Carbon Black.

PROOF OF CONCEPT CHECKLIST

It's Time To Replace Your Antivirus

Your Next-Gen Antivirus (NGAV) Capabilities Checklist

Traditional antivirus (AV) is no longer up to the challenge posed by modern attackers. Signature and heuristic-based antivirus is ineffective against the types of attacks that organizations experience today, which increasingly rely on malware-less techniques that are invisible to AV. The problem is so bad that almost half of organizations have been affected by ransomware in the past 12 months *(Osterman Research)*.

To protect your organization against today's threats, you need an endpoint-security solution that goes beyond malware, incorporating next-generation features that target the tools, techniques, tactics, and procedures used every day by both mass scale opportunistic attackers and targeted advanced threats.

This checklist will help you assess the capabilities of your current antivirus solution and will provide the requirements needed to shift to a next-generation antivirus (NGAV) approach.

CATEGORY: PROTECTION FROM FULL RANGE OF MODERN ATTACKS

Why it matters: Modern attackers generate malware faster than traditional AV stops it. Furthermore, they are mastering techniques that don't even require malware. Your endpoint security solution should protect against all attacks, not just malware-based threats.

Your NGAV solution should:	**AV**	**NGAV 1**	**NGAV 2**
Protect against known malware and variants including malware-based ransomware			
Protect against obfuscated malware, unknown malware, and zero-day attacks			
Protect against malicious scripts that leverage: PowerShell, Visual Basic, Perl, Python, Java/JAR			
Protect against memory-resident attacks and other malware-less attacks			
Protect against document-based attacks (PDFs and macros)			
Protect against remote login attacks and the malicious use of good software			

CATEGORY: EXTENSIBLE CLOUD SECURITY INTELLIGENCE AND ANALYTICS

Why it matters: As attackers evolve and adapt their tactics and techniques, you need to deploy new analytic capabilities and attack intelligence to properly defend yourself – without having to redeploy your security infrastructure.

Your NGAV solution should contain:	**AV**	**NGAV 1**	**NGAV 2**
Cloud-based behavioral detection, machine learning, and reputation/relationship analysis			
Open & extensible threat feeds for third-party attack intelligence			
Configurable detection to prioritize important events and reduce unnecessary alerts			
Community-based threat sharing and collaborative threat discussion forums			

CATEGORY: VISIBILITY AND CONTEXT INTO ATTACK AND DETECTION EVENTS

Why it matters: After an attack attempt, you need to understand what happened so you can contain and control the situation, prevent further damage, and improve your overall security posture. The right context helps you do all that quickly and easily.

Your NGAV solution should:	AV	NGAV 1	NGAV 2
Provide insight into how the threat started, even before it was detected			
Provide visibility into where else in your organization this threat may exist			
Provide guidance on what's needed to recover and how to close security holes			
Share data with third-party systems (SIEM, analytics, workflow, etc)			

CATEGORY: INTEGRATED RAPID-RESPONSE CAPABILITIES

Why it matters: Not every attack can be prevented. Skilled attackers can use stolen credentials and native system tools, such as PowerShell to infiltrate a machine without using any malware. These attacks can still be detected and, when they are, you need to be able to respond quickly.

Your NGAV solution should make it easy to:	AV	NGAV 1	NGAV 2
Delete malware or temporary files across the organization			
Stop network activity for a specific process			
Quarantine a system and isolate it from the network			
Blacklist files from executing anywhere in the environment			

CATEGORY: LIGHTWEIGHT OPERATIONS

Why it matters: We've all experienced antivirus grinding our computer to a halt while it scans the drive. Thankfully, those days are gone. Next-generation antivirus should be lightweight on the system and easy to administer so it doesn't slow you or your users down.

Your NGAV solution should:	AV	NGAV 1	NGAV 2
Deploy to an environment quickly and automatically			
Have no impact to the end-user's productivity or typical user experience			
Exhibit lightweight resource usage on the endpoint			
Provide cross-platform support: Windows & Mac			

CATEGORY: A PLATFORM THAT GROWS WITH YOUR USERS, SYSTEMS, AND TEAMS

Why it matters: You have different assets, and they require different strategies for protection. Servers, for example, don't change often and have highly restrictive protection policies. Meanwhile, your developers need more flexibility. Your solution should adapt to your needs and be part of a platform that provides you with a growth path to a better security posture over time.

Your NGAV solution should be part of a platform that provides:	AV	NGAV 1	NGAV 2
Group-based policy that applies different security strategies to different systems			
Upgrade path to advanced incident response and threat hunting for SOCs and IR teams			
Upgrade path to default-deny and lockdown policies for sensitive or high-risk systems			
Upgrade path to app control, device control, and file integrity monitoring for servers and critical systems			

ABOUT CARBON BLACK

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses.