Carbon Black.

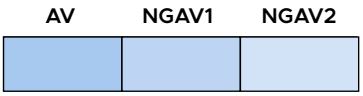
Is It Time To Replace Your Antivirus?

Your traditional endpoint security is not solving problems for you—it's creating them. 70% of successful breaches begin at the endpoint. One has to ask: if traditional antivirus was doing its job, why are these attacks so successful?

If you want to leave all of your endpoint security problems behind, then you're ready to move from on-premise to the cloud. Here is a handy checklist to use when you are evaluating next-generation antivirus (NGAV) in the cloud and looking for a reliable provider to work with:

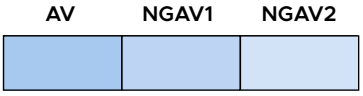
CATEGORY: A SINGLE AUTOMATED CONSOLE FOR EASY, AUTOMATED UPDATES

Why it matters: Threats evolve quickly, and software needs to be updated regularly. The cloud streamlines endpoint security through a single console and automates updates, implementing the latest protection and features as soon as they are released.



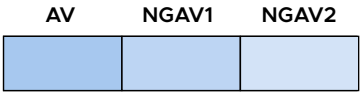
CATEGORY: OPEN APIS FOR THE UTMOST IN SECURITY INTEGRATION

Why it matters: When security solutions operate separately, the complexity creates friction across processes and teams. The cloud lets you take advantage of standardized open APIs that integrate endpoint security with the rest of your defense stack.



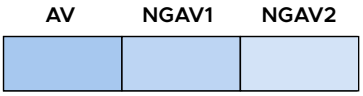
CATEGORY: A SINGLE LIGHTWEIGHT AGENT

Why it matters: When you deploy security solutions with separate agents, you must configure and monitor each one separately. The cloud consolidates disparate solutions easily with multiple security functions on a single agent.



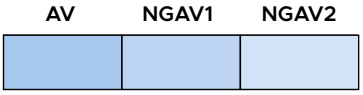
CATEGORY: ENDPOINTS THAT ARE TREATED EQUALLY

Why it matters: Traditional security solutions weren't built to secure endpoints outside the corporate network. With the cloud, all endpoints connect back to the same cloud-based service for configuration and updates, giving them equal protection.



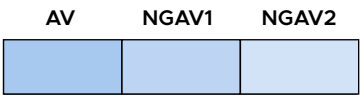
CATEGORY: NO PERFORMANCE IMPACT ON ENDPOINTS

Why it matters: Traditional antivirus scans and other protection modes can be a significant performance drain on endpoints. With the cloud, only one lightweight agent performs all security processes, causing no drain on computing resources.



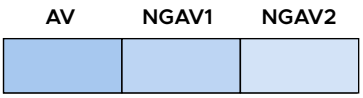
CATEGORY: PREDICTIVE BIG DATA INSIGHTS INTO EMERGING ATTACKS

Why it matters: Traditional antivirus can only stop and prevent known malware, which accounts for a mere 30% of today's attacks. The cloud uses big data and sophisticated analytics to predict new threats and prevent unknown malicious behavior.



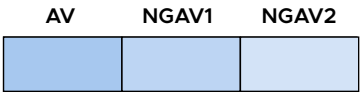
CATEGORY: COMPLETE VISIBILITY INTO ALL ENDPOINT ACTIVITY

Why it matters: Traditional solutions don't have the massive processing power needed to collect and analyze all endpoint activity. The cloud collects unfiltered data and uses streaming analytics to give you real-time visibility into what happened and when.



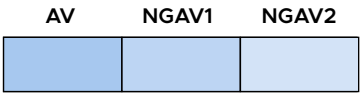
CATEGORY: REAL-TIME RESPONSE AND REMEDIATION

Why it matters: Traditional systems lack built-in tools to address security issues, slowing you down. With the velocity of the cloud, you have the power to identify problems and respond to them in near-real time.



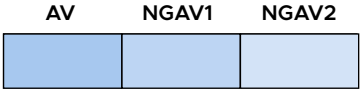
CATEGORY: COLLABORATION AND INSIGHTS FROM GLOBAL SECURITY EXPERTS

Why it matters: Today there are over one million paid cybercriminals behind the incessant attacks organizations face each day. The cloud connects you with thousands of global security experts who share intelligence about emerging threats, in real time.



CATEGORY: SIMPLIFIED IT AND SECURITY OPERATIONS

Why it matters: The management required to keep endpoint security products up to date can be complex and costly. The cloud gives you the benefit of an entire managed operation, with no complex infrastructure. This lets you focus on what matters—security



[1] "Cybercrime: The Credentials Connection," IDC, 2014