GET STARTED

The Future of Remote Work: Securing a Distributed Workforce

Introduction

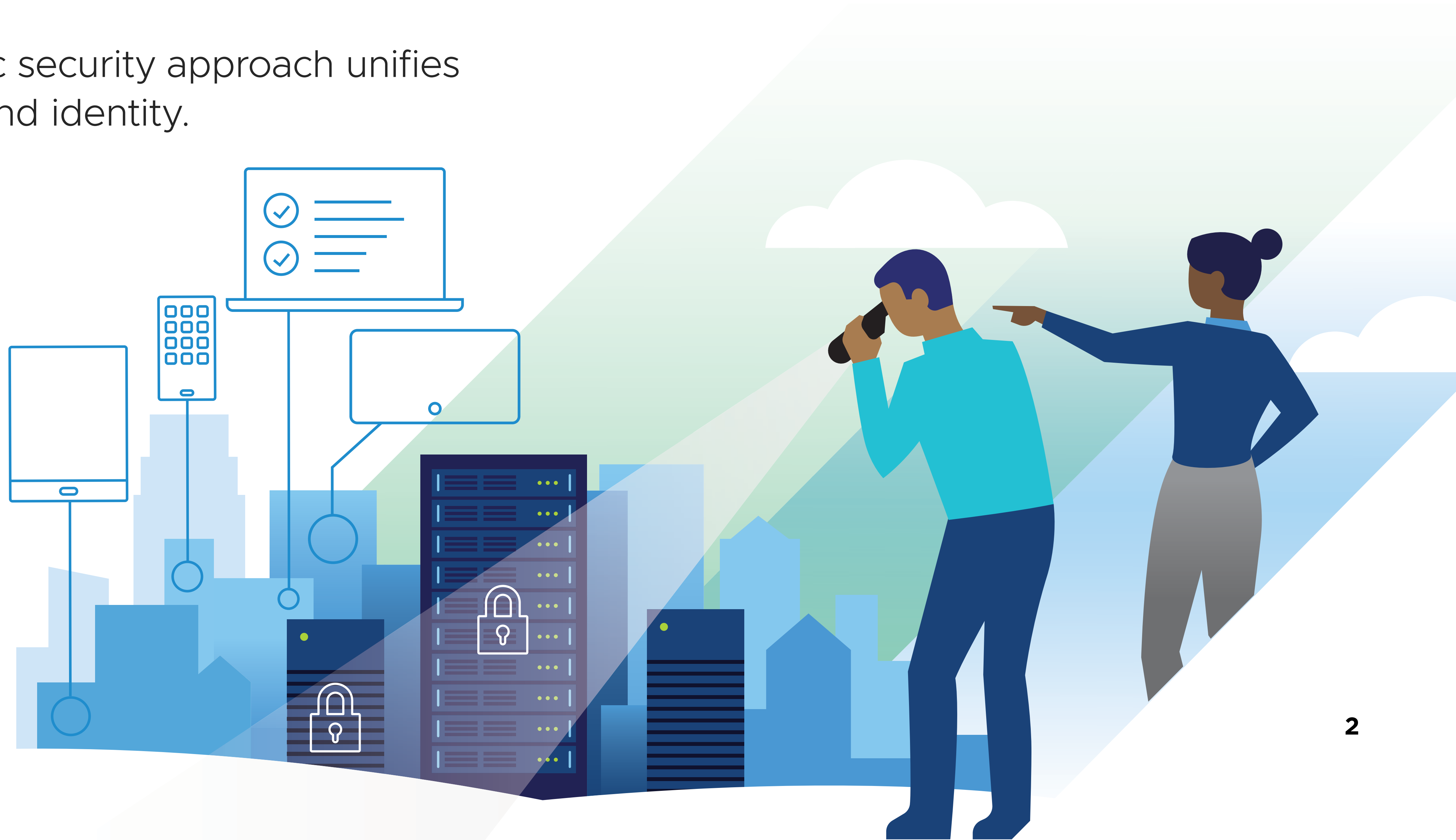
Global events, such as COVID-19, compel enterprises to find new ways to get work done. Whether it's innovating service delivery to their customers or entertaining workforce flexibility, enterprise leaders are becoming more comfortable with change. For example, nearly all non-essential employees are now working remotely, and this trend is likely to continue.

The challenge is in securing a varied and disparate workforce. Many IT security pros rely on a suite of tools to monitor and secure access to corporate data, yet still lack the unified visibility and control needed to prevent, detect and respond to threats. All of which adds to the complexity and urgency in deploying an effective defense.

To support a vastly disparate and distributed workforce, IT teams are best served by looking for consolidation opportunities. Reducing the number of tools and vendors they work with can simplify workflows and help teams operate more quickly and effectively.

VMware Carbon Black Cloud™ offers this consolidation opportunity. Our cloud native, intrinsic security approach unifies security across all control points in an organization: endpoints, workloads, clouds, networks and identity.

Between February 4, 2020 and April 7, 2020, VMware witnessed an estimated 70 percent increase in remote work.[1] While no one knows for certain, remote work may likely become the norm for most enterprises.



[1] VMware Carbon Black. "Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted." Patrick Upatham and Jim Treinin. April 15, 2020.

An intrinsic security approach provides the context you need to strengthen security and the unified, automated tools to manage all security factors. This approach allows organizations to:

Broaden cybersecurity visibility and control

Go beyond the limitations of an HQ context and the constraints of technology silos. Unify monitoring across enterprise control points, so your defense is as cohesive and intentional as an attacker's is.

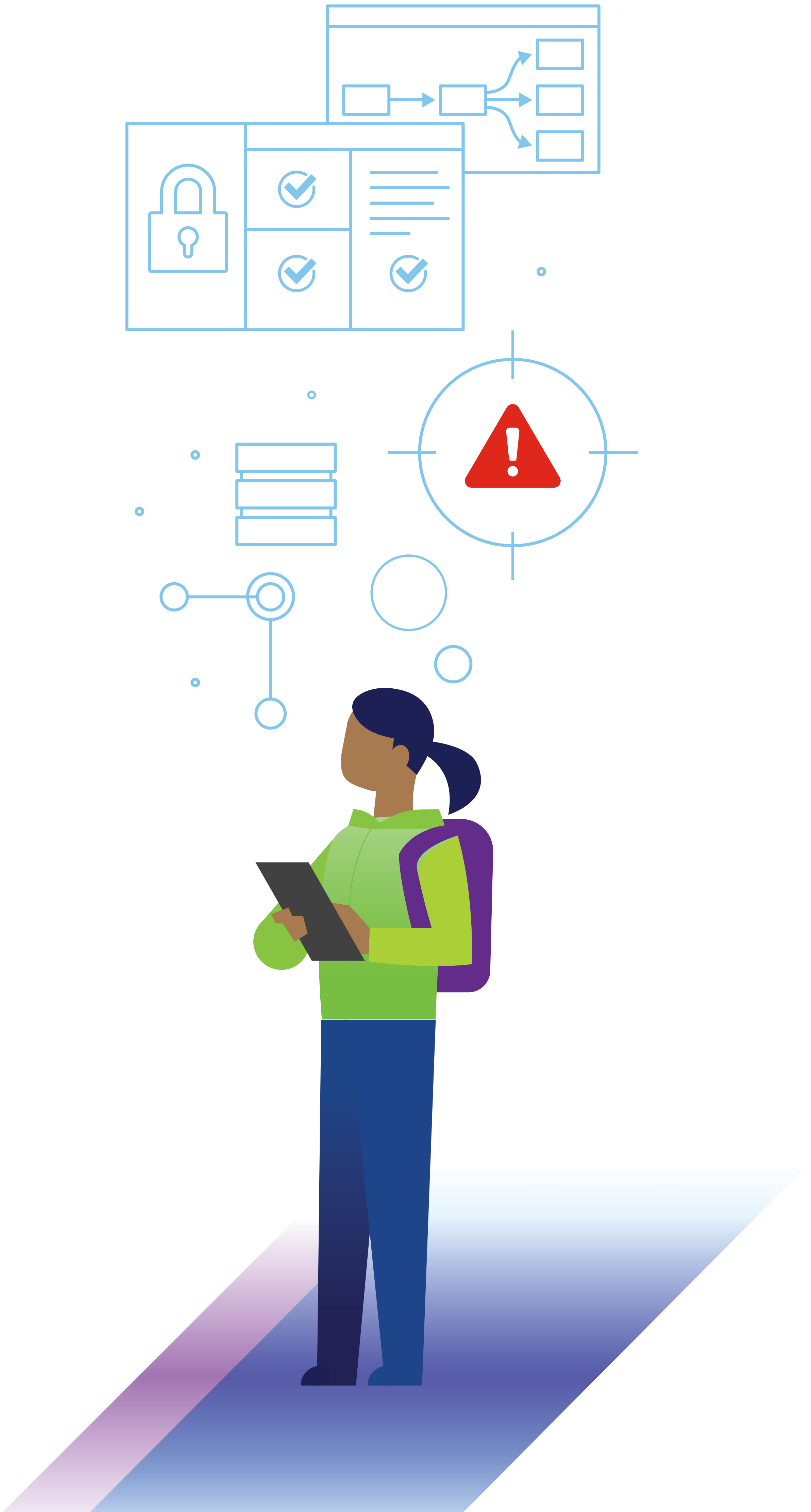
Deepen cybersecurity analysis

Go beyond the surface to identify nefarious, stealthy activity that is often missed by traditional, non-cloud native, legacy/on-premises tools.

Extend cybersecurity countermeasures

Integrate with existing security tools and processes for fast, automated and orchestrated workflows that are easier to implement for a distributed workforce.

This e-book offers IT and security pros a one-stop shop for everything you need to know about workforce security, so your users (and you) stay safe while working remotely. After all, the easier you make it for employees to do the right thing, the better the outcome.



The new normal means (a lot more) new threats

COVID-19 has created the perfect opportunity for a cybercrime spree.

In addition to witnessing a huge spike in ransomware attacks, our Threat Analysis Unit (TAU) has reported that attackers are using COVID-19 to launch phishing attacks, fake apps and maps, trojans, backdoors, cryptominers and botnets.[2] To acclimate to the new normal, it's essential that we arm ourselves with the latest threat intelligence.

Cyberattackers take advantage of chaos by adding to it. And they use disinformation and deception to lay their traps. An organization workforce's natural reactions to any crisis—distraction and division—become accelerants for the attacker/arsonist's cyber fire. Knowing how they work their dark magic can help you better protect your remote workforce.

The following table explains how bad actors often take advantage of bad news.

[2] VMware Carbon Black. "Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted." Patrick Upatham and Jim Treinin. April 15, 2020.

The cyberattack playbook: How bad actors take advantage of bad news

	Method	How it works	Examples
Tactic	Disinformation	During a crisis, having reliable and accurate information is a matter of life and death. Cyberattackers post tons of fake data about the crisis to attract unsuspecting victims and commit crimes against them, or their employers.	Fake domains for the CDC, FEMA, NIH and more are used to set up bogus COVID-19 apps and/or testing sites that contain malicious code. Fake stimulus check websites can steal credentials, private consumer data and taxpayer money. Similarly, fake testing websites are designed to collect personal information, such as Social Security numbers, credit card information, medical data and other private information, that can be sold on the dark web as identity theft opportunities.
	Deception	Even before COVID-19, stealthy attacks were on the rise. Masquerading as a legitimate user or process (e.g., PowerShell) can allow an attacker to do their dirty work under the cover of darkness (and bypass traditional security tools at the same time).	Social engineering attacks (posing as a trusted supplier, partner, governmental official or expert) send texts with malicious links to remote employees. Phishing and spear-phishing campaigns take advantage of consumer anxiety. Process injection attacks hide malware under the address space of legitimate, authorized programs and trusted protocols.
Accelerant	Distraction	Employees are learning how to balance work life with home life responsibilities, such as juggling child care, elder care, and care for the disabled. Trying to stay focused on work activities, which can stretch into evening and weekend hours, can add to feelings of increased anxiety and distraction. Cyberattackers use all of this to their advantage.	Easily distracted victims are much easier to trick. Changes in employee behavior and activity patterns may complicate traditional security monitoring efforts. Attackers know this and have escalated their disinformation and deception efforts to target remote employees and contractors at large global enterprises (that’s where the money is, after all).
	Division	With more than 40 million people filing for unemployment in the U.S., bitterness and resentment among the ranks is inevitable. Cyberattackers exploit these divides by preying on concerned, about-to-be-laid-off employees who can escalate their privileges before they walk out the door. After all, selling their credentials on the dark web might be seen as their only ticket out of a vulnerable financial future.	Authorized credentials give attackers the backdoor access they need for a virtual home invasion. There’s no need to break down the door or trigger any alerts. When posing as a legitimate remote employee, a cyberattacker can move laterally across a network, compromise a domain controller, gain administrative access, and essentially own the environment. Exploiting the division between an employee and their employer sets up a cyberattacker for success.

Remote workforce risks and rewards

Many executive teams are now voluntarily considering more flexible workforce relationships after experiencing the benefits a remote workforce can provide. Whether your organization has embraced long-term remote working setups or not, we've outlined the three most common risk scenarios that might impact your remote employees, and what you can do about them.

Scenario 1: — Deception and disinformation converge: COVID-19 phishing scams target remote employees

What it is – Whether it's an email offer for a medical breakthrough, a new vaccine, a charitable donation request or an exciting new investment, chances are it's a scam. In February 2020, the FTC started warning consumers of all of these dangers and provided *guidelines* that remote employees can use to stay aware and remain skeptical.

How it works – As with other phishing scams, the goal is to appear legitimate enough to fool the victim—often a remote employee—to download an attachment, click a malicious link, or log in to a bogus site using their corporate credentials. The latest scams are more sophisticated in how they exploit an endpoint once they gain initial access. Designed to reside in memory and use authorized applications to launch, the malicious code executes without being blocked by traditional antivirus (AV) or setting off any security information and event management (SIEM) alerts.

What to do about it – In addition to training employees how to identify phishing scams, organizations are encouraged to deploy next-generation antivirus (NGAV) and endpoint detection and response (EDR) technologies, such as VMware Carbon Black Cloud. So even if an employee is tricked by a phishing scam and the malware initiates, our solution will detect these process injection attacks by analyzing system behavior, and shut it down. The power of our solution remains in our ability to recognize what appears to be innocuous on the surface but is actually highly dangerous. Additionally, using cloud native technologies such as VMware Carbon Black Cloud ensures continuous coverage no matter where your employees live.

Scenario 2: The dangers of island hopping: Threat actors unleash proximity attacks via smart devices

What it is – Island hopping is when cybercriminals creep into enterprises at their most vulnerable points, and then hop to higher security sections of the network. With most employees working from home, each home network has now become part of the corporate environment, making island hopping much easier for attackers and much harder for defenders to prevent, detect and stop.

How it works – Let's face it: Home networks are much more porous than corporate ones. Smart devices, personal devices used by children and other family members, gaming systems, and home routers likely have insecure configurations, default passwords, outdated firmware, and a myriad of other vulnerabilities—all of which provides the perfect opportunity for attackers to gain access via these devices. Once in, an attacker hops—launches a proximity attack—from a smart device to your remote employee's workstation.

What to do about it – Encourage your employees to isolate their work devices from the rest of their home networks. Most home routers can be configured to support more than one network, so provide detailed instructions on how to do this, or consider provisioning secure home routers to high-risk, high-value employees such as executives or other VIPs. At the very least, ask them to dedicate a digital safe room where they can go for sensitive conversations regarding corporate strategy, customer negotiations or other company secrets.

According to the VMware 2019 Global Incident Response Threat Report, more than 40 percent of attacks targeted victims via island hopping.[3]

PRO TIP

Make sure your endpoint security platform can detect behavior patterns consistent with attacker persistence and lateral movement. VMware Carbon Black Cloud detects these behaviors and auto-quarantines infected systems before attackers can make their next hop.

[3] VMware Carbon Black. "Global Incident Response Threat Report." November 2019.

Scenario 3: Disinformation targets the distracted: Cybercriminals embed malware in COVID-19 apps and maps[4]

What it is – Anxious employees working from home are hungry for the latest information about COVID-19, making them easy targets for disinformation. Whether it’s a fraudulent coronavirus map modeled on the Johns Hopkins site or a bogus real-time disease tracking app infected with malware, attackers leverage the distraction of worried remote employees. Promises of scanning the area and notifying employees of nearby COVID-19 cases is enough to fool victims into installing an infected app.

How it works – In a recent attack, criminals repurposed malware from 2016 called AZORult and inserted it into a fake coronavirus map. When a web visitor navigated to this map, AZORult stole their browsing history, cookies, credentials and cryptocurrency, and also downloaded additional malware.[5] A particularly nefarious variant even creates an administrator account on the new machine to enable Remote Desktop Protocol (RDP) and maintain persistence on the system. Another example involves an Android app called COVID Tracker, which installs CovidLock ransomware and automatically locks the victim’s phone until they pay the $250 bitcoin ransom.[6,7]

What to do about it – Maintain consistent communications and provide timely updates and advisories to your workforce regarding COVID-19 safety, with reminders on how to avoid becoming cybercrime victims. For example, it’s far better to navigate directly to official public health sites, such as the *World Health Organization*, as opposed to clicking a link. Additionally, invest in NGAV, EDR technology and threat intelligence to identify malware such as AZORult before it gains a foothold. Finally, consider implementing a threat hunting program so that IT teams can find and fix insecure browser

PRO TIP

With VMware Carbon Black® Cloud Audit and Remediation™, threat hunters can proactively search for vulnerable configurations and other exposures across all your endpoints, so you can implement fixes before becoming the next malware target.

[4] SecurityWeek. “Security, Privacy Issues Found in Government COVID-19 Mobile Apps.” Ionut Arghire. April 8, 2020.

[5] VMware Carbon Black. “CB TAU Threat Intelligence Notification: Common to Russian Underground Forums, AZORult Aims to Connect to C&C Server, Steal Sensitive Data.” Swee Lai Lee. September 24, 2019.

[6] The Hacker News. “Beware of ‘Coronavirus Maps’ — It’s a malware infecting PCs to steal passwords.” Wang Wei. March 11, 2020.

[7] Nokia. “A growing cyber threat linked to COVID-19.” March 2020.

Q&A with Tom Kellermann

Q: You've shared with us that cyberattacks have evolved over the past several years—moving from burglary to home invasion—in terms of how attackers use a company's own infrastructure against them. Can you describe this in more detail? What are some examples?

TK: Cyberattackers have become increasingly more punitive, more brazen and more destructive. No longer content to steal data, secrets and monies, attackers are now colonizing corporate infrastructure. They embed themselves within the infrastructure as part of an enterprise's digital transformation efforts, and corrupt the infrastructure by using it to attack an enterprise's customers, partners and board members.

These attacks can manifest in three forms:

1. Your corporate network begins attacking visitors and your users.
2. Your website or mobile application becomes a watering hole, and it begins to attack visitors and users.
3. Hackers take over your mail server, known as a reverse business email compromise.

And not only are they reading all of your mail, but they're sending out select emails to your board members, investors, your most important partners and customers, and these emails are laden with malware. You can see that these destructive attacks go well beyond traditional cyber risk management, and can potentially destroy an enterprise's brand reputation.

Tom Kellermann is the head of cybersecurity strategy for VMware. Tom serves as the Wilson Center's Global Fellow for Cybersecurity Policy and sits on the Technology Executive Council for CNBC. In 2008, Tom was appointed a commissioner on the Commission on Cybersecurity for the 44th President of the United States.

Q: How can executives and IT security teams best respond to these destructive attacks, especially when working remotely?

TK: To really solve this, it’s imperative that the voice of the CISO be heard at the highest levels. Also, proactive cyberthreat hunting must happen because it can discern if there are any criminals already inside the network and operating within the environment. The bottom line is that controls and limits need to be put in place. Much like adding doors and installing locking mechanisms inside your house, use network micro-segmentation to limit what a remote worker has access to, which also limits an attacker’s ability to traverse across network segments. Follow the philosophy of just-in-time administration and limit administrative access as much as possible—no one needs perpetual administrative access ever.

Another good practice is to ensure you have the capacity to run a health check across all of your IT assets to ensure that they’re not sick or making the rest of your corporate IT assets sick, for that matter. Next, increase visibility across all of your remote users to ensure that no one has broken into their laptops and used them to move laterally into your organization. And that’s only achieved through deploying EDR, which is like a motion-sensitive surveillance camera in that when a behavioral anomaly is detected, it alerts the security team to go out and halt the crime in progress.

The five C's of workspace security: How to embrace the new normal

Along with frequent hand-washing, social distancing has become a common best practice to reduce the risk of infection. Digital distancing is a best practice we recommend to reduce the risk of cyber infection now that the majority of us are working from home.

As the name indicates, digital distancing means that within our home environment, our work devices should not be on the same network as our smart devices, our children's devices, our spouse's devices, or any devices we use for recreational or personal purposes. If you wouldn't have plugged it into the office network before COVID-19, it needs to reside on a network separate from your work device.

In addition to digital distancing, consider the following framework as a way to manage the risks inherited in this new age and new normal.

BOTTOM LINE

To reduce the spread of cyber infection and/or attack, devices for different functions need to be completely isolated and digitally distant from each other.

PRO TIP

Make sure your employees know how to segment their home networks, and offer user-friendly self-service options for those who don't have the skills or tools to implement digital distancing at home.

Cloud – Prioritize cloud native technology and service providers

Now more than ever, the cloud is essential infrastructure. Whether a public cloud such as AWS or Microsoft Azure, or a private cloud powered by VMware technology, most of the world's organizations rely on cloud computing to get business done. Cloud native security technologies have an edge when it comes to securing remote employee access and workspaces. Rather than trying to adjust to supporting remote employees by figuring out how to architect an on-premises solution in the cloud, VMware has been there all along.

> "By consolidating [our] security products, we'll be able to eliminate at least three servers and all the overhead that goes with it."
>
> WILLIAM BOCASH, IT MANAGER, STONEWALL KITCHEN

Context – Focus on context as opposed to threat

Threat indicators, such as file hashes and other indicators of compromise (IoCs), are extremely helpful for threat hunters and other security operations center (SOC) personnel to track down attacker activity. Even focusing on one step in a process offers little for defenders to go on when prioritizing incident response efforts. Having the full context of a process sequence as well as granular details of how endpoints are configured is essential. Today, cyberdefenders risk wasting their time on hunting down false positives or miss subtle signals that become more meaningful when viewed in totality. VMware Carbon Black Cloud collects more than 1,500 characteristics on every endpoint in the enterprise and records all activity, including which processes get launched and by which parent binaries, enabling us to identify deceptive attacks missed by traditional technologies.

> "VMware Carbon Black Cloud Endpoint™ Standard tells me exactly what happens when it happens. I no longer need to chase after unnecessary reports or logs."
>
> JOE MRAZIK, NETWORK ADMINISTRATOR, KAAS TAILORED

Convenience – Complex power under the hood, yet simple for users

In today's cyberthreat landscape, the nitty-gritty world of threat intelligence and endpoint security can become quite complex. The challenge is that if any security control is too complicated, cumbersome or even too noticeable to users, and they think it gets in the way of their job, they'll find a way to bypass it. Deployed in minutes, the VMware Carbon Black Cloud lightweight multipurpose agent uses less than 1 percent CPU on average. With VMware Carbon Black Cloud, IT teams can establish secure remote access to employees' workstations whenever they need to troubleshoot an operational issue, and SOC team members can remotely detect, investigate and resolve security incidents. Our technology makes it easy for employees to be secure, whether they're using their own devices or corporate-owned ones.

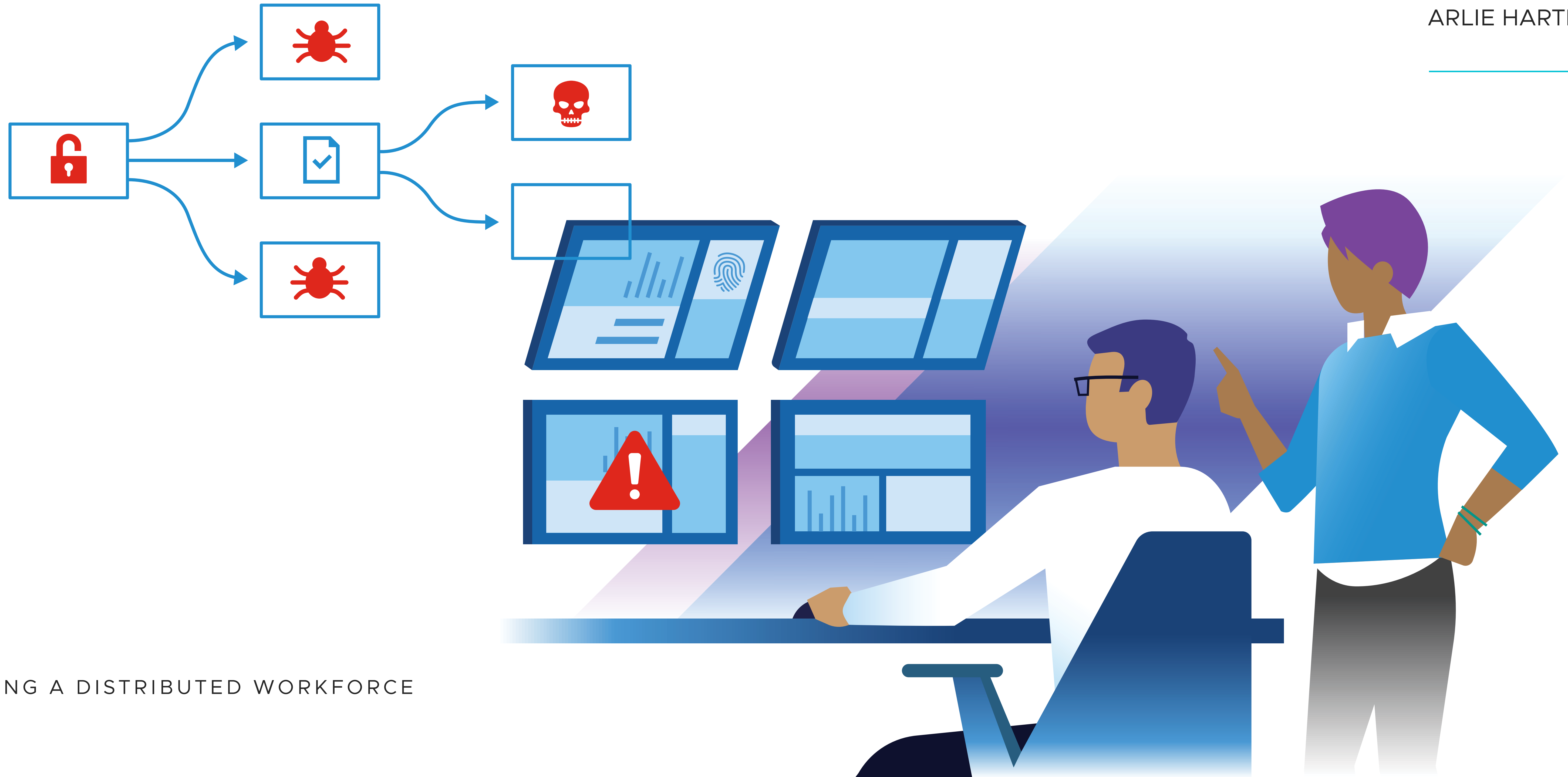
> "Carbon Black Cloud Endpoint Standard is easy. Through a single cloud portal, you can manage everything in one of two clicks—simple as that."
>
> ISANKA ATTANAYAKE,
> MANAGER IT INFRASTRUCTURE,
> ROYAL CERAMICS LANKA

Coordination – Unified intelligence across the enterprise, plus community-sourced

Every organization's IT security team is charged with securing their corporate apps and data via five key control points: endpoints, workloads, clouds, networks and identities. Remotely coordinating countermeasures across all five control points is tough. That's why intrinsic security is your best bet for spotting (and stopping) threats against your remote employees. Additionally, the VMware Carbon Black User Exchange supports community coordination by providing a real-time forum where practitioners can share the latest threat intelligence indicators; adversary tactics, techniques and procedures (TTPs); and watchlists.

> "VMware Carbon Black has been a nice change of pace compared to the other security companies I've worked with…and thanks to the User Exchange Community, I have a lot more confidence to start tuning the product and elevate our maturity with the tool."

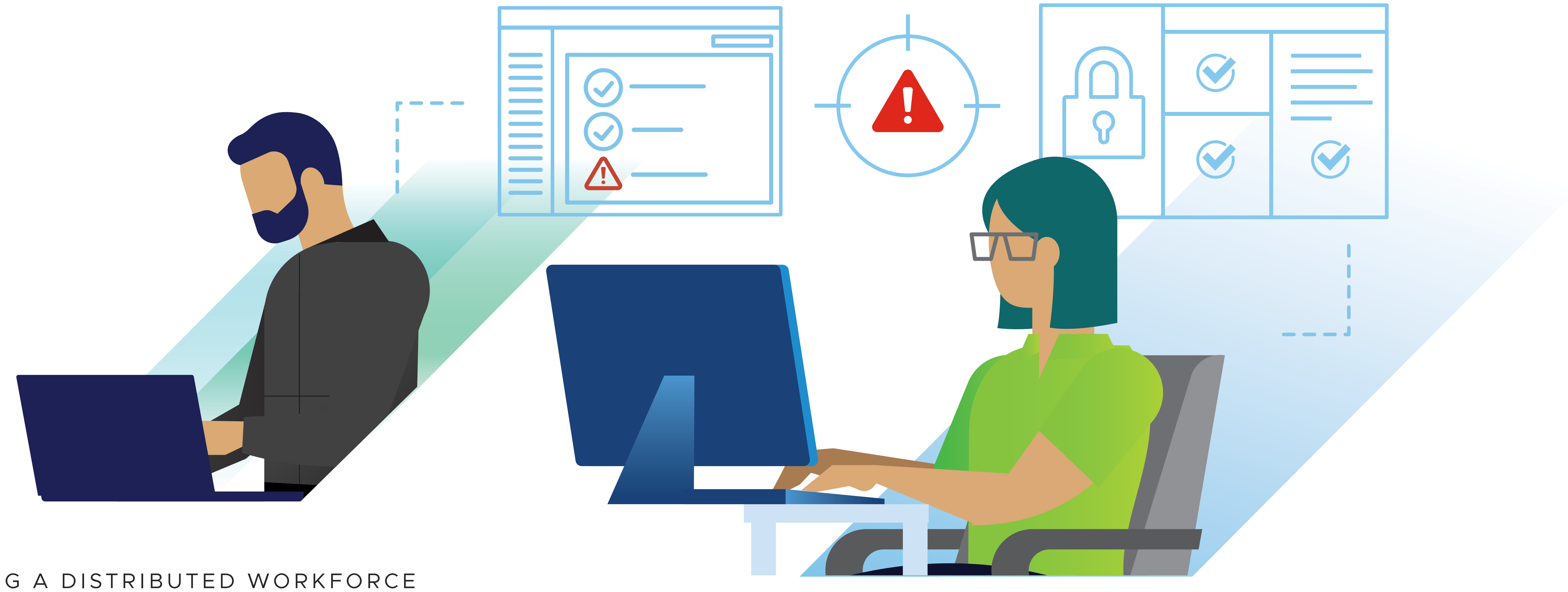
ARLIE HARTMAN, CISO, BRAUNABILITY



Cohesion – Remove blind spots with a cohesive defense

In too many organizations, teams and technologies are completely walled off from each other. These silos impede efficiency across the enterprise, allowing attackers to exploit gaps in your infrastructure. Now that IT and IT security teams are working remotely, having a cohesive, unified defense is even more vital for secure remote worker access. VMware offers teams a unified set of solutions that gets rid of agents and appliances, so organizations can move from a threat-centric model to one that is broadly context-rich. After all, context transcends the threat, and this broader perspective enables teams to examine the full scope—the applications and the infrastructure behind each application to truly understand what it is that they are protecting.

> "One of the biggest benefits of adopting VMware is how all of the solutions integrate together so seamlessly. With just a click of a button, solutions start working together to give us the compliance and performance we need."
>
> DANIEL CABAN, DIRECTOR OF INFORMATION TECHNOLOGY, OSCEOLA COUNTY SHERIFF'S OFFICE



Building business resilience and continuity

There's nothing like a major global crisis to help businesses realize what's important. In addition to learning very quickly how essential it is to secure a remote workforce, businesses are also gaining valuable lessons in the virtues of business continuity and resilience.

Take advantage of the opportunity that the moment has offered the world to review, assess and enhance your business continuity plans.

> "People only accept change if needs must, and only see needs when in crisis."
>
> JEAN MONNET

Top 6 tips for updating your business continuity plan in 2020

1: Assess risks and their impacts

Expand your aperture beyond the immediate moment. Whether it’s a natural event (such as a hurricane, fire or flood) or an operational one involving a myriad of possibilities (espionage, fraud, operational or procedural failure, cyberattack, liability or supply-chain issue), evaluate their impacts on your company’s bottom line.

For each risk scenario, evaluate the estimated costs associated with each impact, as well as consequences that aren’t as easy to quantify yet remain important, such as brand reputation, employee loyalty and/or consumer trust. Identify areas of weakness for each scenario or risk category, and create an action plan to mitigate these risks.

Document your team’s ability to address each risk scenario by listing and evaluating the effectiveness of any tools, technologies and processes in place to prevent the scenario or minimize its impacts.

2: Clarify and communicate team roles and responsibilities

Knowing who needs to do what, when and where is fundamental, especially during an emergency. Assess your current business continuity plans and procedures to determine if there are well-defined roles and responsibilities, or if clarification is required. Clear lines of command are essential during emergencies, so educate staff on who to listen to, how to implement emergency procedures, where to go for more help, and what is required of them and why.

Communicate clearly and on a consistent basis to customers, employees, suppliers and partners. Make sure that employees remain vigilant and are aware that scammers will often show up during critical moments to take advantage of their distraction.

3: Secure, scale and stabilize access to systems-of-record applications

During any crisis, business leaders need reliable access to the data that will help them make the right decisions. This data is housed in systems-of-record applications that need to be securely accessed from anywhere, at any time. Additionally, business leaders use a variety of devices to access these apps, so it’s essential to extend the scope of what IT secures and manages to include corporate-owned and personal devices. Finally, consider how to stabilize network quality of service for remote employees, particularly those in IT who secure and maintain the infrastructure.

4: Modernize applications and embrace cloud-based flexibility

The hybrid cloud computing model can offer your business the ability to accelerate application delivery, and enable you to share service delivery responsibility with your infrastructure partners. Consider shifting to an as-a-service model to help your business remain nimble during any event that impacts operations.

5: Practice response plans to improve resilience

Improve your team’s business resilience by running through various risk scenarios with structured run-throughs, table-top exercises, and other business continuity practice tools. Document any hiccups or other lessons learned during practice exercises, so you can tweak action plans as needed. Practice sessions not only improve an individual team member’s skills, they can also build team cohesion, coordination and connection.

6: Consider establishing remote work programs

Every emergency presents an opportunity to rethink how business gets done. Yesterday’s lesson learned may become tomorrow’s standard operating procedure. Consider if an intentional remote workforce strategy makes sense for your enterprise.

55 percent of U.S. workers say their industry can succeed when most or all of the staff are distributed, according to the latest LinkedIn Workforce Confidence Index.[8]

[8] LinkedIn. “As remote work sweeps the U.S., 55% say it can succeed in their industry.” George Anders. May 13, 2020.

Summary/next steps: What now?

Whether a remote workforce is temporary, optional or an exception to the rule for a select few, you still need full visibility and control over any threats that may impact operations. VMware Carbon Black Cloud enables teams to identify risks and prevent, detect and respond from a single platform by increasing visibility into an organization’s devices and workforce, from anywhere.

VMware Carbon Black Cloud empowers your business to not only continue as it previously did, but do so swiftly and with more agility than ever before. Our cloud-based platform and single lightweight agent are deployed easily and quickly, ensuring remote employees as well as SOC team members are onboarded as soon as possible. By moving to VMware Carbon Black Cloud, you equip your IT and security teams to thoroughly protect and support a distributed workforce.

The Global Workplace Analytics 2020 estimate is that about 75 million U.S. employees could work remotely at least part of the time, representing 56 percent of the workforce.[9]

Resources

Federal Trade Commission scam alerts

ZDNet: “Contact tracing apps unsafe if Bluetooth vulnerabilities not fixed”

American Psychological Association: “The future of remote work”

[9] Global Workplace Analytics. “How Many People Cloud Work-from-home.” March 2020.

About VMware

VMware software powers the world’s complex digital infrastructure. The company’s cloud, app modernization, networking, security and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit *vmware.com/company*.

Join us online:

vmware®

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

Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 563562aq-ebook-future-rmt-wrk-en-us-1080p 7/20