It’s Tough Keeping Pace with Today’s Cyberattackers

Cyberattacks are rapidly evolving. It is more critical than ever that your company be protected by the latest innovations in endpoint security. And if you’re dealing with outdated antivirus solutions, your risk of experiencing damaging attacks is increasing exponentially.

Attacks Go Beyond Malware

The fact is, legacy antivirus only helps you fight known malware, which continues to decrease in volume as a type of attack you will face. A recent survey of IR professionals shows that cyberattackers are utilizing more complex tools to launch more sophisticated attacks.

The growing sophistication of attackers is clear when respondents said that counter-incident response occurred in 51% of attacks last quarter. Furthermore, 72% of IR professionals saw counter IR in the form of destruction logs.

**Attacker Finding New Entry Points**

Attacker are also finding new ways to enter your networks. 50% of attacks are leveraging “island hopping”. That means attacks can come through your affiliates or that you could be responsible for entry of an attack on a partner organization.

And it’s not just traditional endpoints being targeted. Attackers are finding ways to enter via Internet of Things (IoT) devices. In fact, 38% of IR professionals saw attacks directed at enterprise IoT devices for entry and that number is only expected to grow.

**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 with today’s cyberattackers. Carbon Black is at the forefront of cybersecurity innovation and has a simple way for you to replace McAfee endpoint protection with the CB Predictive Security Cloud.

You can get unstuck. This paper will help by laying out the steps you need to take to confidently move “improving endpoint protection” to the top of your to do list.

---

1 Carbon Black Quarterly Incident Response Threat Report
BENEFITS

Significant Benefits of Switching to the CB Predictive Security Cloud

The CB Predictive Security Cloud (PSC) is Carbon Black’s endpoint protection platform (EPP) 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. The PSC delivers superior protection, actionable insights, and simplified operations, making the switch a true upgrade.

1. Protection from the Unknown
   The PSC 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.

2. Easier to Manage
   The PSC provides everything you need to secure your endpoints from a single lightweight agent, including next-generation antivirus, endpoint detection and response, 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.

3. Informed Decision Making
   The PSC 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 that a threat took and understand root cause so that 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.

TOP PAIN POINTS OF MCAFEE USERS

HERE’S WHAT FORMER MCAFEE CUSTOMERS TOLD CARBON BLACK ABOUT THE PAIN THEY WERE EXPERIENCING THAT CAUSED THEM TO MAKE A SWITCH IN ENDPOINT PROTECTION.

POOR PERFORMANCE
Having multiple agents and out-of-date technology causes performance issues on the endpoint.

LACK OF VISIBILITY
Without the ability to see context around threats or endpoint activity, it is virtually impossible to track threats, find root cause and close gaps.

DIFFICULT TO UPDATE
Keeping current is difficult and resource intensive, which results in out-of-date technology.

WEAK PROTECTION
Legacy AV only provides basic protection against known malware, leaving users unprotected against advanced threats like fileless attacks and ransomware.

COMPLEX TO CONFIGURE
ePO is very complex and hard to configure, let alone keep in sync, which leaves policies vulnerable to attacker entry.

EXPENSIVE TO MAINTAIN
With multiple ePO servers that don’t work together, there is a big CapEx outlay to keep running.

LACK OF VISIBILITY
Without the ability to see context around threats or endpoint activity, it is virtually impossible to track threats, find root cause and close gaps.

POOR PERFORMANCE
Having multiple agents and out-of-date technology causes performance issues on the endpoint.

DIFFICULT TO UPDATE
Keeping current is difficult and resource intensive, which results in out-of-date technology.

WEAK PROTECTION
Legacy AV only provides basic protection against known malware, leaving users unprotected against advanced threats like fileless attacks and ransomware.

LACK OF VISIBILITY
Without the ability to see context around threats or endpoint activity, it is virtually impossible to track threats, find root cause and close gaps.

COMPLEX TO CONFIGURE
ePO is very complex and hard to configure, let alone keep in sync, which leaves policies vulnerable to attacker entry.

EXPENSIVE TO MAINTAIN
With multiple ePO servers that don’t work together, there is a big CapEx outlay to keep running.
Create Your Plan to Remove McAfee from the Endpoint

The best way to reduce your payments to McAfee and have a clean upgrade is to remove McAfee completely from the endpoint. This will make a significant reduction in your McAfee contract, allowing you the flexibility to upgrade to a better endpoint security solution.

**Step 1: Determine Products to Remove**
Any McAfee product that sits on the endpoint will need to be removed. Check for the following McAfee products that you may have installed:
- Endpoint Security
- Endpoint Protection
- DLP Endpoint

**Step 2: Understand What Will Change Operationally**
Some McAfee products you’ll want to continue to use, but manage them differently.
- Firewall & 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 & Filevault.

**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 that 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
- 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 the CB Predictive Security Cloud that will add value for your organization:
- Next-generation antivirus + endpoint detection and response
- Real-time query and remediation
- Managed alert monitoring and triage
- Advanced threat hunting
- Virtual datacenter security

With Carbon Black we are able to react to situations in real time. This was very helpful compared to traditional AV such as McAfee, where we wouldn’t be able to identify issues until sometimes a year later. Additionally, CB is much easier to deploy and manage than McAfee.

CHRISTOPHER ST. AMAND
SR. NETWORK SECURITY ENGINEER AT PEOPLE’S BANK
One of our goals was to consolidate our security products. What Carbon Black was able to do was bring multiple systems into one. The fact that it’s keeping up with the latest threats out there really made it a differentiator from the other solutions we looked at.

WILLIAM BOCASH
IT MANAGER, STONEWALL KITCHEN

ENDPOINT PROTECTION PLATFORM

Power of the Platform

The PSC 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. The Predictive Security Cloud brings together the following team of security solutions onto a single platform:

The CB Predictive Security Cloud removes friction between security and IT information, arming users with these key capabilities to keep pace with today’s cyberattackers:

1. Comprehensive Endpoint Data
   All activity from the endpoints is continuously being recorded and centralized to provide the full context.

2. Behavioral Analytics
   The PSC 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, the PSC analyzes more than 500B events per day across millions of global endpoints, helping you stay ahead of emerging attacks.

3. Reduced Complexity
   Operate faster and more effectively. Deploy with ease, auto-update your defenses, and reduce overhead with no onsite infrastructure to manage.
Your Step-By-Step Guide to Upgrading Endpoint Protection

With the rate of advancement of cyberattackers, it is critical for McAfee users to start the process to make the switch. Implementing the PSC will be much easier than what you’ve experienced with McAfee because the PSC uses just a single agent and is in the cloud. In fact, many customers working with Carbon Black Professional Services complete their implementation work within 10-12 weeks from purchase.

Follow the steps below to begin your 3 month journey toward speed, clarity and confidence in your endpoint protection. And if you need any help along the way, contact us. Carbon Black regularly helps McAfee users make the switch. Let us help you get the protection you need.

### Planning
- Build project definition and plan
- Identify McAfee agents to replace
- Test drive the PSC and learn the console

### Installing
- Install the PSC agent on your endpoints
- Set up policies to allow the system to learn
- Configure prevention and detection to maximize efficacy and minimize false positives

### Testing
- Monitor and compare McAfee and the PSC reports
- Review alerts and begin to group, filter and tune priority
- Refine views and searches for investigations and hunting

### Change Over
- Configure OS security controls
- Elevate the PSC policies on endpoints
- Move McAfee into unmanaged mode
- Uninstall McAfee locally or through remote administration means

### Rollout
- Hold interactive Q&A session with real-time example
- Train on best practices
- Review alerts and optimize policies
- Teach team to investigate and hunt threats
ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers’ behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company’s partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world’s leading IR firms, who use Carbon Black’s technology in more than 500 breach investigations per year.

Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.