Geek-to-Guru Guide:

OFFENSIVE NETWORK SECURITY

KEYSIGHT TECHNOLOGIES

INTRODUCTION

“Good Enough” is Not Enough

When it comes to network security, “good enough” is not enough. With a world full of bad actors hammering at your digital door, you need to fight back and meet them head on. That means hacking yourself to find and fix vulnerabilities — before an attacker can exploit them.

As you read through this guide, you’ll discover the benefits of taking an offensive approach to security. Whether you’re looking to stop configuration drift, stay ahead of the latest attacks, or prevent misconfigurations from jeopardizing your network, you’ll get the insights you need to take control of a rapidly changing threat landscape.

CHAPTER 1

Be Your Own Worst Enemy

Why an Offensive Approach to Security Is Nonnegotiable

Page 3

CHAPTER 2

What is Breach and Attack Simulation?

Tech Tips with Packet Boi

Page 7

CHAPTER 3

Take Five

Keysight’s CISO Discusses Cybersecurity’s Past, Present, and Future

Page 9

CHAPTER 4

Uncertainty Is the Enemy

Three Reasons Your Network Isn’t as Secure as You Think

Page 14

CHAPTER 1

Be Your Own Worst Enemy

Why an Offensive Approach to Security Is Nonnegotiable

There's a world of bad actors hammering at your digital door. There's only one way to be sure you're secure: you need to fight back against attackers and take an offensive approach to network security.

CHAPTER 1

Be Your Own Worst Enemy

Why an Offensive Approach to Security Is Nonnegotiable

There's a world of bad actors hammering at your digital door. You've invested in an array of network security tools, and your enterprise security team works tirelessly to fend off attacks. But configuration drift is a persistent, latent threat. After a steady stream of patches and updates, it's hard to know if your network, applications, and data are still as safe as they were the day those tools went live.

With so much at stake, do you want to wait for attackers to point out your vulnerabilities? After all, they only have to be successful once. You, on the other hand, had better succeed every single time.

There's only one way to be sure you're secure: you need to fight back against attackers, and take an offensive approach to network security.

Hack Yourself — or Others Will Do It for You

You know how persistent and clever your attackers are. So flip the script and make the first move. Using a breach and attack simulation (BAS) platform such as Keysight's Threat Simulator, you can safely simulate attacks on your production network to uncover weaknesses and vulnerabilities. These tools use the trusted MITRE ATT&CK framework to simulate malware campaigns, spear phishing, data exfiltration, cross-site scripting, database exploits, advanced persistent threats, and more.

By performing automated assessments, you can continuously test your security solutions against a wide range of threats — right on your production network. Should your security solutions fail to mitigate a simulated attack, your team will be the first to know.

Prevent Attacks Before They Happen

Finding problems is easy. Fixing them is harder. Your team doesn't need to waste cycles researching fixes — it needs step-by-step instructions to remediate problem areas quickly.

Fortunately, a good BAS solution can help you cut through the clutter. Look for tools that provide detailed directions to remediate any gaps, misconfigurations, or vulnerabilities you find. Whether you need to deploy a patch on your next-generation firewall, enable new functionality on your intrusion prevention system, or install a new tool altogether, these kinds of product-specific, step-by-step instructions can help you optimize your architecture and strengthen your cyber defenses.

Think Like the Enemy

The threat landscape is in a constant state of flux. New attacks and exploits emerge every day. It's easy to miss something and not even know your network is at risk. That's why it's so important to make sure your BAS tools are plugged into a continuously updated threat intelligence feed. Otherwise, you won't be able to test your defenses against the latest attacks, find out whether you're vulnerable, or close any gaps before bad actors can exploit them.

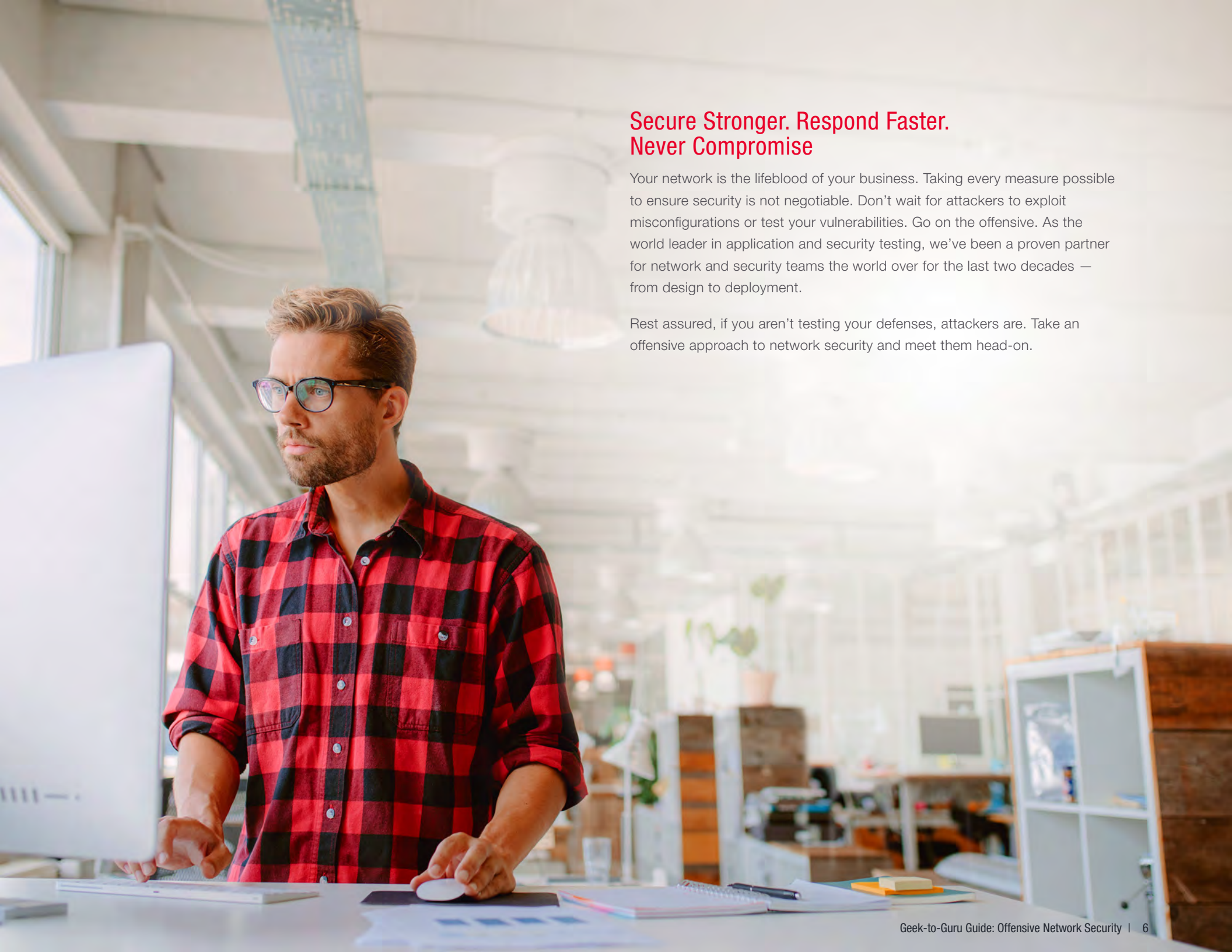
As their name implies, threat intelligence feeds stay up to date on the latest threats and exploits via a continuously updated database of known attacks, vulnerabilities, and malicious IP addresses. For example, Threat Simulator receives regular updates from Keysight's Application and Threat Intelligence (ATI) Research Center — including new audits, assessments, and attack scenarios based on emerging threats. The ATI team operates a global network of honeypots and oversees a robust database of over 50 million records and counting.

A Good Offense

In a world of constant flux — and unrelenting risk — your best defense is a good offense. Use breach and attack simulation to prevent configuration drift, pinpoint vulnerabilities in your security posture, and keep you protected against emerging threats and exploits.

With an offensive approach to security, you can take control of your network defenses — making it easy to do the following:

- emulate real-world attacks on your production network
- discover security gaps and misconfigurations
- remediate issues with detailed, step-by-step instruction
- stay ahead of attackers with 24/7/365 threat intelligence
- measure security effectiveness and optimize tool spending



Secure Stronger. Respond Faster. Never Compromise

Your network is the lifeblood of your business. Taking every measure possible to ensure security is not negotiable. Don't wait for attackers to exploit misconfigurations or test your vulnerabilities. Go on the offensive. As the world leader in application and security testing, we've been a proven partner for network and security teams the world over for the last two decades — from design to deployment.

Rest assured, if you aren't testing your defenses, attackers are. Take an offensive approach to network security and meet them head-on.

CHAPTER 2

What is Breach and Attack Simulation?

Tech Tips with Packet Boi

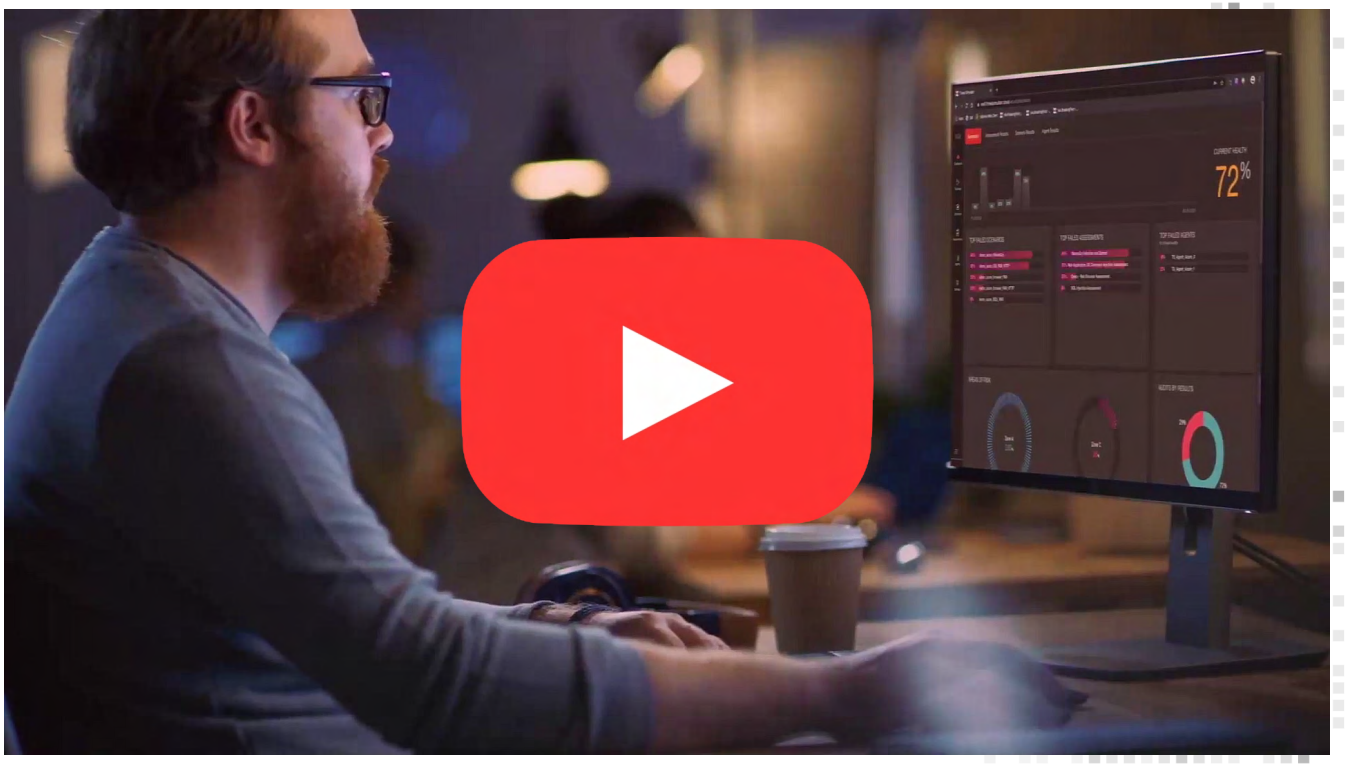
When it comes to network security, your best defense is a good offense. If you want to get ahead, you need to think like the enemy and hack yourself — before the bad guys get a chance.

CHAPTER 2

What is Breach and Attack Simulation?

Tech Tips with Packet Boi

When it comes to network security, your best defense is a good offense.



Source: https://youtu.be/hqQyBBteJV4

CHAPTER 3

Take Five

Keysight's CISO Discusses Cybersecurity's Past, Present, and Future

Scott Behm, Keysight's chief information security officer, shares his thoughts on leading enterprise security teams, how 2020 shook things up, and what the future may have in store.

CHAPTER 3

Take Five

Keysight's CISO Discusses Cybersecurity's Past, Present, and Future

Security is a journey, not a destination. Between new technologies, emerging threats, and seismic shifts in the cultural landscape, nothing stays static for long. In that spirit, we caught up with Scott Behm, Keysight's chief information security officer, to get his take on leading enterprise security teams, how 2020 shook things up, and what the future may have in store.

Scott Behm
Chief Information Security Officer

1 If we could rewind the clock two years, what could the IT world have done to better prepare for the diversity of risks offered by 2020?

2020 did indeed deliver the IT and cybersecurity community a diversity of trials and associated risks. Defending against increasingly sophisticated threat actors while addressing the people, process, and technology challenges associated with enabling effective and secure remote work almost overnight has definitely been interesting. On a positive note, we have all learned new ways to innovate and deliver. In some cases, we have yielded results even better than before.

As they say, hindsight is 20 / 20. In 2020, the IT world has proven its resiliency — and, overall, done well at enabling organizations to get the job done under extreme circumstances. Many lessons were learned along the way, and it most certainly wasn't the same journey for all. Looking forward, a greater focus on scenario planning for unthinkable crises will help us better future-proof our institutions and interests.

2 If you learned tomorrow that you were the victim of a ransomware attack, what's the first thing you'd do?

As you know, ransomware attacks — if successful — can have a major impact on their intended targets. As such, it is imperative that companies prepare using tabletop exercises, coordinated blind simulations (making participants believe it is the real thing), or purple team exercises to test not only their response but their ability to detect.

At Keysight, if we discovered or otherwise learned that there were indications of a ransomware attack, the SOC [security operations center] would immediately enact the ransomware playbook. The designated incident commander would begin coordinating communications with both responders and business stakeholders. Concurrently, the SOC would work to understand the scope of the attack, so appropriate containment and mitigation procedures begin as soon as possible.

3 What role do you think artificial intelligence (AI) and machine learning (ML) play in cybersecurity? What role can they play in the next five years? Do you think offensive use of ML will offset potential gains in security?

Artificial intelligence and machine learning are indeed starting to play a role in cyber defense. Today, AI / ML is helping in two areas:

- eliminating the ever-increasing false positives the SOC has to sift through to find the truly actionable alerts
- improving the ability to detect and alert on anomalous behavior or network activity

In the future, AI / ML will likely help cyber defenders even more in these two areas as the technology improves. Looking forward, quantum computing algorithms combined with AI and ML may make predictive cyber defense a true reality. This is based on the premise that quantum computing is able to represent several states at the same time — which will enable faster processing of related data sets and result in high-speed, high-fidelity threat predictions. Whether or not this happens in five years is anyone's guess.

4 How do you weigh the trade-off between "tool sprawl" and managing dozens of different security dashboards versus single-vendor solutions that might not be as good in all security categories? How do you consider the impact of management complexity?

In many cases, organizations do not entirely leverage their investments in cybersecurity defense and visibility tools. The full capabilities of existing cyber defenses may not be deployed, and existing configurations might not be tuned appropriately. So, do that first.

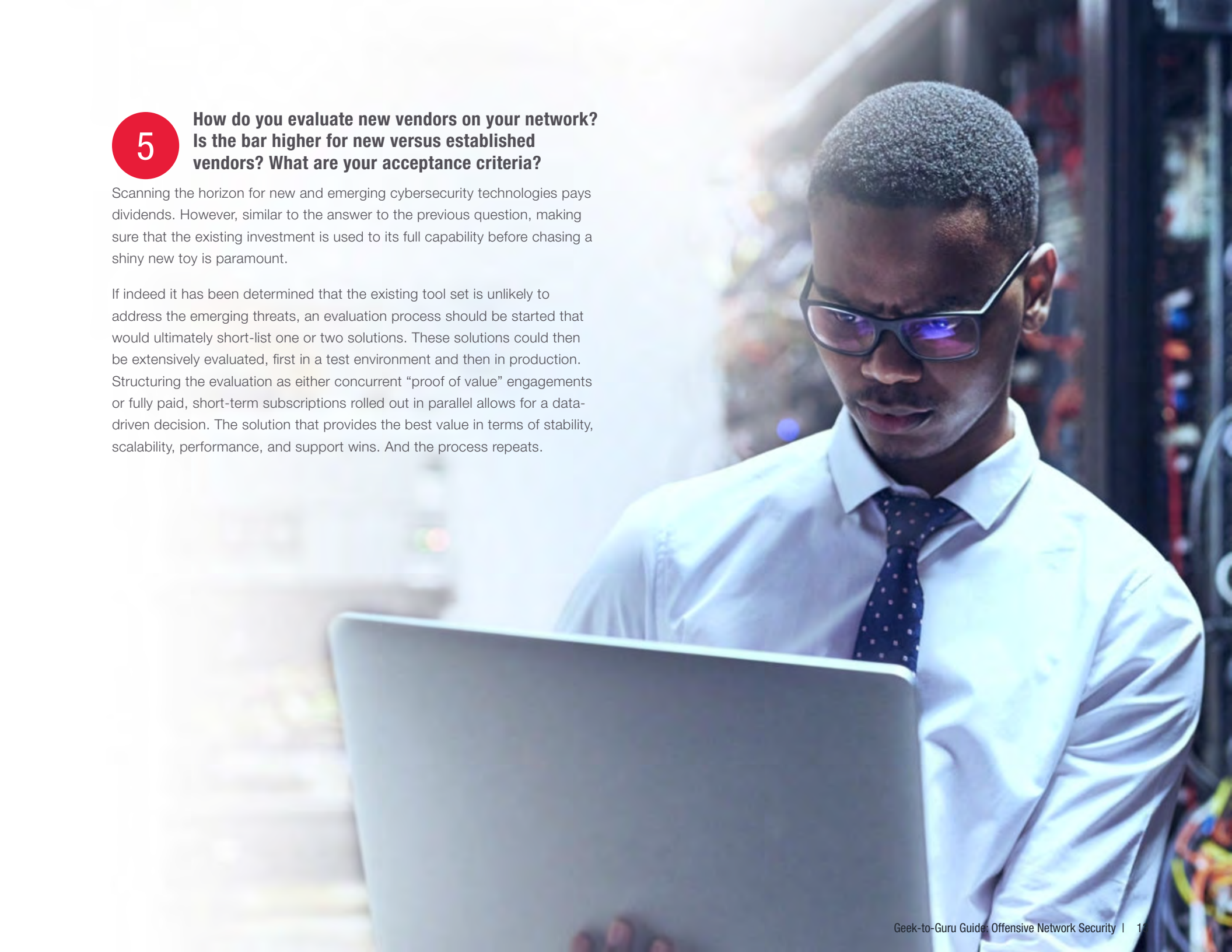
On cybersecurity defense: if the digital estate is entirely cloud-based from a single provider, leveraging the native cloud provider's cybersecurity defense capabilities to the greatest extent possible may make sense. However, if the organization's architecture is hybrid cloud — or a mix of everything, including on-prem IT and OT, multiple cloud instances, and edge computing — finding a single-vendor solution is likely impossible.

On cybersecurity visibility: developing a flexible security architecture that allows all security-relevant data to be centrally collected for cross-referencing, contextualization, and alerting will enable the SOC to be most effective in detecting threats, regardless of the threat vector.

5 How do you evaluate new vendors on your network? Is the bar higher for new versus established vendors? What are your acceptance criteria?

Scanning the horizon for new and emerging cybersecurity technologies pays dividends. However, similar to the answer to the previous question, making sure that the existing investment is used to its full capability before chasing a shiny new toy is paramount.

If indeed it has been determined that the existing tool set is unlikely to address the emerging threats, an evaluation process should be started that would ultimately short-list one or two solutions. These solutions could then be extensively evaluated, first in a test environment and then in production. Structuring the evaluation as either concurrent “proof of value” engagements or fully paid, short-term subscriptions rolled out in parallel allows for a data-driven decision. The solution that provides the best value in terms of stability, scalability, performance, and support wins. And the process repeats.



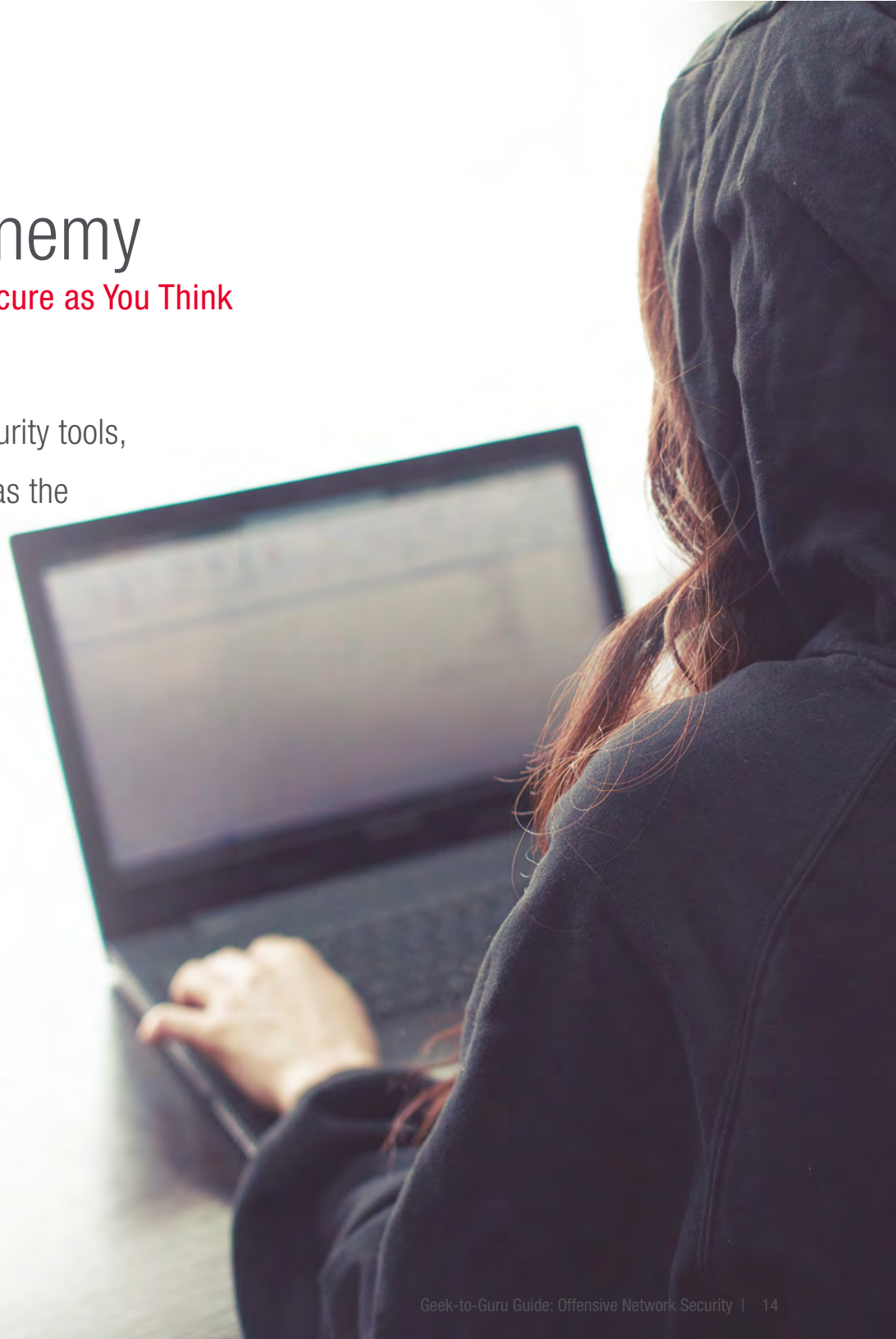
CHAPTER 4

Uncertainty is the Enemy

Three Reasons Your Network Isn't as Secure as You Think

There's a lot riding on your network security tools, but are they still protecting you as well as the day you installed them?

The answer might surprise you.



CHAPTER 4

Uncertainty is the Enemy

Three Reasons Your Network Isn't as Secure as You Think

Your network is under attack. As you're reading this, there's a good chance someone's trying to break into your network. Attackers don't sleep or take days off. They're testing your defenses 24 hours a day, seven days a week, and 365 days a year. To your credit, you've invested in an arsenal of powerful network security tools. But your network has undergone a stream of patches and updates. And hackers are learning and adapting as well. Can you really validate that your network, applications, and data are as safe as they were the day you installed your tools?

With an environment that's always in flux, you can't be sure that what worked yesterday is working today. Mischief makers and their bots are constantly testing your defenses. Just one of them needs to succeed just once to wreak havoc. You had better succeed all the time. But how would you know if you are?

Suppose you haven't detected any network intrusions. Is it because your security tools are working well? You could be lucky, and hackers have spared you. Or maybe — a big, scary maybe — attackers are already inside your network and you don't even know it.

The point isn't that you should throw up your hands in defeat. It's that network security isn't once and done. It's a never-ending cat-and-mouse game on a fluctuating board. When you're aware of the pitfalls, however, you can adopt new strategies that let you take back control and gain the upper hand.

Here are three reasons your network might not be as secure as you think.

1. You Can't Just "Set and Forget" Your Network Security Tools

Security is never static. On one hand, new threats, exploits, and attacks emerge daily. On the other, your security tools are continuously updated, patched, and tweaked. With so much in flux, you can't trust that being secure yesterday means you're still safe today.

For security organizations, configuration drift is a serious — and underappreciated — concern. Even if your network, applications, and data were 100% secure the day your tools went live, a perpetually shifting threat landscape means they may not be tomorrow. You can't just have your reseller set everything up and walk away. If you aren't reassessing your security stack on an ongoing basis, you're essentially flying blind.

But applications are not the only things that change. Networks are always changing — and improperly deployed infrastructure, security solutions, and applications cause plenty of breaches on their own. Even networks architected with best practices face a constant stream of adjustments based on the growth of the organization, the volume of users, and the changing needs of both groups. With multiple physical locations and cloud deployments in use, keeping best practices in place is an uphill battle.

ProTip

Be your own worst enemy

If you aren't testing your own defenses, attackers are. Fortunately, in the case of security measures, nondestructive testing is not only possible, is easy to perform. Breach and attack simulation (BAS) tools, like Keysight's Threat Simulator, make it easy to stay ahead by safely simulating a wide array of attacks on your production network. With automated assessments, you can prevent configuration drift by continuously evaluating your security tools, pinpointing vulnerabilities, and remediating gaps with step-by-step instructions.

ProTip

Prevent attacks before they happen

BAS tools make it easy for security teams to prevent two of the most common tool errors that occur during network breaches: failure to mitigate the initial exploit and failure to prevent lateral movement.

1. BAS tools ensure proper security rules are initiated when attacks start. In addition, automated assessments validate that overnight changes to security rules get proper vetting before taking effect.
2. Organizations can deploy BAS tool agents in multiple network zones to mitigate attackers' lateral movement after an initial breach. Should a simulated attack traverse those zones, alerts will notify the security operations center that security solutions are not scrubbing network traffic.

2. New Attacks Capture Headlines, but Most Threats Hit Closer to Home

While new exploits and attack vectors get the most media attention, a single unpatched security vulnerability can create a direct pathway into your application database. In fact, Ponemon Institute reports that nearly half of all breaches stem from human error, system glitches, and misconfigurations.

Vulnerabilities like these can affect any point in your organization's application stack, including network services, platforms, databases, web servers, application servers, custom code, virtual machines, containers, and storage. Unpatched flaws — including default access accounts, unused web pages, and unprotected files or directories — are among the most frequently used paths for gaining unauthorized access to a victim's system. After all, attackers may be sophisticated, but they often opt for the path of least resistance.

The sheer level of effort needed to ensure that every patch, release, and update is free of vulnerabilities is too great an expense for any company to bear, however. The diminishing returns do not justify the cost, even for the Fortune 100 companies that dedicate huge budgets and highly skilled individuals to solving this problem. For instance, one operating system kernel or driver update can have ripple effects on related software elements. That's why you continue to find new Common Vulnerabilities and Exposures (CVE) entries for almost every software solution in existence.

3. What You Don't Know Can Hurt You

Despite rapid technological advancement, modern applications are not getting any simpler. Enterprises count on security operations (SecOps) and development teams to understand the latest application and threat vulnerabilities, but that is asking a lot. Operating systems, software development environments, and new attack methods all require constant attention — and multiple teams often find themselves scouring message boards around the clock for new threats.

You need to validate your entire security ecosystem to prevent attackers from capitalizing on your system's weaknesses. But there is only so much time — and budget — to go around. Development teams are under pressure to fix bugs and meet delivery schedules, while SecOps is working to secure an ever-expanding attack surface. Something has to give, and many teams struggle to keep up.

But capturing "threat intelligence" like this is not enough. Staying ahead of the latest attacks is a good start, but SecOps and development teams need to be aware of risks in their applications as well. "Application intelligence" like this isn't as common as threat intelligence, but it's no less important.

ProTip

Train like you fight, fight like you train

Your tools are only as good as the attacks you test them against. That's why so many organizations choose BAS tools that are backed by professionally curated application and threat intelligence feeds. With regular updates, you can assess your network's readiness against the latest known threats and vulnerabilities. That way, when your tools face the real thing, you can be confident your assets and applications are secure.

For example, Keysight's Application and Threat Intelligence (ATI) Research Center keeps Threat Simulator updated on a regular basis with new audits, assessments, and attack scenarios. With tools that automatically stay a step ahead of cybercriminals, you can keep the members of your team focused on mission-critical tasks like investigating potential intrusions while your tools do the heavy lifting for you.

Be a Hero, Not a Headline

With attackers constantly probing for weakness in your network, installing robust security tools is just the first step. Attacks are coming from all angles, and latent threats lurk around every corner. For true peace of mind, you need to fortify your defenses from multiple fronts:

1. **Don't "set and forget" your tools.** Assess your security stack regularly with breach and attack simulation (BAS) tools, such as Keysight's Threat Simulator. By safely simulating real attacks on your live network, you can make sure your tools are always prepared to meet the needs of an ever-changing threat landscape.
2. **Protect the path of least resistance.** Use automated BAS tools to catch unpatched flaws, find hidden vulnerabilities, and prevent common tool failures.
3. **Stay a step ahead of cybercriminals.** Back up your security stack with a professionally curated application and threat intelligence feed to continuously test your defenses against the latest attacks, vulnerabilities, and exploits.

Don't wait for attackers to make the first move. With just a few proactive steps, you can make them fight on your terms. Keysight makes it easy to proactively protect your network without compromise. As the world leader in application and security testing, we understand the threats you face and the business goals you seek. From design to deployment, we'll help you take charge of your network defenses. With Keysight, you can focus on adding value — not fighting fires.

Information is subject to change without notice. | 7121-1091.EN © Keysight Technologies, 2020 - 2021 | Published in USA, June 19, 2021 | keysight.com