businesses are at high-risk of infection.

The Hacker News

Millions hit with banking malware using new Microsoft Word zero day

79%

of companies have had an attack get by their antivirus

— Barkly

SC

Japanese Honda factory hit with WannaCry ransomware, halts production

NBC NEWS

Three U.S. Hospitals Hit in String of Ransomware Attacks

How Barkly Replaces Antivirus and Blocks Modern Attacks

Barkly's Endpoint Protection Platform™ delivers the strongest protection against file-based malware, fileless attacks, and exploits. Barkly doesn't scan files or look at signatures. Our patented agent, Rapidvisor, watches processes across multiple-layers of the system, and detects attacks through a combination of machine-learning attribute analysis and real-time behavior analysis. Barkly can identify and block attacks whether they are known or unknown, file-based or fileless.

Comparison of Endpoint Protection Options

	TRADITIONAL ANTIVIRUS	NEXT-GEN ANTIVIRUS	BARKLY ENDPOINT PROTECTION
PROTECTION TECHNIQUE	Signature-matching	Machine learning analysis	Machine learning analysis + behavior analysis
KNOWN FILE-BASED MALWARE	✓	✓	✓
UNKNOWN FILE-BASED MALWARE		✓	✓
SCRIPT-BASED MALWARE			✓
MACRO MALWARE			✓
EXPLOITS			✓

Barkly

Contact us: **info@barkly.com 617.275.2074** |

Traditional AV vs. Next-Generation Attacks

"Traditional endpoint protection platforms that rely solely on signature-based malware detection are not completely effective when it comes to repacked or new malware until new signatures are distributed. A response lag opens opportunities for attackers to target organizations that are essentially unprotected until all their endpoints are updated with the latest signature."

— Gartner, The Real Value of a Non-Signature-Based Anti-Malware Solution to Your Organization, September 2016

Barkly delivers the strongest protection with the simplest management.

Multi-layered protection

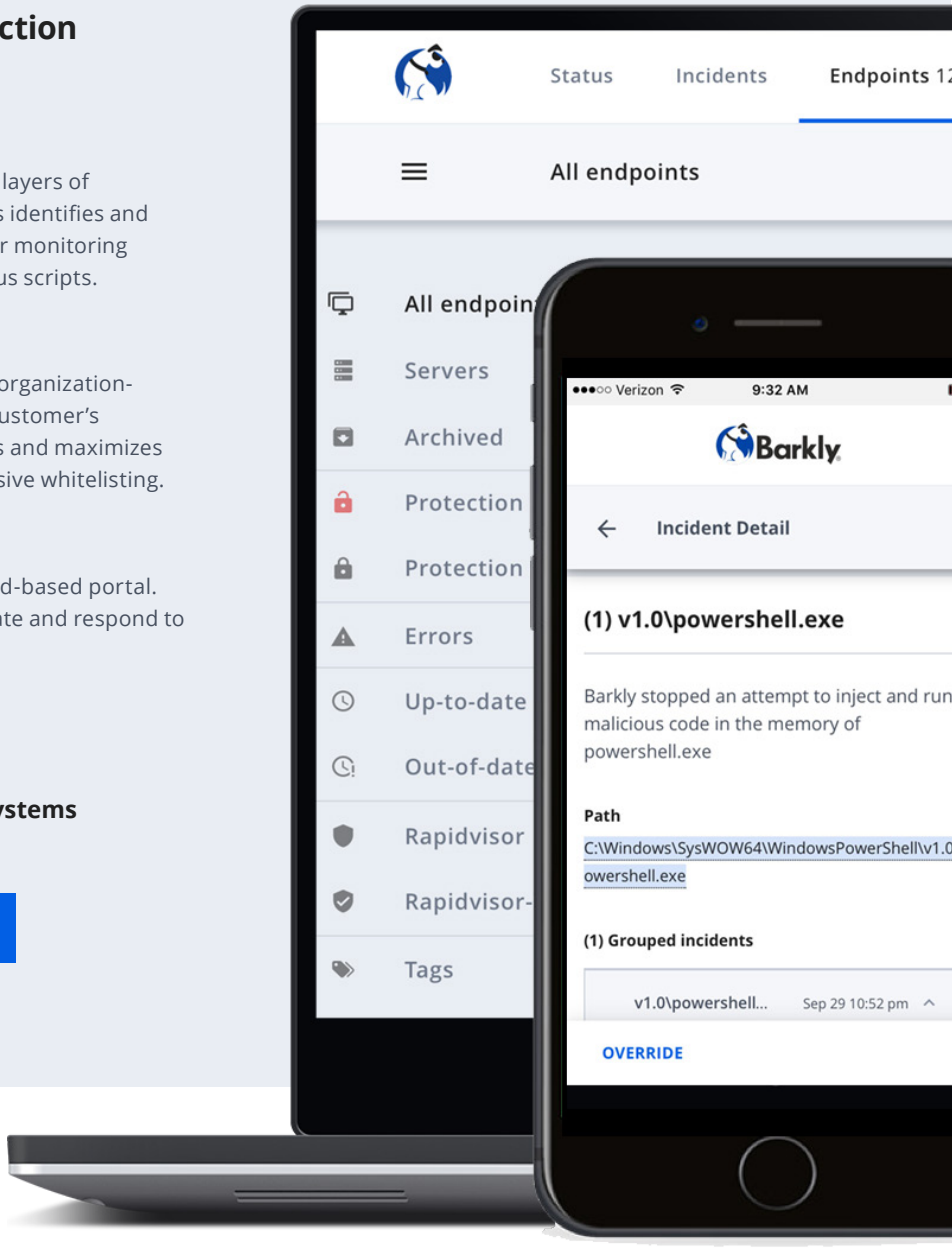
Barkly blocks attacks at every turn with two powerful layers of protection. Machine-learning driven attribute analysis identifies and blocks malicious executables, while real-time behavior monitoring protects against exploits, fileless attacks, and malicious scripts.

Low noise

Barkly uses Responsive Machine Learning to develop organization-specific protection models that are tailored for each customer's unique software profile. This minimizes false positives and maximizes protection for your business, without requiring extensive whitelisting.

Mobile-friendly management

Barkly is easy to deploy and manage through our cloud-based portal. It's mobile friendly, so you can get alerts and investigate and respond to incidents on the go.



Barkly supports Windows 7, 8, and 10 64-bit systems and Windows 8, 12, and 16 servers.

Don't wait — get a quote or demo today.

Barkly

Contact us: **info@barkly.com 617.275.2074** |