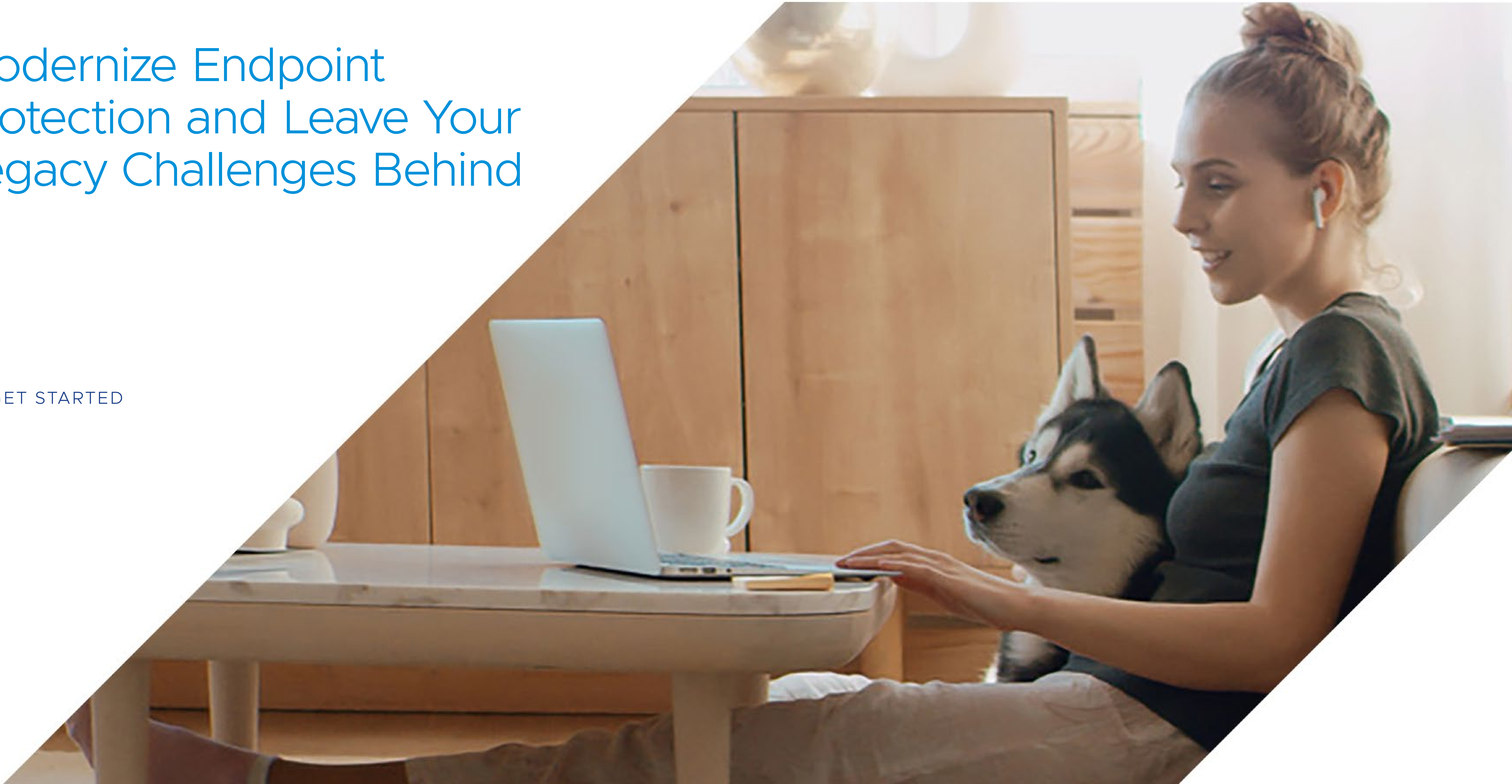
Modernize Endpoint Protection and Leave Your Legacy Challenges Behind

▶ GET STARTED



The Risk of Keeping Your Legacy Endpoint Security Tools

You are continuously combating new and increasingly sophisticated threats, many of which target your endpoints. Using legacy endpoint security tools is not effective at preventing these advanced attacks as your team is burdened by maintaining an overly complex environment with outdated policies and facing performance issues. Outdated approaches are no longer enough to keep your systems safe—they create more problems for you than they solve.

Take a step back and ask yourself these five questions for an endpoint security reality check and to determine if you are ready for modernization:

1. **Does your endpoint security tool provide you with robust detection capabilities?** Some endpoint security tools only protect against known malware, leaving you at risk for more advanced risks, such as ransomware. If you don't have fileless attack protection because your solution is only signature-based, then it means your endpoints are still vulnerable.
2. **Is your endpoint security tool integrated and easy to manage?** Many organizations use siloed technologies that are difficult to manage. This most likely means that your security staff wastes time on simply maintaining the technology rather than discovering active threats.

3. **Is there a single cloud-based console where your admins can manage your endpoints, investigate incidents, and triage alerts?** Continual maintenance and patching of on-premises tools, frequent manual upgrades to each agent, and pivoting between consoles is not efficient. It results in draining your security resources unnecessarily.
4. **Can you easily visualize an attack timeline and quickly close gaps?** Users of legacy endpoint security tools are hindered by limited visibility into how and where threats enter from and move laterally. This results in limited remediation capabilities with no customizable prevention or threat hunting features, making it a challenge to respond to threats effectively. Plus, with limited reporting, you may have difficulty in finding root causes and preventing future attacks of the same pattern—all of which increases your organization's risk.
5. **Is your endpoint security tool software-driven, cloud-based, and constantly updated with the latest technology advancements?** To be effective, today's security capabilities must stay one step ahead of threat actors that are using innovative attack methods. If your products don't have the latest advancements in endpoint protection, you may be unable to respond effectively to the new and emerging threats that are evolving daily across increasingly distributed IT environments and workforces.

Considering Modern Endpoint Security

If you answered no to any of the previous questions, it's time to consider a more modernized approach to endpoint protection. In today's world of rapidly evolving threats, you need to gain a decisive advantage over attackers that are becoming more innovative and resourceful. This will alleviate the pressure on you and your security team—all while providing better protection for your organization. The following capabilities are a few of the features of modern endpoint protection to consider:

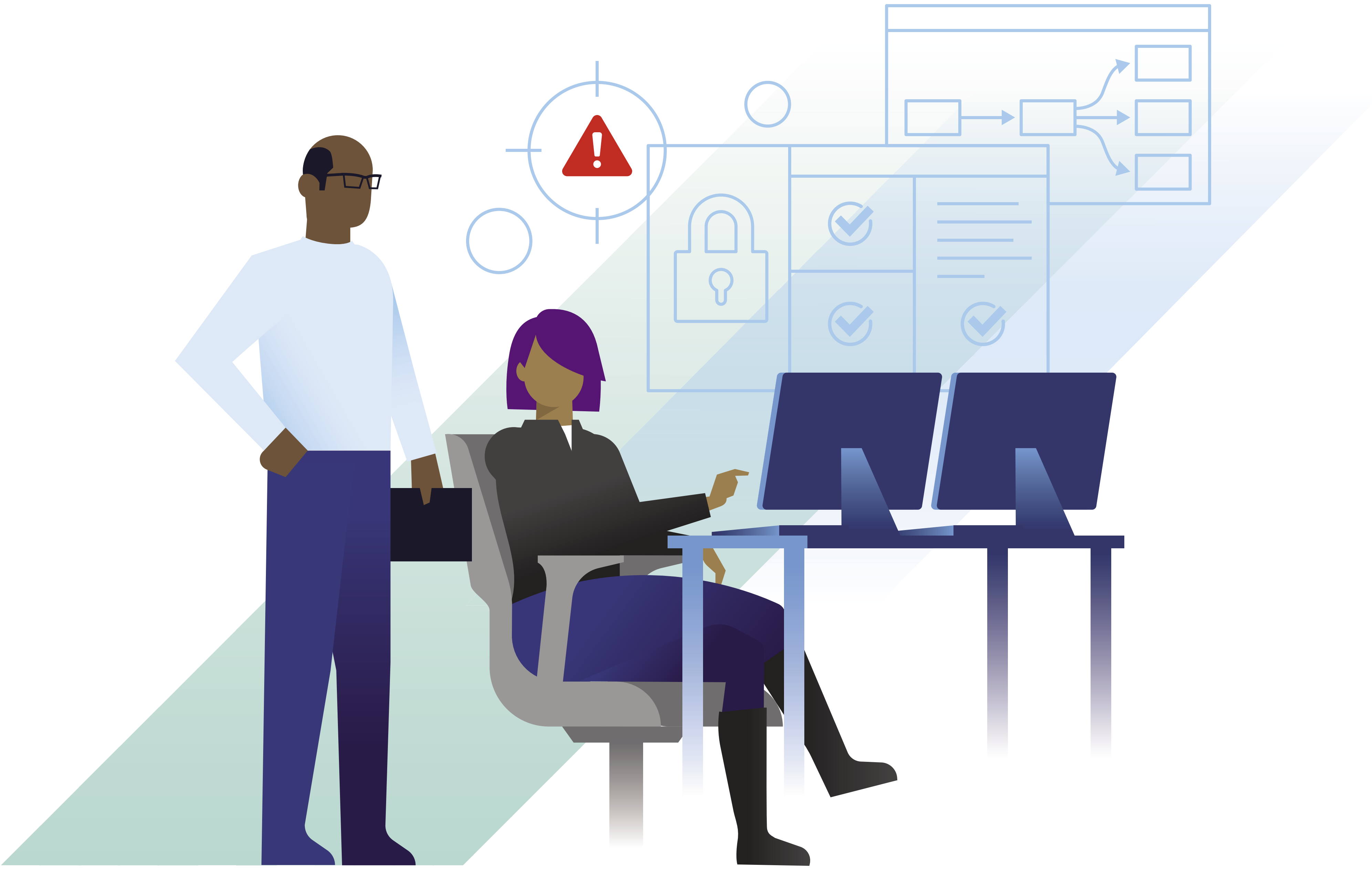
- Converged prevention, detection and response in a single, intuitive cloud-based platform
- Superior, third-party tested, multilevel protection that incorporates heuristics, machine learning, AI, device control, and behavioral analysis
- A single cloud-based agent and console with no onsite infrastructure needed to decrease negative endpoint performance impacts
- Integration across your security and IT stacks, unifying your defenses and IT operations to quickly patch and harden systems
- The ability to secure the distribution of IT environments and enable an increasingly anywhere workforce
- The flexibility for your endpoint security tool to be managed in house or by your third-party service provider

> "With COVID-19 catalyzing digital transformation and a shift to cloud services, these sorts of sophisticated attacks will only increase in frequency."
>
> TOM KELLERMANN
> HEAD OF CYBERSECURITY STRATEGY
> VMWARE SECURITY BUSINESS UNIT

Legacy Endpoint Security Challenges Solved by Modernization

Modernizing endpoint security will alleviate the most common challenges faced by users of legacy endpoint security tools. These tools are overly complex and often cause more problems than they are worth, such as limited prevention capabilities, multiple agents, slower endpoint performance, and an inability to identify security gaps. The following list of common challenges are caused by these inadequate tools, and VMware offers recommended solutions based on our proven leadership in endpoint security:

1. Keeping systems up to date
2. Integrating security products
3. Securing remote workers
4. Slowing down endpoints
5. Ensuring cyber resilience toward new breaches
6. Increasing processing power and speed
7. Responding quickly to threats
8. Managing infrastructure



Challenge 1

Keeping systems up to date

Modern software changes regularly and needs to be updated in an agile way. However, legacy endpoint security tools often deploy disparate technologies that require their own consoles, software deployments, and policy configurations. Example technologies include signatures, firewall, host intrusion prevention system (IPS), device control, and application control, to name a few. As the threat landscape changes, each of these technologies inevitably requires new configurations or updates. With so many independent modules, it becomes harder to keep endpoints current with the latest and greatest protection. This is a disruptive, counter-productive process—even error-prone—as misconfigured technologies can open doors for attackers. It's also a significant resource drain for you and your administrators.

> "Traditional AV wasn't cutting it. We would often get alerts too late, or not even get them at all."
>
> RICH PELKIE
> HELP DESK ENGINEER
> GENTLE GIANT MOVING COMPANY

Modern solution: Simplified and automated updates

Streamline 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 cloud-delivered security, every endpoint becomes part of a global threat monitoring system with real-time threat intelligence shared across all endpoints and configuration that is largely automated through big data analytics. 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.

Challenge 2

Integrating security products

You most likely have deployed security operations investments beyond endpoint protection, such as security information and event management (SIEM), network security, automation tools, and threat intelligence.

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.

Island hopping is increasingly prevalent, as attackers hop from one network to another along its supply chain. Of the 180 incident response (IR), cybersecurity and IT professionals (including CTOs, CIOs and CISOs) surveyed, nearly half (44 percent) said they witnessed island hopping in more than 25 percent of all IR engagements.[1]

Modern solution: Unify products with 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 a unified platform comes in. With a single cloud-based platform, you can take advantage of standardized open APIs that help you integrate endpoint security with the rest of your defense stack. Seamless, pre-built integrations tie products together and give you the ability to integrate endpoint security with any custom-built systems and tools. This allows you to develop custom workflows and automate processes for any attack scenario. This collective defense strategy improves your visibility because critical endpoint telemetry is shared across the security stack. This increases the efficiency of your analysis of and response to threats, and maximizes your investments in your existing security products.

[1] VMware. "2021 Cybersecurity Outlook: Attackers vs. Defenders." March 10, 2021.

Challenge 3

Securing remote workers

Your workforce needs the flexibility to connect from anywhere. However, legacy endpoint security solutions were not built to secure endpoints outside the corporate network. Whether employees are located in a branch office or halfway around the globe, protecting them with traditional endpoint security creates a variety of challenges.

You will end up with inconsistent policies or configurations on your fleet of endpoints, resulting in out-of-date software and policy updates that don't reach remote devices. On-premises servers require endpoints to be on the local network for policy updates, yet remote employees now go weeks or months without connecting back to the corporate network. That means endpoints can be significantly out of date with respect to security policy and endpoint management requirements from IT. This increases your vulnerability and contributes to a lack of control, with little to no visibility into what is happening on these remote endpoints.

63 percent of respondents witnessed counter-IR since the start of the pandemic. Security tooling disablement was the most observed technique.[2]

Modern solution: Workspace security combined with integrated insights

Eliminate the need for endpoints to connect back to the corporate network. This consistently protects every endpoint anywhere they are located. Implement a cloud-based platform that integrates with your unified endpoint management (UEM) tool. This enables all your endpoints to connect to the same service for configuration and updates, and ensures they are treated equally with the latest protection. As a result, all your assets are easily kept current and compliant, and you retain complete control of all your endpoints while enabling a distributed workforce.

[2] VMware. "2021 Cybersecurity Outlook: Attackers vs. Defenders." March 10, 2021.

Challenge 4

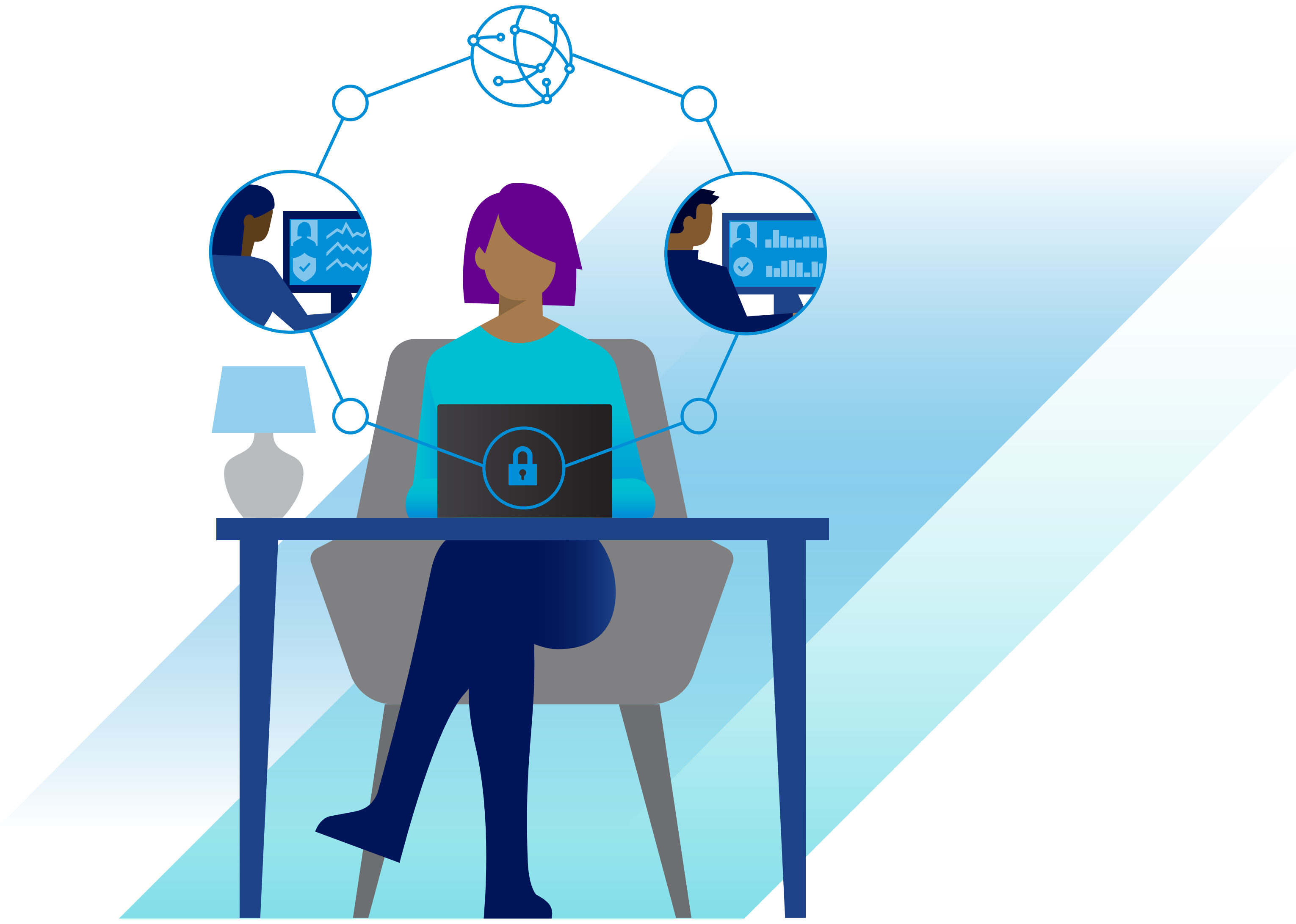
Slowing down endpoints

The last thing you want is decreased system performance that creates unhappy users. But with legacy tools running in the background and inhibiting their productivity, that's what you're likely to get. 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, legacy tools have limited visibility. If there is an issue, it can be a major productivity drain across your security and IT teams, especially if you need to reimage user machines. Interruptions and aggravations such as these affect you and your users, and 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 non-compliance, and at worst, opens the door for a major breach.

> "Our time to value with your product was almost instantaneous. I'm spending less time tracking down false positives and spending more time triaging and acting on legitimate threats. We don't bog down our internal network with legacy virus updates."
>
> JEREMY WILKINS
> SECURITY TECHNOLOGY ADMINISTRATOR
> OFS

Modern solution: A single lightweight agent

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 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 reimaging.



Challenge 5

Ensuring cyber resilience toward new breaches

With the volume and severity of known and unknown attacks today, uncertainty and a lack of visibility have unfortunately become the new normal.

As new attacks emerge, legacy endpoint security vendors must react quickly to identify the attack's signature and provide you with a signature pack update to defend against it. This process could take days or weeks to resolve. That 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. Once inside, they can dwell stealthily to move laterally and keep probing, learning and accessing data until the root cause is found and eradicated.

> "If you're hit by ransomware today, it's safe to assume the attacker has a second command and control post inside your infrastructure."
>
> TOM KELLERMANN
> HEAD OF CYBERSECURITY STRATEGY
> VMWARE SECURITY BUSINESS UNIT

Modern solution: Leverage big data and sophisticated analytics to predict attacks

Big data analytics in the cloud captures real-time activity data from all your endpoints and analyzes it for malicious behavior to create a global threat monitoring system. With sophisticated machine learning and analytics processes that study behaviors, file reputations, threat feeds, and other data sources, 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 sophisticated attacks.

Challenge 6

Increasing processing power and speed

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 daily. This data should help you identify malicious activity that could lead to a harmful attack—if you could only see it. But most legacy tools 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 the problems on your endpoints, how important they are to fix, or what resources are required to fix them. This limits your ability to discover and prioritize risk, and 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 reimaging machines to close the gaps that allowed the attack initially.

Modern solution: Analyze unfiltered endpoint data for more visibility

Quickly analyzing unfiltered data, whether related to a threat or not, accelerates your ability to zero in on new attacks and take immediate action. Streaming analytics connects a high volume of endpoint events together to give you more context and 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.

Challenge 7

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 laterally 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 to address it, legacy tools can still slow you down. Without built-in operational tools to address security issues, you are forced to move into 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.

Security teams have now adopted a proactive mindset. 81 percent of organizations surveyed reported having a threat hunting program.[3]

Modern solution: Real-time investigation and remediation

With the velocity of a cloud-based, next-generation endpoint protection platform, 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 located. With real-time operational tools built directly into an endpoint protection platform, you have centralized, secure remote access to endpoints for response and remediation. A cloud-first approach gives you the most efficient way to take corrective action to defend against attacks as they happen.

[3] VMware. "2021 Cybersecurity Outlook: Attackers vs. Defenders." March 10, 2021.

Challenge 8

Managing infrastructure

Whether you have one on-premises solution or 10, 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-premises infrastructure requires costly CapEx for servers, storage and networks, all of which become obsolete quickly as new technology emerges. 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.

> "With the traditional AV products, we had to have someone dedicated specifically to running the AV. [VMware Carbon Black Cloud] is easy. Through a single cloud portal, you can manage everything in one or two clicks—simple as that."
>
> ISANKA ATTANAYAKE
> MANAGER, IT INFRASTRUCTURE
> ROYAL CERAMICS LANKA

Modern solution: No 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. Finances and vendor management are also made easier because the cloud's OpEx model does not require a long-term capital investment. The management model of cloud-delivered software greatly simplifies operations with seamless updates to your software and hardware, turning around new capabilities faster than you can with on-premises tools. And all that massive-scale, big data processing is configured, deployed and managed for you. Plus, modern software is elastic by nature, so you can easily scale the number of endpoints up and down as your organization grows.

Moving Forward with Modernization

Modernizing your approach to endpoint security is defined by utilizing a software-driven, cloud-delivered platform that supports the distribution of your workforce and IT environments. When evaluating the legacy tools in your environment, keep the following shortlist of requirements in mind:

- A single automated console for easy, automated updates
- A single lightweight agent with 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 challenges

VMware Carbon Black Cloud™ is a cloud native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay using a single lightweight agent and an easy-to-use console. Instead of needing to deploy a variety of products—each with their own setups, configurations and policies—you will receive multiple security capabilities through a common, cloud-delivered platform that shares one sensor, one cloud console, and one dataset.

As your requirements change, adding new services is fast and easy, eliminating the need for additional CapEx investment or the need to deploy new agents. The platform is built on a comprehensive endpoint dataset that can be used and shared across tools and services, whether provided by VMware or other vendors. This creates a single source of truth and adds context to security operations across the board. The platform was constructed with the understanding that your security needs grow and change as the threat landscape evolves.

Receive modernized endpoint security for your team with:

- **Superior protection** – Stop more attacks, take back control over your endpoints, and worry less. VMware Carbon Black Cloud applies predictive modeling to unfiltered data to stay one step of ahead of sophisticated threats.
- **Actionable visibility** – Cut down the guesswork and close security gaps fast. VMware Carbon Black Cloud empowers you to accelerate investigations and respond confidently to threats. While legacy toolsets can make it hard to know what you're dealing with, VMware Carbon Black Cloud 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, VMware Carbon Black Cloud 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. Integrations with the VMware portfolio, such as VMware Workspace ONE® and VMware Horizon® virtual desktop infrastructure (VDI), ensures the enablement of your distributed workforce and breaks down siloes between security and IT teams.
- **Situational intelligence** – VMware Carbon Black Cloud supports a variety of powerful, next-generation endpoint security services. These services are powered by the situational intelligence generated in VMware Carbon Black Cloud from data collected across millions of endpoints under management and enriched with threat intelligence from around the world in real time.

VMware Carbon Black Cloud products and services

Consolidate multiple endpoint security capabilities, and operate faster and more effectively with a single, cloud native platform that provides:

- Next-generation antivirus and behavioral endpoint detection and response (EDR)
- Managed alert monitoring and triage
- Real-time device assessment and remediation
- Threat hunting and containment

Get Started Today

Transform your endpoint protection.

Learn More

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Item No: 830224aq-ebook-mdrnz-ept-prtctn-en-us-1080p 4/21