Carbon Black.

How the cloud solves 10 endpoint security problems for SMBs
Is your traditional endpoint security getting the best of you?

It’s time to move to the cloud.

Small and medium businesses (SMBs) like yours are facing massive cyber security challenges. In fact, according to the Verizon 2017 Data Breach Investigations report, 61% of breach victims in the previous year were businesses with fewer than 1000 employees.

It’s time to proactively protect your company—and the place to start is your endpoints. Why? Because IDC research found that 70% of successful breaches begin at the endpoint.¹ However, if you are taking a traditional approach to endpoint security, it may be causing you more problems than it solves and here’s why:

¹ “Cybercrime: The Credentials Connection,” IDC, 2014
Too Much to Manage

Too Little Time

Too Few Skilled Staff

In many SMBs, the staff in charge of security often also has to manage the entire IT infrastructure. That can be challenging, especially when it is critical to secure the endpoints and patch vulnerabilities. Plus, traditional endpoint security can’t keep up with attackers, so you often need to deploy a whole array of different tools as you attempt to protect your environment. And because each solution has its own agent, backend console, policies, configurations and costs, there is a great deal of complexity that is difficult to manage.

Managing a full IT infrastructure leaves little time to keep all your security products up-to-date and properly configured to protect against the latest threats. This leaves your environment full of gaps and vulnerabilities that allow attackers in the door. Ransomware and cryptocurrency mining, along with targeted breaches, are just a few examples of the malicious events that are continuously evolving to circumvent common security products – and the attackers don’t care if your company is large or small.

A good understanding of the rapidly changing threat landscape is essential because proper IT hygiene and best security practices are a powerful weapon against any attacker. But what if you are one of the 67% of cybersecurity professionals that can’t keep their skills up-to-date due to the demands of their job? That’s understandable, especially in a company your size, with a staff that fills multiple roles. More people might be the answer, but that too is a challenge as there is a severe shortage of skilled security professionals right now.

2 “The Life and Times of Cybersecurity Professionals,” ESG, November 2017
The Top 10 Problems Solved by the Cloud

Traditional endpoint security can result in ten real and tangible problems that require lots of time and resources to address.

<table>
<thead>
<tr>
<th></th>
<th>Problem Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Managing Infrastructure</td>
</tr>
<tr>
<td>2</td>
<td>Preventing New Attacks</td>
</tr>
<tr>
<td>3</td>
<td>Getting the Help You Need</td>
</tr>
<tr>
<td>4</td>
<td>Identifying Problems</td>
</tr>
<tr>
<td>5</td>
<td>Responding Quickly to Threats</td>
</tr>
<tr>
<td>6</td>
<td>Keeping Up to Date</td>
</tr>
<tr>
<td>7</td>
<td>Securing Remote Workers</td>
</tr>
<tr>
<td>8</td>
<td>Integrating Security Products</td>
</tr>
<tr>
<td>9</td>
<td>Managing Multiple Agents</td>
</tr>
<tr>
<td>10</td>
<td>Slowing Down Endpoints</td>
</tr>
</tbody>
</table>

If you are experiencing any or all of these, don’t worry. There is a solution: cloud-based endpoint security.
The Cloud is Your Only Choice

The cloud provides you with a cost-effective, continually up-to-date solution that can alleviate the pressure on you and your security team – all while providing better protection for your organization. The cloud can solve the most common problems caused by traditional approaches because it has much more processing, storage and analytics power than any on-premise solution.

AND HERE’S WHAT THAT POWER DELIVERS:

• Converged prevention, detection and response in a single solution.
• Superior protection due to advanced big data analytics capabilities.
• A simplified cloud-based management model with no onsite infrastructure to manage.
• Integration across your security stack, unifying your defenses.
• The ability to focus on what really matters, protecting your organization proactively.

In today’s world of rapidly evolving threats, there is only one choice for SMBs that want to gain an advantage over attackers – and that’s an endpoint security platform that runs in the cloud.

87% of organizations report some of their SOC functions are handled in the cloud or plan to move them there in the next 24 months.³

³ “Future SOC: SANS 2017 Security Operations Center Survey,” SANS Institute, May 2017, p. 4, Figure 3
PROBLEM:

Managing Infrastructure

Whether you have one on-premise solution or ten, the management required to keep all your endpoint security products up-to-date can be complex and costly. From an operations point of view, an on-premise infrastructure requires costly capital expenditures (CapEx) for servers, storage and networks, all of which become obsolete quickly as new technology emerges. And as an SMB, you most likely have limited computing, storage and analytics power on site, so your ability to fully protect your endpoints is constricted.

"Managing between our traditional AV and all the other security tools my team has to manage, all the on-prem infrastructure becomes a nightmare – to maintain upgrades, to make sure you have enough storage and compute power."

— RYAN MANNI
SECURITY OPERATIONS MANAGER / HOLOGIC

SOLUTION:

The Cloud Has No Infrastructure to Manage

When you turn to the cloud, you get the immediate benefit of an entire managed operation whose only job is keeping your security solutions running, updated and secure. You can focus on security without the complications that come with a self-managed infrastructure. Finances are easier, since the cloud’s OpEx (operational expenditure) model does not require a long-term capital investment. The cloud’s management model greatly simplifies operations, with seamless updates to your software and hardware, turning around new capabilities faster than you can on premise. And all that massive-scale big data processing is configured, deployed and managed for you. Plus, a cloud solution is elastic in nature, so you can easily scale the number of endpoints up and down as your business grows.
# Problem:

## 2 Preventing New Attacks

With the volume and severity of unknown attacks today, uncertainty and lack of visibility has become the new norm in cyber security. Traditional antivirus can only stop and prevent known malware attacks, which only accounts for 30% of today’s attacks.

So, as new attacks emerge, vendors must react quickly to identify the attack’s signature and provide you with a signature-pack update to defend against it – which is a process that could take days or weeks to resolve. This leaves your organization highly vulnerable, as attackers are innovating rapidly, utilizing advanced capabilities to easily get into your environment. Plus, many of the new attack techniques leverage known, good applications and use exploits that escalate privileges to bypass your defenses – a class of threats known as fileless or non-malware attacks. And once inside, they can stealthily keep probing, learning and accessing data until the root cause is found and eradicated.

## Solution:

### The cloud leverages big data and sophisticated analytics to predict attacks

Big data analytics in the cloud is the future of security – and it’s your best opportunity to fully protect your organization. By capturing real-time activity data from all your endpoints and analyzing it for malicious behavior, the cloud effectively creates a global threat monitoring system. With sophisticated machine learning and analytic processes that study behaviors, file reputations, threat feeds and other sources of information, the cloud proactively identifies anomalies as they occur. Predictive models are generated and streamed down to the endpoint, allowing local systems to predict new threats and prevent unknown malicious behavior without signatures or pre-existing knowledge of the specific threat. This data-driven model of prediction and prevention is an important requirement for protecting endpoints from the types of sophisticated attacks seen today and expected over the next several years.

60% of security and IT personnel say their top challenge is finding new unknown threats for which their current security doesn’t have signatures.  

---

4 “Exploits at the Endpoint: SANS 2016 Threat Landscape Survey,” SANS Institute, September 2016, p. 14, Figure 10
Gone are the days when viruses were created by individual hackers for no other reason than to prove they could. Today there are reportedly over one million paid cyber criminals that are behind the incessant, non-stop attacks organizations large and small face each day. Cyber criminals operate within a large black-market economy, working together to enrich themselves and the people they work for. How can you – whether you are a staff of one security professional or even a staff of 40 – combat that?

The cloud is there when you need help, as it gives you access to broad and deep collaboration that goes beyond what your own staff can provide. By its very nature, the cloud can quickly connect you with thousands of global security experts that share best practices, compromise indicators and intelligence about emerging threats in real time. Your cloud-based endpoint security vendor can help you access this network of defenders. These security professionals continually research new threats, share their findings and build best-in-class security products to help organizations like yours. So when you are under attack from a new unknown threat, you can solve issues faster as you tap into this global resource of knowledge and expertise.

49% say lack of staffing and a skills shortage are top inhibitors to effective response.5

5 “The Show Must Go On!: The 2017 Incident Response Survey,” SANS Institute, June 2017, p. 23, Table 4
PROBLEM: 4 Identifying Problems

The adage “you can’t fix what you can’t see” applies here. Endpoints generate a lot of activity – in fact, a single endpoint can generate between 10,000 and 40,000 individual events on a daily basis.

This information could readily help you identify malicious activity that could lead to a harmful attack – if you could see it. But most traditional solutions don’t give you the massive processing power you need to collect that data, much less analyze it. Without visibility into endpoint activity, you can’t pinpoint what problems you have on your endpoints, where they are located, how important they are to fix or what resources are required to fix them. Not only does this limit your ability to discover and prioritize problems – it impacts your overall ability to build an effective security program. Ultimately, this leaves you in a constant state of reacting to issues and the tedious process of re-imaging machines in an attempt to close the gaps that allowed the attack initially.

SOLUTION: The Cloud Analyzes Unfiltered Endpoint Data to Give You the Visibility You Need

The cloud accelerates your ability to zero in on new attacks and take immediate action. You can quickly analyze unfiltered data, whether related to a threat or not. Streaming analytics connects these endpoint events together to give you a clear picture of what happened and when. This allows you to gain complete real-time visibility into all threat-related activity while identifying priority issues. You can see how attacks behave, what else is affected in your environment, where an attack might have spread and even identify the root causes within minutes. You can also get a broader picture of trends and patterns, so you can remediate future attacks more rapidly, without delays. And you can clearly communicate the state of your endpoints and the success of your security program to your management team.

40% of organizations say they can improve visibility into network and endpoint behavior for quicker detection to prevent threats that have taken place on their endpoints.6

60% say determining the scope of a threat across multiple endpoints is difficult.7

---

6 “2017 Threat Landscape Survey: Users on the Front Line,” August 2017, p. 9, Figure 13
7 “Next-Gen Endpoint Risks and Protections: A SANS Survey,” March 2017, p. 14, Figure 12
PROBLEM:

5 Responding Quickly to Threats

Even when you have the information you need about an incident and you know what steps you need to take in order to address it, traditional systems can still slow you down. Without built-in operational tools to address security issues, you are forced to move into completely separate tools, often owned by entirely different teams. This can take hours or even days to fully stop an attacker in their tracks and remediate the situation.

SOLUTION:

The Cloud Enables Real-time Investigation and Remediation

With the velocity of the cloud, you have the power to respond quickly, almost instantaneously. You can immediately identify problems, see where they started and stop them in near real-time, no matter where in the world the endpoint is. With real-time, live operational tools built directly into a cloud-based endpoint security system, you have centralized, secure remote access to endpoints for response and remediation. The cloud gives you the most efficient way to take corrective action to defend against attacks as they happen.

Speed is a big factor in effective endpoint security. When attacks occur, your want to see the problem, find the root cause and contain the situation – fast. But if you are unsure of when or where an attack started, it’s difficult to respond quickly and efficiently, especially if the attackers are moving faster than you are remediating.

55% say of organizations it takes 3 or more hours per endpoint to remediate, with most taking more than 24 hours.8

8 “Can We Say Next-Gen Yet? State of Endpoint Security,” SANS Institute, March 2016, p. 13, Figure 9
PROBLEM:

Keeping Up to Date

One of the first big problems with on-premise security solutions is the fact that software changes regularly, and therefore needs to be updated frequently. With lots of disparate solutions – and a quickly evolving threat landscape – keeping everything up to date is no small feat.

Take a look at a typical antivirus suite. It has at least five independent technologies, including signatures, firewall, host IPS, device control and application control, to name a few. And each has its own complex security policy configuration. As the threat landscape changes, each of these technologies inevitably requires new configurations or updates. With so many independent modules, it becomes harder and harder to keep endpoints current with the latest and greatest protection. This is a disruptive process that is counter-productive – even error-prone – as misconfigured technologies can open doors for attackers. It's also a significant resource drain for you and your administrators.

"[With traditional AV,] configuration settings were not intuitive, and we had updates fail and break a lot of things."

- CHRIS ST. AMAND
  NETWORK SECURITY ENGINEER / PEOPLESBANK

SOLUTION:

The Cloud Simplifies and Automates Updates

The cloud streamlines endpoint security management through a centralized, managed infrastructure that is much simpler, more accurate and less time-consuming for you and your IT staff. With your security in the cloud, every endpoint becomes part of a global threat monitoring system with real-time threat intelligence that is shared across all endpoints and configuration that is largely automated through big data analytics. The cloud can automatically and proactively adapt to new attacks and keep your endpoints up to date and protected. You can also safely leverage new and updated features as soon as they are released, which frees you up to focus on more pressing security issues.
PROBLEM:

7 Securing Remote Workers

You could end up with inconsistent individual setups on hundreds or thousands of endpoints, with out-of-date software and policy updates that don’t reach the remote devices. On-premise servers require endpoints to be on the local network for policy updates, yet remote employees often go weeks or months without connecting back to the corporate network. That means that endpoints can be significantly out of date with respect to your security policies. This increases your vulnerability and contributes to a lack of control, with little to no visibility into what is actually happening on these remote endpoints.

SOLUTION:
The Cloud Treats Every Endpoint the Same

The cloud eliminates the need for endpoints to connect back to the corporate network. It consistently protects every single endpoint, no matter whether the user is on the corporate network or halfway around the world. With the cloud, your endpoints all connect to the same, cloud-based service for configuration and updates – so they are all treated equally, with all the latest protection. As a result, all your assets are easily kept current and compliant and you retain complete control of all your endpoints.

46% of organizations have operations in more than one country.9

8 Integrating Security Products

Complexity arises when these solutions don’t work together: each product is controlled independently, storing independent copies of similar data and managing isolated workflows that create friction within processes and between teams. Without a single, unified view of your environment across all your security products, the overall value of each individual product is greatly reduced.

Many organizations have significant security investments beyond endpoint protection in products such as security information and event management (SIEM), analytics, network security and threat intelligence.

49% of organizations describe their endpoint detection and response (EDR) systems as not integrated or only partly integrated.10

4% consider their security analytics to be fully integrated.11

SOLUTION:
Cloud APIs and Pre-built Integrations
Unify Products

You’ll get the best protection when you have comprehensive access to all your security data – and this is where the cloud comes in. With the cloud, you can take advantage of standardized open APIs that help you integrate endpoint security with the rest of your defense stack. Look for cloud-based security products that come with seamless, pre-built integrations to tie products together and give you the ability to integrate your endpoint security with your own custom-built systems and tools. You can even develop custom workflows and automate practices for any scenario. This collective defense strategy improves your visibility because critical endpoint data is shared across the security stack. This increases the efficiency of your analysis and response to threats and maximizes your investments in your existing security products.

10 “The Show Must Go On! The 2017 Incident Response Survey,” SANS Institute, June 2017, p. 16, Table 3
11 “SANS 2016 Security Analytics Survey,” SANS Institute, December 2016, p. 1
PROBLEM:

Managing Multiple Agents

You’ll have to work out compatibility issues and technical support processes. Hopefully you won’t see performance issues between agents. If you have hundreds, or even thousands, of endpoints in your organization, it’s difficult to know where all the agents are deployed and which versions are where. And because each product has its own purpose and its own workflow, you’ll still need to tie all this information together somehow on the backend. It’s no wonder that staffs like yours just can’t keep up.

"IT and security personnel are tasked with managing and maintaining multiple endpoint agents that often have fragmented security systems."12

SOLUTION:

The Cloud Enables a Single Consolidated Agent

The cloud consolidates disparate solutions easily with multiple security functions on a single agent. Integrated policies keep all endpoints current and a single, centralized console integrates all workflows. The cloud’s single agent collects enormous amounts of valuable data once, which is then analyzed in the cloud and leveraged for smarter, more proactive protection across a variety of security services. As a result, you have one agent that performs the tasks of many. All of this is easy to deploy and configure through the cloud, so services can be added without the need for entirely new and different solutions. Plus, with a fully converged agent, you can eliminate products on your endpoints that you no longer need, which in turn reduces the impact on your employees.

12 "Endpoint Security: Preventing Threats on Devices Connected to Your Network," eSecurity Planet, March 2017
PROBLEM:

Slowing Down Endpoints

Antivirus scans and other protection modes require a lot of local processing power and hard disk scanning, which is a significant performance drain on your endpoints. Plus, traditional AV has limited visibility, so if there is an issue, it can be a major productivity drain for you, especially if you need to re-image user machines. Interruptions and aggravations like these not only affect you and your users, but they can also have a wider, more costly impact on your entire organization. Savvy users will simply turn off their endpoints security altogether – a situation that at best puts you in non-compliance and at worst, opens the door for a major breach.

"[We were] trying to find a really comprehensive security solution without impacting the behavior of our endpoints and the usability of them. A lot of them tend to take up a lot of system resources."

- TREVOR ALBRECHT, TECHNICAL OPERATIONS ENGINEER / DRAFT KINGS

SOLUTION:

Cloud Processing Keeps the Agent Lightweight

With all that you’re managing, the last thing you want is unhappy users. But with traditional antivirus running in the background and inhibiting user productivity, that’s what you’re going to get.

With the cloud, your users won’t even notice the impact endpoint security is having, because there is only one lightweight agent on their endpoints that performs all security processes without draining computing resources. Complex tasks are offloaded to the cloud where its unlimited storage and processing power can do the heavy lifting, making for an optimized experience and leaving users happy and productive. And you get all the visibility you need to keep endpoints protected, drastically reducing or even eliminating the need for reimagining.
Carbon Black.
The Easy Answer to Endpoint Security Problems

The Cb Predictive Security Cloud (PSC) is an endpoint protection platform that consolidates security in the cloud, making it easy to prevent, investigate, remediate and hunt for threats.

While other endpoint security products only collect a filtered dataset related to what’s “known bad,” the PSC collects all endpoint activity data, because attackers intentionally look normal in order to hide their attacks. This unfiltered data is the unique power of the PSC.

**THE PSC DELIVERS:**

**Superior Protection**
Stop more attacks, take back control over your endpoints, and worry less. The PSC applies predictive modeling to unfiltered data to stay one step ahead of sophisticated threats.

**Actionable Visibility**
Cut down the guesswork and close security gaps fast. The PSC empowers you to accelerate investigations and respond confidently to threats. While siloed toolsets can make it hard to know what you’re dealing with, the PSC gives you a comprehensive picture of what happened in the past and is happening now.

**Simplified Operations**
While most endpoint security programs require multiple siloed systems that burden end users and complicate management, the PSC consolidates multiple capabilities in the cloud using a single endpoint agent, console and dataset.

**Unified Defenses**
Full-stack integration shares unfiltered endpoint data to extract more value from existing investments while improving your security posture.

The PSC supports a variety of powerful next-generation endpoint security services, all of which are powered by the collective intelligence generated in the PSC. This collective intelligence is generated from data collected across millions of endpoints under management and enriched with threat intelligence from around the world in real-time.
Cb Defense is our next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution. Using advanced predictive models, Cb Defense uncovers malicious behavior and stops all types of attacks before they compromise systems.

Cb Defense for VMware

Cb Defense for VMWare is a cloud-delivered, purpose-built security solution for protecting applications deployed in the virtualized data center.

Cb ThreatSight

Cb ThreatSight is a managed service for Cb Defense customers that provides a world-class team of Carbon Black security experts who work side-by-side with your organization to validate and prioritize alerts, uncover new threats, and accelerate investigations.

Cb ThreatHunter

Cb ThreatHunter is a threat hunting and incident response solution delivering unfiltered visibility for top security operations centers and IR teams.

Cb LiveOps

Cb LiveOps is a real-time security operations solution that enables organizations to ask questions of all endpoints and take action to instantly remediate issues.

To learn more about how the cloud can solve your problems, view this informational webinar.

CLICK HERE TO VIEW THE WEBINAR
About Carbon Black.

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

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

SOME OF OUR HAPPY CUSTOMERS: