10 ENDPOINT SECURITY PROBLEMS AND HOW THE CLOUD SOLVES THEM
The evidence is clear.
Your traditional endpoint security is not solving problems for you – it’s creating them.

Companies are facing massive cybersecurity challenges – many of which are rooted in the endpoint. In fact, according to IDC\(^1\), 70% of successful breaches begin at the endpoint. One has to ask: if traditional endpoint security was doing its job, why are these attacks so successful? Does that technology work anymore? Many believe not. In fact, it can be argued that legacy endpoint security products are actually creating more problems than they solve – and here’s why:

---

\(^1\)“Cybercrime: The Credentials Connection,” IDC, 2014
Because traditional antivirus (AV) software is limited, security organizations often deploy a whole array of different security tools – ten, on average. Each solution has its own agent, backend console, policies, configurations and costs. This creates an overly complex, resource-intensive environment that is challenging to maintain and integrate. It’s almost impossible to keep all these products current, and as a result, your environment could be full of gaps and vulnerabilities that allow attackers in the door.

With all these solutions in place, organizations face challenges in keeping them all up to date and properly configured to protect against the latest threats. Ransomware and malicious cryptocurrency mining, along with targeted breaches, are just a few examples of the malicious events that are continuously evolving to circumvent common security products. If your organization is like most, it’s difficult to move beyond a reactive operational model, leaving you unable to defend your environment properly.

Are you one of the 67% of cybersecurity professionals that say it’s hard to keep their skills up to date due to the demands of their job? That’s understandable, because there is a severe shortage of skilled security professionals across the industry – not enough people are trained to address the issues we all face. Meanwhile, a good understanding of the rapidly changing threat landscape is essential because proper IT hygiene and best security practices, tuned to the state of current cyber threats, are a powerful weapon against the attacker. If you don’t have time to take these steps, you leave your environment exposed.

2 “The Life and Times of Cybersecurity Professionals,” ESG, November 2017
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 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 on-site infrastructure to manage
• Integration across your security stack, unifying your defenses
• The ability to focus on what really matters, protecting your organization proactively

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

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.²

² “Future SOC: SANS 2017 Security Operations Center Survey,” SANS Institute, May 2017, p. 4, Figure 3
PROBLEM:

1. Keeping Up to Date

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: 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.

SOLUTION: Cloud APIs and Pre-built Integrations

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.

49% describe their endpoint detection and response (EDR) systems as not integrated or only partly integrated.4

4% consider their security analytics to be fully integrated.5
**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 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." — E-SECURITY PLANET

**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.

6 “Endpoint Security: Preventing Threats on Devices Connected to Your Network,” eSecurity Planet, March 2017
PROBLEM:

4 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 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.

46% of organizations have operations in more than one country.7

SOLUTION:
The Cloud Treats Every Endpoint the Same

Almost every company has remote workers today. However, traditional security solutions were not built to secure endpoints outside the corporate network. Whether employees are around the corner, in a branch office or halfway around the globe, protecting them with traditional endpoint security can be problematic.

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.

PROBLEM:

5 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.

The last thing you want is unhappy users – but with traditional antivirus running in the background and inhibiting their productivity, that’s what you’re going to get.

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 endpoint security altogether – a situation that at best puts you in noncompliance, 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, SYSTEM ADMINISTRATOR / DRAFTKINGS

SOLUTION:

Cloud Processing Keeps the Agent Lightweight

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 re-imaging.
PROBLEM:

6 Preventing New Attacks

With the volume and severity of unknown attacks today, uncertainty and lack of visibility has become the new norm in cybersecurity. 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 and 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 we are seeing today and will see for 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.8

8 “Exploits at the Endpoint: SANS 2016 Threat Landscape Survey,” SANS Institute, September 2016, p. 14, Figure 10
**PROBLEM:**

7 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 in order 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 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. 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. 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. 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.

40% say they can improve visibility into network and endpoint behavior for quicker detection to prevent threats that have taken place on their endpoints.9

60% say determining the scope of a threat across multiple endpoints is difficult.10

---

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

Speed is a big factor in effective endpoint security. When attacks occur, you 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.

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.

55% say it takes three or more hours per endpoint to remediate, with most taking more than 24 hours.11

---

11 “Can We Say Next-Gen Yet? State of Endpoint Security,” SANS Institute, March 2016, p. 13, Figure 9
PROBLEM: Getting the Help You Need

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 cybercriminals that are behind the incessant, nonstop attacks organizations face each day. Cybercriminals 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?

SOLUTION: The Cloud Facilitates Collaboration and Education

The cloud is there when you need help, as it gives you access to broad and deep collaboration that goes beyond your own enterprise. 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.12

12 “The Show Must Go On! The 2017 Incident Response Survey,” SANS Institute, June 2017, p. 23, Table 4
PROBLEM: 
10 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 even if they are kept current, there is often 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 that application 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 operational expenditure (opex) 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 organization grows.
Ready to move to the cloud?

If you want to leave all of your on-premise endpoint security problems behind, then you’re ready to move to the cloud. Here is a handy checklist to use when you evaluate cloud-based endpoint security solutions and look for a reliable provider to work with:

• A single automated console for easy, automated updates
• A single lightweight agent
• Endpoints that are treated equally
• No performance impact on endpoints
• Open APIs for the utmost in security integration
• Complete visibility into all endpoint activity
• Real-time response and remediation
• Predictive big data insights into emerging attacks
• Collaboration and insights from global security experts
• Simplified IT and security operations

The Easy Answer to Endpoint Security Problems

VMware Carbon Black is the leading provider of next-generation endpoint security solutions. The VMware Carbon Black Cloud continuously captures, records and analyzes rich, unfiltered endpoint data that enables our customers to predict, prevent, detect and remediate the most advanced cyber threats.

The Carbon Black Cloud platform sits at the heart of VMware Carbon Black’s endpoint security solutions and provides advanced intelligence to all VMware Carbon Black products based on big data analytics across hundreds of billions of endpoint events per day.

THE CARBON BLACK CLOUD

Superior Protection
Combine prevention, detection and response with predictive modeling based on big data analytics to stay one step ahead of sophisticated threats. Stop more attacks, take back control over your endpoints and worry less.

Actionable Visibility
Respond quickly and confidently to attacks and breaches. While siloed toolsets can make it hard to know what you’re dealing with, the Carbon Black Cloud gives you a comprehensive picture so you can cut down the guesswork and close security gaps fast.

Simplified Operations
While most endpoint security programs require multiple siloed systems that burden end users and complicate management, the Carbon Black Cloud is a converged cloud platform that delivers next-generation security services so you can free.

The Carbon Black Cloud supports a variety of next-generation endpoint security services, all of which are powered by the collective intelligence generated in the Carbon Black Cloud. This collective intelligence is amassed from data collected across millions of endpoints under management and enriched with threat intelligence from around the world in real time.