A Guide to Replacing Legacy Tools with Modernized Endpoint Security

McAfee edition
It’s tough keeping pace with today’s cyberattackers

Cyberattacks are rapidly evolving amid the recent global health crisis. They are getting smarter and coming up with new, sophisticated threats to exploit your distributed workforce. In fact, according to the 2020 Global Threat Report by VMware, 90 percent of security professionals surveyed said the volume of attacks they faced has increased, while 80 percent said attacks became more sophisticated.1

It is more critical than ever that you are protected by the latest innovations in modern endpoint security. And if you’re using legacy endpoint security tools, your risk of experiencing damaging attacks increases exponentially.

Attacks go beyond malware

The fact is that legacy endpoint security tools only help you fight known malware. Cybercriminals are relentlessly creating newer and more advanced malware variants that can infiltrate your applications, services, networks and systems without your knowledge. And it’s not just traditional malware targeting your endpoints. 66 percent of organizations reported being targeted by ransomware during the past year, much of which may have been sold by e-crime groups on the dark web.1

Attackers are finding new entry points

Attackers are also finding new ways to enter your networks. 44 percent of attacks leverage island hopping.2 That means attacks can come through your affiliates or that you could be responsible for entry of an attack on a partner organization.

The growing sophistication of attackers is clear. 82 percent of recently surveyed respondents said they had to report an incident to regulators or engaged an incident response firm to overcome the reputational problems caused by breaches.1

Upgrade easily

You need a way to upgrade your protection without bringing the productivity of your team to a halt. Plus, you need protection that continues to advance along with the capabilities of today’s cyberattackers. VMware Carbon Black Cloud™ is at the forefront of cybersecurity innovation and has a simple way for you to replace legacy endpoint protection. This white paper will help by laying out the steps you can follow to confidently modernize endpoint protection.

Top pain points of legacy endpoint users

Here’s what former McAfee customers told VMware about the pain they were experiencing that caused them to make a switch in endpoint protection:

• **Lack of visibility** – Without the ability to see context around threats or endpoint activity, it is virtually impossible to track threats, find the root cause, and close gaps.

• **Weak protection** – Legacy endpoint tools may only provide basic protection against known malware, leaving users unprotected against advanced threats, such as fileless attacks and ransomware.

• **Expensive to maintain** – With multiple McAfee ePolicy Orchestrator (ePO) servers that don’t work together, there is often a big CapEx outlay required to keep the systems running.

• **Poor performance** – Having multiple agents and out-of-date technology may cause performance issues on the endpoint.

• **Difficult to update** – Keeping current is difficult and resource intensive, which can result in out-of-date technology.

• **Complex to configure** – ePO is very complex and hard to configure, let alone keep in sync, which leaves policies vulnerable to attacker entry.

A Guide to Replacing Legacy Tools with Modernized Endpoint Security

Significant benefits of switching to VMware Carbon Black Cloud
VMware Carbon Black Cloud is a market-leading endpoint protection platform that provides everything you need to secure your endpoints. It consolidates endpoint security, making it easier to prevent, investigate and remediate threats using a single lightweight agent. VMware Carbon Black Cloud delivers superior protection, actionable insights, and simplified operations, making the switch a true upgrade.

Protection from the unknown
VMware Carbon Black Cloud stops both malware and non-malware attacks, protecting users from all forms of attacks. McAfee’s signature-based technology only stops file-based attacks, leaving customers at risk for more advanced breaches.

Easier to manage
VMware Carbon Black Cloud provides everything you need to secure your endpoints from a single lightweight agent, including next-generation antivirus, endpoint detection and response (EDR), and more. The platform has a clean, cloud-based UI, requires no infrastructure to manage, has automated updates, and has simple policies. McAfee requires regular manual updates, which can quickly become out of date, causing performance issues that frustrate end users.

Informed decision-making
VMware Carbon Black Cloud provides actionable insights into emerging threats for real-time investigation and remediation. This gives you the ability to see hard-to-find threats, track the path a threat took, and understand the root cause so you can close security gaps. McAfee users can’t see endpoint activity or the context around threats, leaving them powerless to determine how threats happen.

Create your plan to remove McAfee from the endpoint
The following steps can be taken to upgrade to a modern endpoint protection platform.

Step 1: Determine products to remove
Evaluate your environment to determine which McAfee endpoint security products installed on your endpoints should be removed to upgrade to modern endpoint protection.

Step 2: Understand what will change operationally
Some McAfee products you’ll want to continue to use but manage them differently:
• Firewall and device control – If you use McAfee products to manage personal firewall and device control via the endpoint, you’ll need to change those to manage them via the operating systems. Use Group Policy Objects or Apple management to handle configuration settings.
• Encryption – If you use McAfee products for endpoint encryption, you’ll switch management to run through BitLocker and FileVault.

“I really like the web-based console. The ability to hop on and research an event from anywhere, on any internet-connected device is great.”
RICH PELKIE
HELP DESK ENGINEER
GENTLE GIANT MOVING COMPANY
Step 3: Identify products to keep using (or switch)
For McAfee products that don’t live on the endpoint, you’ll want to evaluate what to keep using or switch. Depending on how you want to handle your McAfee contracts, there may be some products you want to continue to use or take the action to switch them to an alternative available in the market. The typical products considered for keeping or switching are:

- Antivirus for Exchange
- Cloud Security
- Network Security
- SIEM

Step 4: Select capabilities to extend cloud-based endpoint security
When your endpoint security is based in the cloud, it’s easy to add new capabilities that support a growing and maturing security practice. Determine the functionality within VMware Carbon Black Cloud that will add value for your organization:

- Next-generation antivirus and EDR
- Real-time query and remediation
- Managed alert monitoring and triage
- Advanced threat hunting
- Workload security

Power of the platform
VMware Carbon Black Cloud does more than serve as an antivirus replacement. It’s delivered on a cloud native endpoint protection platform that allows for consolidation of multiple security solutions onto a single agent. VMware Carbon Black Cloud removes friction between security and IT teams, arming users with the following key capabilities to keep pace with today’s cyberattackers.

Comprehensive endpoint data
All activity from your endpoints is continuously recorded and centralized to provide the full historical context. In fact, a single endpoint can generate between 10,000 and 40,000 individual events daily. This data should help you identify malicious activity that could lead to a harmful attack.

Behavioral analytics
VMware Carbon Black Cloud focuses on understanding attackers’ behavior patterns, enabling it to detect and stop never-seen-before attacks in real time. Leveraging the power of the cloud, VMware Carbon Black Cloud analyzes more than 500 billion events per day across millions of global endpoints, helping you stay ahead of emerging attacks.

Reduced complexity
Operate faster and more effectively. Deploy with ease, auto-update your defenses, and reduce overhead with no onsite infrastructure to manage. Removing infrastructure management by shifting to the cloud helps you focus on running effective security operations without the complications that come with a self-managed infrastructure.
Your step-by-step guide to upgrading endpoint protection

McAfee users can easily start the process to implement modernized endpoint protection. Implementing VMware Carbon Black Cloud is a seamless process, and many customers that work with the VMware Professional Services team complete their implementation within 10–12 weeks from purchase.

The following steps will help you begin your journey toward speed, clarity and confidence in your endpoint protection. And if you need any help along the way, contact us. VMware regularly helps McAfee users make the switch. Let us help you get the modern protection you need.

Weeks 1–2: Planning
• Build project definition and plan
• Identify McAfee agent(s) to replace
• Test-drive VMware Carbon Black Cloud and learn the console

Weeks 3–4: Installing
• Install the VMware Carbon Black Cloud agent on your endpoints
• Set up policies to allow the system to learn
• Configure prevention and detection to maximize efficacy and minimize false positives

Weeks 5–6: Testing
• Monitor and compare McAfee and the VMware Carbon Black Cloud reports
• Review alerts and begin to group, filter and tune priority
• Refine views and searches for investigations and hunting

Weeks 7–10: Changing over
• Configure OS security controls
• Elevate the VMware Carbon Black Cloud policies on endpoints
• Move McAfee into unmanaged mode
• Uninstall McAfee locally or through remote administration means

Weeks 11–12: Rolling out
• Hold an interactive Q&A session with a real-time example
• Train on best practices
• Review alerts and optimize policies
• Teach the team to investigate and hunt threats