Intrinsic Security

How to unify and accelerate endpoint security across the enterprise

vmware® Carbon Black

Table of contents

Introduction 3

A short history of cybersecurity 3

Intrinsic security components 4

The table stakes: Five control points 5

Unified attacks require unified defenses 6

Sample risk scenarios 8

Ransomware 9

Credential theft, abuse or misuse 11

Phishing, spearphishing and other email-based attacks 13

Summary 16

Introduction

Now more than ever, for every global organization, the cloud is essential.

Adapting to COVID-19 is consuming nearly all of our collective attention at the moment. Yet, even before meeting today's crisis, private and public sector leaders were focused on how to expand global operations while also navigating their teams through a digital transformation.

As most executives come to realize, the cloud is **the** way—truly the only viable way—for businesses to thrive. In fact, no matter what captures our attention today or next year, the path forward hangs on the promise of the cloud.

Yet, with opportunities come risks. Especially when moves are made without considering likely security outcomes (e.g., cloud misconfigurations, unprotected Amazon S3 buckets, etc.). Unless and until security is **built in** straight from the start, every step of a digital transformation is at risk.

This paper provides a roadmap for putting your cybersecurity program on solid footing. By implementing unified security at the core control layers—endpoints, networks, identity systems, clouds and the workloads running on them—enterprise teams can reduce risk and costs while also meeting business goals. That's what intrinsic security is all about.

A short history of cybersecurity

In the late 1980s, the first computer-borne worm was accidentally launched as part of a research project to discern the size of the internet.[1] Since then, while we don't have precise numbers, we have determined that the internet is doubling at nearly twice its size every two years.[2]

And sadly, self-propagating worms and viruses are still with us. The way in which the cybersecurity industry has responded to these risks (and others) has been to focus on the specific layers, vectors and avenues that these attacks exploit. Rather than seeing these risks in context and addressing them holistically, most enterprises and the security vendors who support them have taken a vector-by-vector approach.

As the cybersecurity industry has grown from these early days, each vendor has come to market focusing on one aspect of cyber risk, whether that's risks to the endpoint, the network, the applications, or authentication systems and transactions. This best-of-breed approach encourages a disjointed and vulnerable defense with each team focusing on one type of product or aspect of IT infrastructure. By creating silos for IT operations and security, enterprises invite complexity and sacrifice unified visibility.

Plus, this legacy approach lends itself to a reactionary response. IT security teams become overly threat-centric because they're not able to see each threat within its broader context. And when teams do see the need for threat mitigations, they're often forced to figure out how to add security on top of processes and systems, rather than have security considerations addressed at the start.

Regardless of industry or geographic location, every enterprise has had to reckon with the challenges of a siloed, threat-centric and bolted-on security approach. Fortunately, there's a way out. And now is the perfect time. Considering that more than 50 percent of IT and security teams report being understaffed[3], it's critical we find ways to move forward to maximize effectiveness.

1. Forbes. "This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries." Gil Press. November 1, 2015.
2. Live-Counter.com. "How Big Is The Internet?"
3. VMware Carbon Black. "2020 Cybersecurity Outlook Report." March 2020.

Intrinsic security represents VMware's vision to disrupt cybersecurity by **embedding** unified visibility and control into every aspect of an enterprise's infrastructure: network, workload, cloud, workspace/ endpoint and identity.

ARM YOUR THREAT HUNTERS

One big takeaway from security-mature enterprises is that threat hunting programs work. According to a 2019 SANS survey, 36 percent of respondents report significant improvement in robust detections and better coverage after implementing threat hunting programs.[4] Like an early warning alarm system, threat hunters uncover hidden attacks that may have percolated under the radar of traditional security tools such as antivirus tools, security information and event management (SIEM) solutions, and intrusion detection systems (IDSes). By proactively discovering these stealthy indicators of compromise, threat hunters can disrupt them before they take hold and wreak significant havoc. For information on how VMware Carbon Black Cloud™ can power your threat hunting program, please register for our *virtual Become a Threat Hunter workshop*.

Intrinsic security components

It's all hands on deck when it comes to cyberthreats. Considering that IT teams are now responsible for more devices, applications and data than ever before, defending against these constant attacks has never been more challenging. A new approach is desperately needed. One that can scale to accommodate an ever-expanding risk surface area. That's precisely what intrinsic security offers. In fact, it's truly the only way to make real progress in fighting against cyberattacks.

To meet an ever-expanding risk surface area, enterprise teams must:

- **Broaden their defenses** – Go beyond siloes; implement unified security across endpoint, workloads, clouds, networks and identities.
- **Deepen their analysis** – Capture and analyze activity based on multiple methods (machine learning, signatures, behavioral, etc.) and from vast data sets (cloud-based and endpoint-based).
- **Extend their reach** – Integrate easily with other security technology for orchestrated and automated workflows.

This is the core framework for intrinsic security. Breadth. Depth. Extensibility.

The three distinct attributes that intrinsic security is based on deliver the breadth, depth and extensibility that today's global enterprises require:

- Security is unified across tools and teams.
- Security is context-centric based on what you're trying to protect.
- Security is built in to the infrastructure.

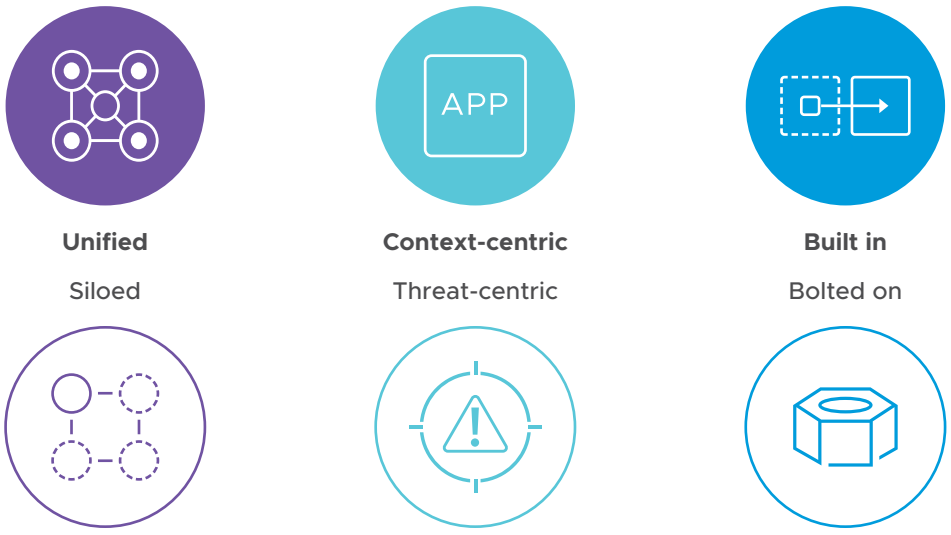

FIGURE 1: Intrinsic security attributes.

4. SANS Institute. "SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters." Mathias Fuchs and Joshua Lemon. October 25, 2019.

The table stakes: Five control points

Five architectural components enable the applications and data that drive enterprise business: endpoints, workloads, clouds, networks and identity systems. By embedding security into each of these control points, and unifying security controls via a single management approach, teams can improve security, eliminate complexity and gain efficiency.

First, it's essential that each team responsible for managing these core control points gain visibility into how enterprise applications and data are accessed. Table 1 lists these control points, along with the key questions faced by the teams managing them.

CONTROL POINT	EXAMPLES	WHO IS RESPONSIBLE	WHAT THEY NEED TO KNOW
Endpoints	Laptops, servers, point-of-sale (POS) systems and so on	IT and/or security	• Have I hardened my devices? • Are my endpoints secure? • Can I trust this device and allow it to connect?
Workloads	Infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), hybrid/multi-cloud	CloudOps/ Infrastructure/ DevOps/ SecDevOps	• Are my workloads configured appropriately? • Have I reduced the attack surface on my workloads? • How can I detect and respond to issues as they arise?
Clouds	Hybrid, edge, public, telco	Cloud team/ service provider	• Are my public clouds configured securely?
Networks	LAN, VLANs, WAN, demilitarized zone (DMZ) and so on	Network operations	• Are my trusted networks secure? • Have I micro-segmented my critical assets? • Do I have malicious traffic internally? • Have I segmented my network to limit lateral movement?
Identities and identity systems	Active Directory, single sign-on (SSO), password managers and so on	IT and/or Infosec application owners	• Is the user who they say they are? • Can I trust this authentication or authorization process (e.g., do I expect this behavior)? • Which credentials may have been compromised?

TABLE 1: Control points that drive enterprise business.

To answer these questions accurately and fast, teams need to know what is happening on these control points, and whether these activity patterns are normal, unusual, or signal a potential attack or intrusion.

Currently, most enterprise teams use multiple technologies accessed through a myriad of consoles to do their jobs on a daily basis. The task is not trivial, nor are attempts at trying to make any sense from all the data. As a result, teams are limited in terms of their threat understanding and ability to prioritize incident response efforts. And because most threats involve more than one control point, gaining full contextual awareness remains elusive.

With our intrinsic security approach, deep monitoring and behavioral analysis are implemented at each control point, and then unified for full contextual awareness. Like a video camera that records every move at each control point, intrinsic security enables comprehensive contextual awareness. Because there's no need to manually stitch together telemetry from disparate control points, teams are empowered to track down threats from the point of entry and every step in between.

Unified attacks require unified defenses

Attackers don't limit their nefarious activity to one control point. In fact, the more sophisticated ones are adept at staying under the radar. Attacker activity on any one individual control point may appear on the surface as benign. But when we put it all together, we're better armed to defend ourselves.

After all, the hidden operational gaps that form when teams work in siloed workflows are cracked open by innovative cybercriminals. An intrinsic security approach breaks down these silos across critical control points so teams can collaborate more quickly and more cohesively. A threat's full context is shared among teams so they can be proactive, prioritizing the threats with the greatest impact, and orchestrating coordinated responses for better outcomes.

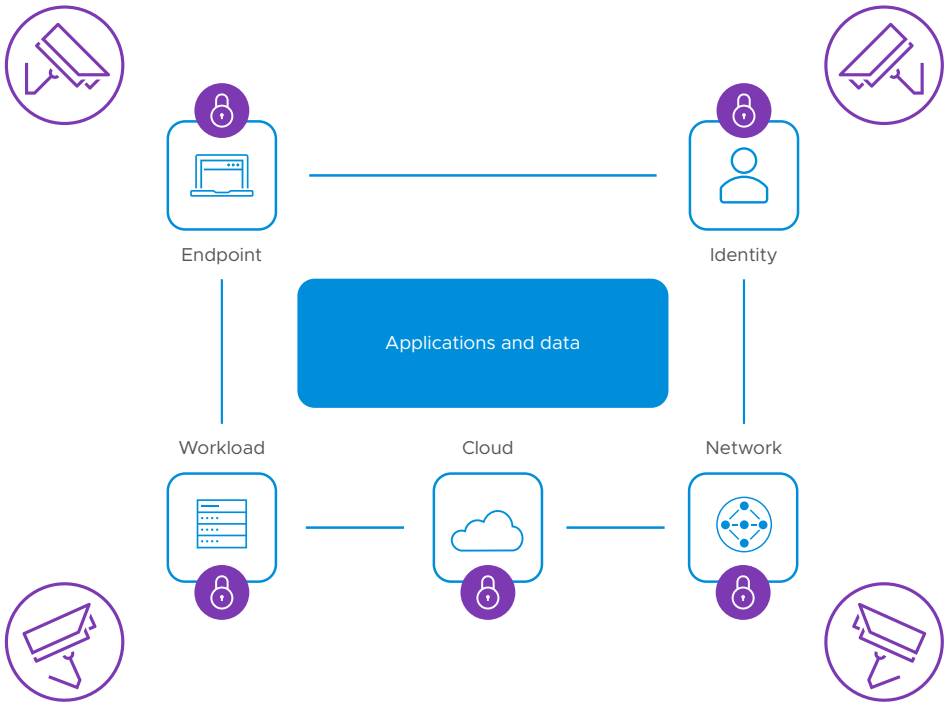

FIGURE 2: The five control points of intrinsic security.

This approach reduces risks as well as costs. Hardening endpoints and improving cyber hygiene goes a long way in preventing attacks from ever starting. Additionally, our approach combines multiple prevention capabilities rather than just relying on one method, such as machine learning, or signatures or behavioral analysis alone. This is why we catch attacks others might miss.

With clear and comprehensive insight into what's happening on every endpoint, you can respond faster and with more precision than ever before. The faster you can detect a threat, the more likely you can disrupt it, and achieve a better outcome.

In the next section, we'll demonstrate how our approach enables you to broaden, deepen and extend your defenses in some common risk scenarios.

Sample risk scenarios

While IT and security teams must defend against a wide variety of attacks, there are some standard attack patterns to recognize. After all, knowing how attacks happen can enable teams to better prepare, prioritize and develop standardized defenses.

We've outlined the typical steps attackers take when targeting a victim, as well as how enterprises can implement intrinsic security countermeasures.

Step 1: Reconnaissance and infiltration

Port scans, network probes, social engineering and other tactics are used to gain intel about the victim to determine how best to infiltrate the network. The goal during this step is to gain initial access without setting off any alarms. Infiltration tactic examples include drive-by compromise (browser session hijacking); exploiting a publicly facing application; compromising an external remote service (e.g., VPN); credential theft and/or reuse; and phishing links or attachments.

Effective countermeasures: Harden and prevent

Forward-thinking enterprises reduce the overall risk surface area exponentially through simple cyber hygiene measures. From patching vulnerabilities to running continuous, proactive scans across their environments, enterprises can shrink the issues they need to respond to, increasing their resilience and efficiency overall. Additionally, by implementing strong authentication and securing remote worker access, enterprises empower employee productivity while effectively keeping attackers from compromising corporate data and communications.

Step 2: Persistence and manipulation

Once an attacker has gained access, the next goal is to maintain that access as long as possible without being detected. Maintaining persistence is accomplished via methods such as manipulation of valid accounts and OS accessibility features; creation of new accounts; accessing hidden files and folders; abusing PowerShell profiles; modifying registry settings and run keys; and shortcut modifications.

Effective countermeasures: Monitor and detect

Capturing detailed activity across endpoints and correlating this data with network traffic and authentication processes provides the necessary context to identify a cyberattack. Unifying the bread crumbs an attacker leaves behind is finally possible with an intrinsic security approach. Because VMware Carbon Black Cloud constantly monitors and analyzes behavioral patterns across each control point, it can discover stealthy attacker activity that may seem innocuous out of a unified context.

Step 3: Execution and exfiltration

Attacker intent is not always known, but one of the most common is to steal data they can resell on the dark web. Whether a customer's private information (e.g., health records) or a company's secrets (e.g., intellectual property theft or corporate espionage), the attacker's goal is to exfiltrate the data without setting off any alarms, and removing all traces of their presence. During this process, the attacker may also move laterally across a network, as well as escalate their privilege to find what they're looking for. Once they do, they often encrypt and compress the data to make it undetectable and faster to transfer (either over a command and control channel, alternative protocol, other network medium or directly to the cloud).

Effective countermeasures: Respond and recover

Block unauthorized lateral movement with micro-segmentation to protect critical applications, data and workloads. Establish monitoring protocols for privileged accounts as well as outbound communications to known command and control servers. Plus, remember the importance of detailed forensic data and artifacts. Without this evidence,

According to our threat data, ransomware attacks against financial services firms increased more than 900 percent in the short period from February 2020 to April 2020.[5]

leaders are unable to make good decisions on whether or how to prosecute the breach, or how to strengthen controls and update security policies.

In each of the following risk scenarios, we outline how VMware Carbon Black Cloud broadens, deepens and extends your defenses across your enterprise.

Ransomware

Ransomware is one of the most disruptive and costly types of malware. Because it renders the victim's data and systems inoperable until the ransom is paid, ransomware threats force businesses to make an intolerable choice: Accede to a criminal's demand to pay up, and pay up quickly, or risk losing even more money while putting your operations, your brand and customer trust at risk.

While no industry is safe from these attacks, recent ransomware attacks against the financial sector are on a particularly high rate of growth, likely designed to exploit the current public health and economic crisis. According to our threat data, ransomware attacks against financial services firms increased more than 900 percent in the short period from February 2020 to April 2020.[5]

Ransomware costs go well beyond the actual ransom (if paid) and can result in data loss, downtime, lost productivity and reputational harm, not to mention all of the costs associated with recovery: restoring systems, processes and brand reputation; educating employees; and conducting complete forensic investigations.

How does it work?

The tip of the spear in ransomware attacks is often a phishing email or other social engineering tactic, to trick users into giving up their credentials or downloading the malware directly. That said, in one of the most devastating ransomware attacks, NotPetya, the attackers relied on exploiting a common vulnerability to infect victim systems, avoiding the need to trick users at all.

The latest ransomware innovations use PowerShell, scripts, macros and memory-based attacks to bypass traditional signature-based antivirus. Leveraging these native technologies allows the attacker to avoid detection during the delivery and installation phase of an attack.

Once installed, the ransomware immediately encrypts some or all of the user files. The files and file system remain encrypted until and unless the victim follows the attacker's directions, pays the ransom, and obtains the decryption key to restore access to their system and data.

Ransomware is big business and continues to grow exponentially. In underground forums, ads for ransomware as a service target inexperienced cyberattackers with the means, guidance and infrastructure to get started on their own for as little as $10 in seed money.[6]

What you can do

Despite the gloomy picture, there are concrete steps you can take to avoid becoming the next ransomware victim. Specifically, VMware Carbon Black solutions prevent ransomware attacks via three specific protection mechanisms. Here's how it works.

Know the real-time security state of each of your endpoints. This is the crucial first step in preventing ransomware and other malware outbreaks. With our platform, IT and security can understand the current state of more than 1,500 artifacts on any endpoint and run ongoing assessments to track IT hygiene. They can also take immediate action remotely with a secure shell into any endpoint on or off the network, performing full investigations and resolving exposures that provide ransomware attackers a foothold.

5. VMware Carbon Black. "Modern Bank Heists 3.0." Tom Kellermann and Ryan Murphy. May 2020.

6. Recorded Future. "5 Ransomware Trends to Watch in 2020." Allan Liska. February 13, 2020.

Pro tip: With VMware Carbon Black® Cloud Enterprise EDR™, your threat hunting teams can proactively explore the environment for vulnerabilities that may expose you to ransomware risks.

By combining next-generation antivirus (NGAV) and behavioral endpoint detection and repsonse (EDR), VMware Carbon Black Cloud offers multiple layers of prevention capabilities to identify and disable ransomware and other types of malware. Rather than relying solely on signatures or machine learning, our solution uses these approaches and more. Our platform is continually updated with dynamic threat intelligence, including the latest signature updates, reputation scores, and more than 110 core attacker behaviors, such as the MITRE ATT&CK TIDs. This way, we can better identify known ransomware attacks before they are executed.

Block access to the goods, identify variants and trap them. Assuming the ransomware attack is able to slip past the first series of prevention measures, and initial execution begins, our behavioral analysis engine will identify the resulting activity and block it before it can cause damage. Specifically, VMware Carbon Black Cloud monitors and blocks access and modification attempts to master boot records and shadow copies. Additionally, it uses canary files, which are benign files that reside on the endpoint to lure, trap and expose evasive ransomware variants.

This approach enables VMware to continually improve our ability to detect new ransomware variants and improve our tactics in disrupting them.

Pro tip: With Carbon Black Cloud Enterprise EDR, you can customize detections based on your own data, or automatically leverage newly released indicators of compromise (IoCs) from VMware Carbon Black Cloud and third-party threat intelligence providers.

Disrupt phone home attempts, patch holes and verify the fixes. VMware Carbon Black Cloud can identify new ransomware variants, even for endpoints that are offline. For example, assume the ransomware in question involves a zero-day attack and has no reputation score on file. In this scenario, VMware Carbon Black Cloud blocks the malicious binary execution based on its nefarious behavior. Any executable that injects code into legitimate running processes or spawns new child processes from packed memory buffers is clearly not benign.

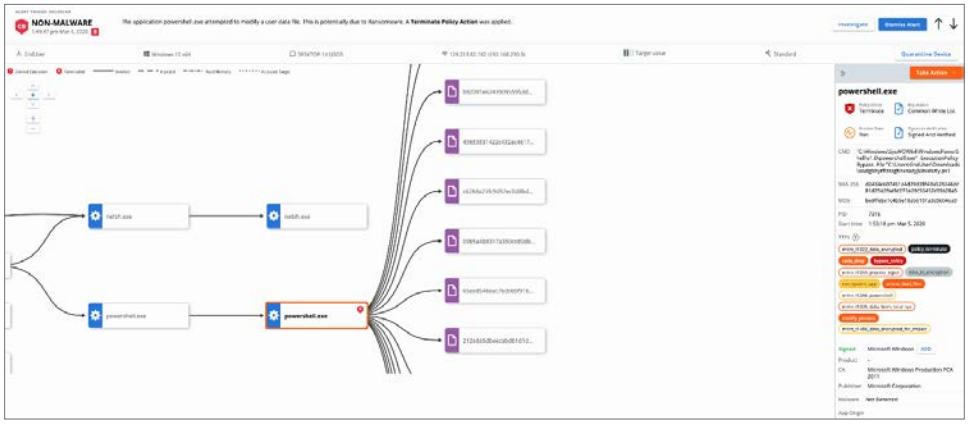

FIGURE 3: See all processes and how they're spawned.

Because our solution relies on patterns of attack rather than IoCs devoid of behavioral context, it has the intelligence necessary to reliably prevent the executable from attempts to phone home to its command and control server. Plus, it has full visibility into how the attack happened. With this insight, IT and SecOps teams can proactively patch relevant vulnerabilities, and use our suite of remediation tools to quarantine machines, block software and remove unwanted items.

Pro tip: With VMware Carbon Black® Cloud Audit and Remediation™, IT and desktop teams can run live queries against their entire endpoint ecosystem to validate that the ransomware outbreak is effectively mitigated.

Credential theft, abuse or misuse

With a valid set of credentials, attackers can accomplish much of their nefarious activity without raising a single alarm. That's why credentials are so often a popular target, particularly during the first stage of an attack. In the latest Verizon Data Breach Investigation Report, 29 percent of data breaches involved the use of stolen credentials.[7]

According to the 2019 IBM Security and Ponemon Institute Cost of a Data Breach study, the total average cost of a data breach is $3.92 million.[8] With this high of a price tag, it's rather astounding that something as simple as an administrative username and password guards against what could be an existential threat for many businesses.

Privileged accounts are the most valuable assets to an attacker. With a privileged account, an attacker essentially has the keys to the entire enterprise. They can create new accounts, modify existing ones to grant excessive privileges, and then delete any trace of their handiwork by zeroing out log files that record their activity.

If an attacker's goal isn't to steal corporate or customer data, they can still sell stolen credentials on the black market to someone whose goal is cybercrime and corporate espionage.

How does it work?

Often, phishing or spearphishing attacks are the ways that attackers gain access to credentials. Other methods include stealing credentials via SQL injection attacks, cross-site scripting (XSS), session hijacking or man-in-the-middle attacks against websites. Some of the most insidious credential attacks use native, authorized tools such as PowerShell so that the activity appears legitimate on the surface and avoids setting off any alarms.

Once an attacker has credentials on an endpoint, the next goal is to expand that privilege and move laterally across the network to find valuable data, such as sensitive customer data and corporate proprietary data, as well as escalate their privileges by compromising the domain controller and Active Directory database.

What you can do

Empower and educate. Each employee in the enterprise is an essential steward for cybersecurity. Make sure employees understand their role, and make it easy for them to protect credentials with password manager software, or obfuscate credentials completely using SSO. Multifactor authentication is another must-have for global enterprises, particularly those with employees connecting from everywhere and anywhere.

On a regular basis, review privileged domain accounts and their access to VIP domain accounts to assess whether these are required and serve a legitimate purpose to business operations. Because these credentials are the most attractive targets for an attacker, keep them closely watched and limited to as few as possible.

Pro tip: Carbon Black Cloud Audit and Remediation allows teams to run security configuration assessments on any aspect of an endpoint's configuration to verify employee compliance with corporate usage policies (e.g., use of password manager software). The same thing goes for domain controller configuration, making it that much harder for attackers to steal credentials.

Spot a stealthy attack, auto-block and tackle. Protecting and monitoring domain controllers and administrative accounts that have direct access to Active Directory is an essential part of stopping an attack before it can even begin.

7. Verizon. "2020 Data Breach Investigations Report."
8. IBM Security and Ponemon Institute. "Cost of a Data Breach Report." 2019.

VMware Carbon Black Cloud detects credential-stealing attacks that hide behind native, authorized applications such as PowerShell. Our event stream processing engine flags behavior that is inconsistent with what we expect to see on endpoints, even if the process is authorized. In this example, we see that PowerShell launches lsass.exe. Once compromised, this executable gives attackers full access to domain account credentials. Because this behavior is not expected and highly suspicious, VMware Carbon Black Cloud immediately blocks this action locally on the endpoint and sends an alert.

Collect forensic data, auto-update security policies. While the credential theft attack may be thwarted, it's still worthwhile to connect to the endpoint to investigate any additional exposure or attacker activity. Use VMware Carbon Black Cloud to isolate affected systems and remotely access them via secure shell to examine more closely, and implement any additional remediation steps.

VMware Carbon Black Cloud automatically collects and stores detailed forensic data so you can investigate the breach attempt and use this data to update endpoint security policies en masse. For example, if you discovered that the credential abuse involved remote access to an administrative account, you might consider adding a rule that allows remote access to administrative accounts only from an approved list of IP addresses or range of addresses.

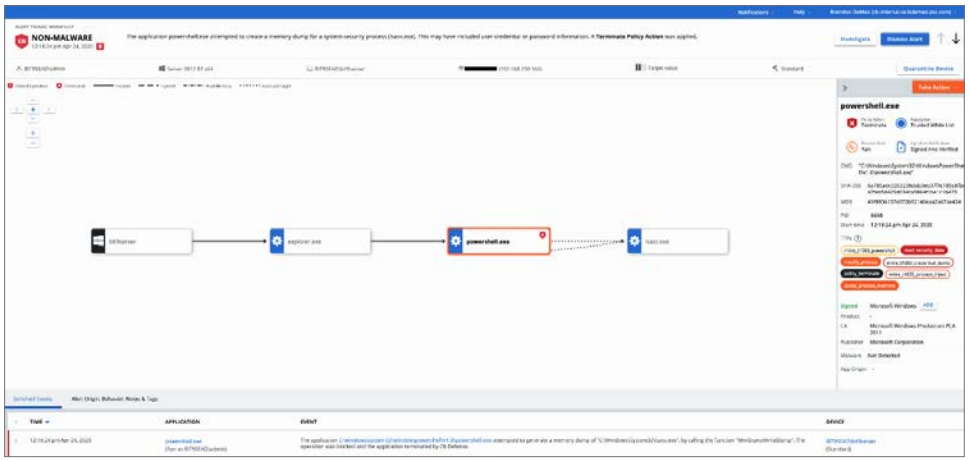

FIGURE 4: Examine process detail in depth.

Having detailed forensic data to review when investigating an incident provides critical accurate details about what occurred on the system. Leveraging a third-party audit trail of this activity ensures security teams have all of the data necessary to make an accurate decision in seconds about what exactly occurred and the scope of the incident. Without this level of an independent activity audit trail, one would often have to assume a larger scope, which can lead to overreporting.

Alternatively, forensic analysis may be leveraged to validate as close to possible what occurred. However, this is extremely costly, cumbersome, time-consuming and requires an extremely high skillset. Even then, forensic analysis often only provides a best guess based on snippets of evidence remaining on the host.

Phishing, spearphishing and other email-based attacks

Cybercriminals are a lot like any other kind of scammers or con men. They take advantage of crises, such as the COVID-19 pandemic, to trick their victims into taking action, and phishing is the perfect way to do it. While phishing tactics were used in 32 percent of the breaches covered in the 2020 Verizon Data Breach Investigation report[9], it's likely that number will be even higher in the 2021 report.

Even before the COVID-19 outbreak, phishing attacks were climbing and on pace to be at the highest level in the past three years.[10] Typically, credential theft is the goal of a phishing campaign, with attackers scamming employees to visit fake login pages to steal their credentials. However, attackers are stepping up their techniques by adding more sophisticated traps targeting employees working from home with fake mobile apps, fake COVID-19 maps and fake VPN software.

Spearphishing is simply a highly targeted version of phishing, often scamming VIPs such as corporate executives or board members using information gleaned from analyzing publicly available information (e.g., social media sites, newspaper articles, etc.) to make their messaging more believable.

How does it work?

Masquerading is a critical element in phishing and spearphishing attacks, and happens when the name or location of an executable—legitimate or malicious—is manipulated to evade defenses and detection. Whether it's a malicious email attachment masquerading as a benign one or a malformed Office 365 login page masquerading as a legitimate one, the goal is to get the user to click. Once the user clicks, the attacker has their chance to gain initial access.

Email attachments are commonly used for obtaining initial infection. Some of the attachment file types we've seen include files with the following extensions: ZIP, 7Z, TAR, RAR, JAR, VBS, IMG, GZ, EXE, ISO, SCR, RTF, PDF, DOC, XLS. The phishing emails often contain spoofed email headers and authentic messaging to lure the victim into a false sense of security. Additionally, phishers will use attractive attachment names to induce users to open them.

Once an attachment is opened, the underlying malware that's embedded within the document (e.g., a malicious Microsoft Office macro using VBA code) will execute. Another example the VMware Carbon Black Threat Analysis Unit has recently seen uses an ISO attachment containing a PE file that is posing as an SCR file. When it's executed, the PE file deploys RemCos. RemCos is a commercialized remote administration tool (RAT) known to be a well-maintained offering on the dark web.[11]

With remote access and a valid set of credentials, an attacker can do significant damage inside an organization, which makes detecting initial access and thwarting execution a priority for enterprises.

What you can do

Deputize employees. As with any social engineering attack, phishers take advantage of human nature—our curiosity as well as our unique ability to be easily distracted. Arm employees so they can profile a potential phish, encourage their skepticism and teach them how to spot these scams. For example, remind them that requests for personal information, usernames and passwords are never acceptable over email.

Encourage them to be wary of poor grammar, misspellings, broken links and images, and other characteristics that seem off in an email. Better yet, set up an email address they can send any suspicious emails to for further investigation **before** they open any attachments or click on any links. Consider implementing safe phishing simulations and training programs to measure and increase employee recognition of phishing and spearphishing attempts (e.g., Gophish).

9. Verizon. "2020 Data Breach Investigations Report."
10. Comparitech. "Phishing statistics and facts for 2019–2020." Sam Cook. February 7, 2020.
11. VMware Carbon Black. "Technical Analysis: Hackers Leveraging COVID-19 Pandemic to Launch Phishing Attacks, Fake Apps/Maps, Trojans, Backdoors, Cryptominers, Botnets & Ransomware." Jared Myers and Ed Murphy. March 19, 2020.

Unmask the malicious. Even if a user makes the mistake of opening a malicious attachment, or clicks on a fake login page and kicks off initial access for an attacker, all is not lost. For example, VMware Carbon Black Cloud will identify a malicious process masquerading as a legitimate one based on its behavior. Our platform captures and collects details on which parent processes spawned which child processes, enabling us to catch anomalous behavior and stop a phishing attack in progress.

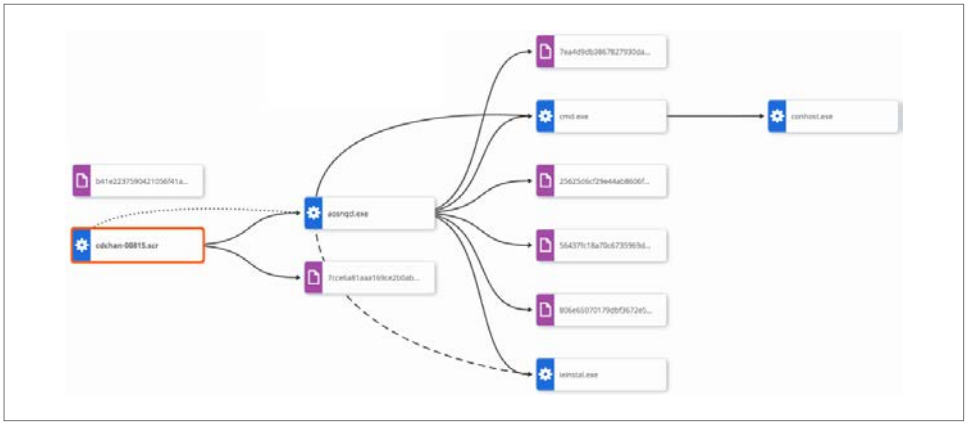

FIGURE 5: Discover malicious behavior.

Pro tip: VMware Carbon Black® Cloud Managed Detection™ extends enterprise security teams by offering advanced alert monitoring and threat triage to notify you of any threats that could expose your business to phishing or spearphishing risks.

Fool me once. That's all, folks. Once the phishing attack or spearphishing has been thwarted, it's essential to be able to recognize it (or something similar) in the future. Carbon Black Cloud Enterprise EDR collects and visualizes detailed information about attacks targeting endpoints, making root-cause analysis easier than ever before. The VMware Carbon Black Cloud behavioral analytics engine automatically analyzes the attack behavior and ensures all customers' endpoints globally are then protected from this specific behavior going forward. This protection profile is extremely effective because preventing these attacks based on behavior requires the attackers to come up with a whole new attack technique on their next attempt. Alternate methods of prevention commonly rely on very brittle indicators of compromise that are incredibly easy to change, such as malicious file hashes, hostnames, IP addresses and registry keys. Additionally, VMware Carbon Black Cloud allows you to easily build custom watchlists to be alerted any time a similar attack is launched again.

For example, if we've seen that a RAT such as RemCos will install itself and initiate a connection to an IP address in Iran, we can set up a watchlist to alert us, and block it when it happens again.

FIGURE 6: Rich details support investigations.

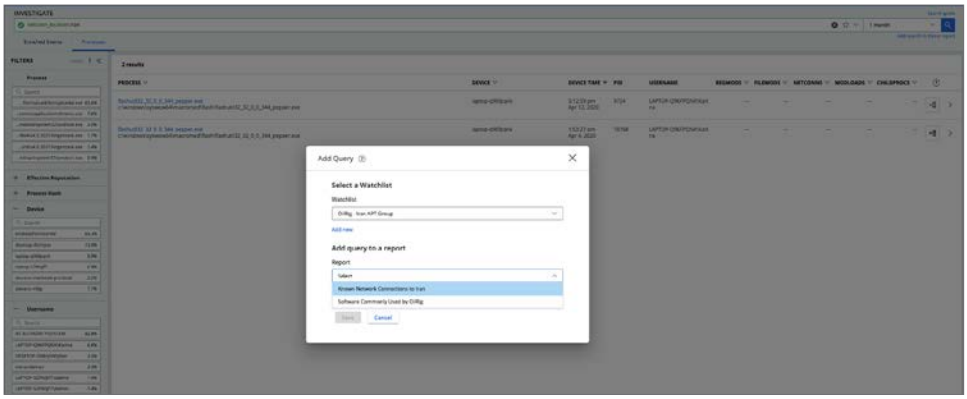

FIGURE 7: Setting up custom watchlists.

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *carbonblack.com/trial*.

For more information or to purchase VMware Carbon Black products, please call 855-525-2489 in the U.S. or +44-118-908-2374 in EMEA.

For more information, email *contact@carbonblack.com* or visit *carbonblack.com/epp-cloud*.

Summary

Enterprises are climbing an uphill battle when it comes to fighting against cybercriminals. Saddled with old, burdensome technologies that fail to mitigate sophisticated attacks and blended threats, teams need a new way forward. One that maximizes shrinking teams and budgets, easily integrates with existing technologies and workflows, and delivers reliable security at each and every control point in an enterprise.

Intrinsic security from VMware Carbon Black does precisely this.

As a leader in cloud native endpoint protection, we're dedicated to keeping the world safe from cyberattacks. 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.

While other endpoint security products only collect a data set related to what is known bad, VMware Carbon Black Cloud continuously collects comprehensive endpoint activity data and analyzes attackers' behavior patterns to proactively stop cyberattacks before attackers can unleash chaos.

By zeroing in on these anomalies quickly, security teams gain visibility, quickly uncover the root causes of attacks, and take action.

With a vibrant user community and a vast integration ecosystem, including open APIs, developer tools and documentation, you'll be well supported when setting our platform up in your environment.

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