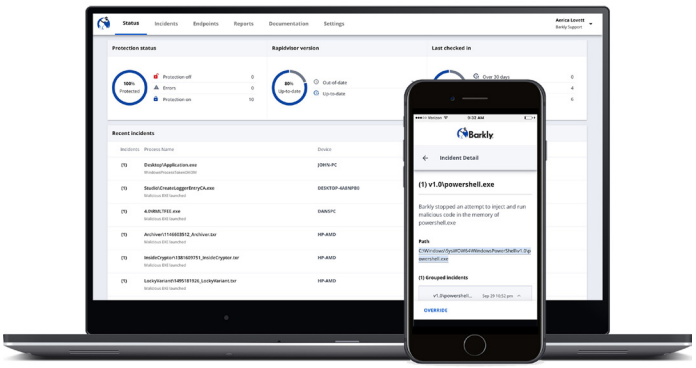

DETAILS

Vendor Barkly

Price Pricing starts at $45 per endpoint per year (for a minimum of 50 endpoints).

Contact barkly.com

Features	★★★★
Documentation	★★★★
Value for money	★★★★½
Performance	★★★★★
Support	★★★★¾
Ease of use	★★★★★

OVERALL RATING ★★★★½

Strengths Ease-of-use and low resource requirements.

Weaknesses Number of features and limited documentation.

Verdict Catering to no-frills, quick implementation expectations, this solution also delivers a modern approach with their instant-chat support available with one click.

www.barkly.com
info@barkly.com

Barkly

Barkly Endpoint Protection Platform

Barkly is an endpoint ransomware solution that recognizes attacks and blocks malicious techniques such as exploits, malicious scripts and executable malware and malicious intents. Credential theft, privilege escalation, and ransomware are all recognized through Barkly's techniques with a combination of attribute- and behavior- analysis, preventing infections before they do harm.

Our initial inspection focused on the merits of Barkly's primary line of defense, the Rapidvisor agent. This is a lightweight hypervisor-based agent with a comprehensive view of user processes, operating system functions, and real time CPU-level processing. Rapidvisor is branded to block exploits from both file-less and file-based attacks.

We did note that Rapidvisor is utilized in a native fashion when you are installing Barkly on both physical or VDI machines. This provision comes by way of a VT-mode that uses built-in virtualization extensions to run a hypervisor, such as Microsoft's Hyper-V or VMware's ESXi. With VT-mode turned off, the resulting functionality is relatively similar with Rapidvisor monitoring processes at the CPU level of the system. Barkly states that enabled VT-mode allows Barkly to provide additional exploit protection. This means Barkly can identify and block some attacks sooner, at the exploit stage, before malicious executables are present on the system.

Installing Barkly on a few endpoints might be useful from the management console, but in larger organizations, Barkly supports deployment tools such as Microsoft's SCCM and group policy using an .msi that can be extracted from the execution file.

We found Barkly's setup to be a simple, hassle-free process. Upon logging into their cloud management console management console, we navigated to their Endpoints tab and clicked on the add endpoints button to download the installer. Once the installer initiates, we were only prompted with user account control (UAC) permissions; then in an instant, Barkly was nestled in the background running silently, hidden from the user. The end user would only know Barkly was on their system if it stopped something malicious.

Barkly's management console is strikingly simplistic while being extremely functional. The console presents you with six tabs but there are four tabs where you will likely prioritize your time: Status Incidents, Devices, Reports. Each of these function sets gives you enough detail for the job without superfluous information. We especially liked the convenience of the ability to manage Barkly from your mobile device by simply navigating to the Barkly portal.

One unique feature that Barkly stands out in their support is its instant messenger style chat support. Its bright blue and white chat icon can be found on the bottom right-hand corner of every single page in the management console. When testing Barkly, we utilized this support feature in several instances and response time was within a few minutes. The support agents seemed knowledgeable and were able to help us resolves our inquiries. The best part of this on-demand support is that you do not need to submit a support ticket. You can even ask the support agent to speak to them via phone.

– Matt Hreben with collaboration from Dan Cure; tested by Matt Hreben