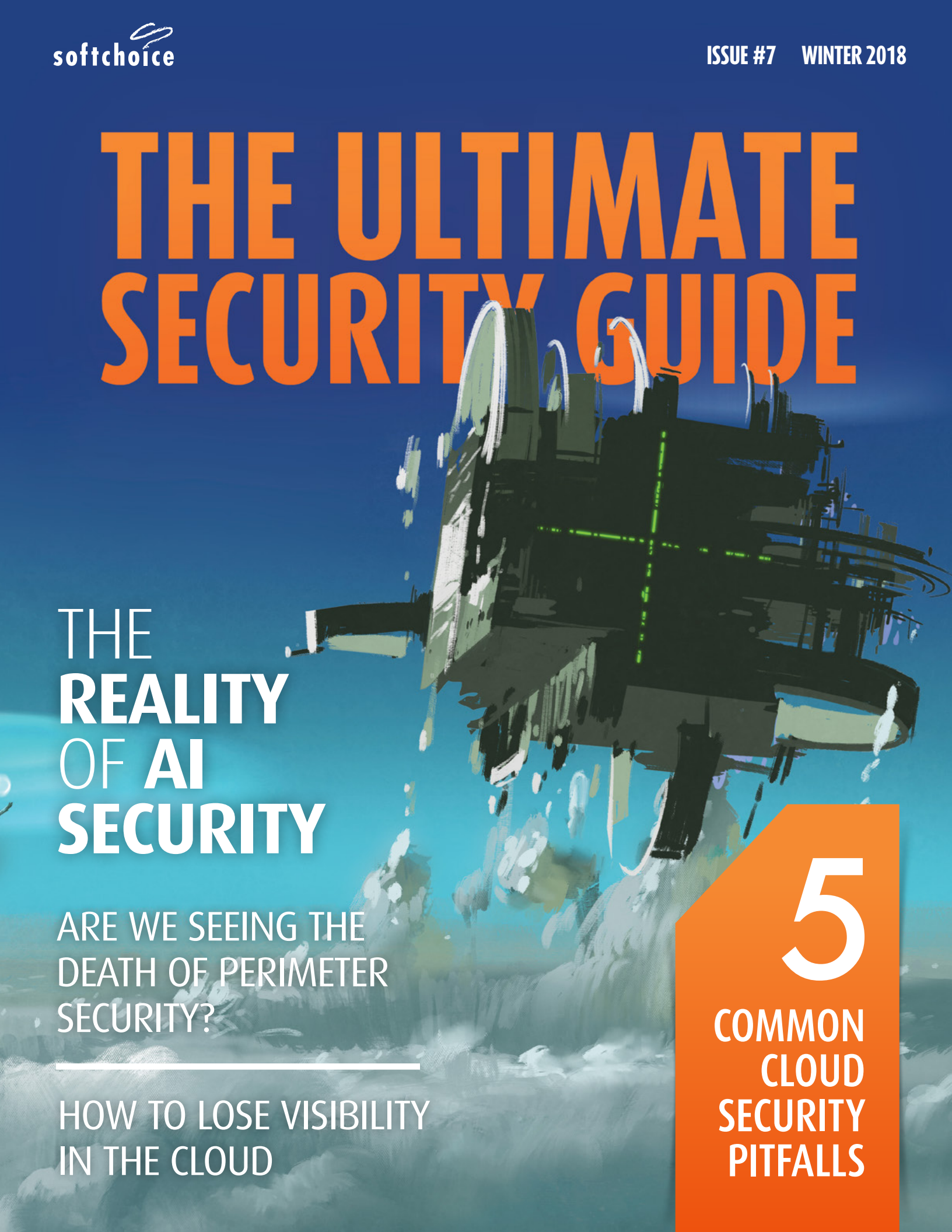
softchoice

ISSUE #7 WINTER 2018

THE ULTIMATE SECURITY GUIDE



THE REALITY OF AI SECURITY

ARE WE SEEING THE DEATH OF PERIMETER SECURITY?

HOW TO LOSE VISIBILITY IN THE CLOUD

5 COMMON CLOUD SECURITY PITFALLS

USG

ULTIMATE SECURITY GUIDE

PLATINUM SPONSOR

softchoice

GOLD SPONSORS

TREND MICRO

gemalto
security to be free

KASPERSKY lab

SILVER SPONSORS

FireEye

SentinelOne

Check Point
SOFTWARE TECHNOLOGIES LTD.

WINTER 2018

ISSUE 7

COMPLETE LIST.
WHAT'S IN THIS ISSUE

CONTRIBUTORS

Wendy Moore
Director of Product Marketing at Trend Micro

Alan Hanway
Business Development Manager at Gemalto

Matthew Balcer
National Sales Engineer at Kaspersky

Joseph Byer
Manager of Client Hardware at Softchoice

ADVERTISING INQUIRIES

Sara Onyschuk
Director, Business Development,
Client Solutions
Sara.Onyschuk@softchoice.com

ULTIMATE SECURITY GUIDE

WINTER 2018 - ISSUE 7

PLATINUM SPONSOR
Softchoice

GOLD SPONSORS
Trend Micro
Gemalto
Kaspersky

Sara Onyschuk
Director, Business Development, Client Solutions
Softchoice Enterprise Software & Security

Dear Reader,

"Taking risks" and **"security"** are rarely used in the same sentence. Security is about being risk-averse, sticking to what works, and not deviating from tried and tested architectures.

Unfortunately, this approach won't cut it anymore. Malicious actors have figured out our old defenses. At the same time, by moving into the cloud, we're embracing totally different environments that demand different approaches. Nobody can afford to do the same old thing more vigorously than before. New approaches and new strategies are a necessity.

That's what the theme of the latest Ultimate Security Guide is all about: progression. Whether it's how machine learning will affect security, or whether you need to update to the new Windows right away, we're here to show you some new ways to think about keeping your systems safe.

It's our hope that this USG will give you a sense that, although times are changing, you can change with them. Embracing the unknown might seem scary, but it's much better than the status quo. Thank you for reading.

Sara Onyschuk
Director, Business Development, Client Solutions
Softchoice Enterprise Software & Security

MEET OUR DEDICATED SECURITY TEAM

SARA ONYSCHUK
Director Client and Security

ANDREW CAMPBELL
Vendor Engagement Manager

MELISSA NITOIU
Vendor Engagement Manager

ANDREA KNOBLAUCH
Technical Solutions Architect

JEREMY BANDLEY
Technical Solutions Architect

MIKE STINES,
Technical Solutions Architect

MIKE COIT
Technical Solutions Architect

ALEX ABERNATHY
Vendor Sales Specialist

JONATHAN BINCE
Vendor Sales Specialist

NABIL KHANDAKER
Vendor Sales Specialist

THE REALITY OF AI SECURITY

ARE WE LOSING THE CYBERSECURITY WAR? THERE ARE GOOD REASONS TO THINK SO. SECURITY SPENDING IS INCREASING. GARTNER PROJECTS THAT IT WILL GROW BY 8 PERCENT IN 2018, REACHING $96.3 BILLION IN 2018. MEANWHILE, RANSOMWARE COSTS ARE ALSO GOING UP. CYBERSECURITY VENTURES ESTIMATES THAT THE RANSOMWARE PRICE TAG WILL APPROACH $11.5 BILLION IN 2019. IT APPEARS THAT WE'RE SPENDING MORE MONEY ON SECURITY AND GETTING LESS OUT OF IT.

We've all heard that there are promises on the horizon in the form of Artificial Intelligence (AI) and machine learning (ML) security solutions. This should prompt some optimism. AI/ML solutions are fast, smart, and comprehensive like no other solutions before them.

But it's very unlikely that they'll solve all of our security woes. While there are huge pluses to AI/ML security solutions, there are significant limitations. To get an idea of where security is going, an acknowledgment of both is required.

In the interest of forming a more informed perspective, let's look at the positives and negatives of each.

POSITIVE 1: Making Up for the Skill Shortage

Machine learning is sometimes feared because of its effects on the labor force. More automation could put a lot of people out of a job. But when it comes to security, shrinking the need for labor is a good thing. It's arguably essential. There's a huge shortage of qualified cybersecurity personnel. In 2018, 51% of respondents to an ESG survey said their organization possessed insufficient security skills. This is 6% growth over 2017 and part of a year-on-year growth going back years.

AI/ML solutions will address this gap by automating the most cumbersome security processes. They can dig through massive amounts of unstructured data and curate selections of security events. Essentially, they rifle through all the haystacks and present the needles to analysts for further inspection. This is a huge gain for overstretched security personnel.

POSITIVE 2: Moving Beyond Signature Recognition

In a pleasant, bygone era, it made sense to identify strains of malware based on their signatures. Then, hackers made a mockery of that technique with polymorphic malware. That's malware capable of rapid, self-administered mutation. This is why, in 2017, Kaspersky Labs detected 360,000 new malicious files every day. There's no keeping up with that kind of variation.

Fortunately, AI/ML security generally doesn't have to. Rather than relying on specific signatures, AI/ML security detects anomalies of any kind. This is achieved by using machine learning techniques on massive sets of unstructured network data. Through this process, security systems gain an understanding of what normal user behavior looks like—and, in turn, a deep understanding of the abnormal.

Once trained, these algorithms can present human analysts with reports of any deviations. These reports can be sorted by how suspicious each deviation is, which helps analysts avoid false positives. This is a more versatile approach that can't be fooled by a simple change of footprint.

NEGATIVE 1: The Human Element

Hype isn't just misleading. It carries real risks. The words "artificial intelligence" shouldn't be taken to mean that a security solution is perfect. In fact, no security solution should be judged based on whether it has AI/ML technologies. It should be judged on its results, no matter what technologies enable them.

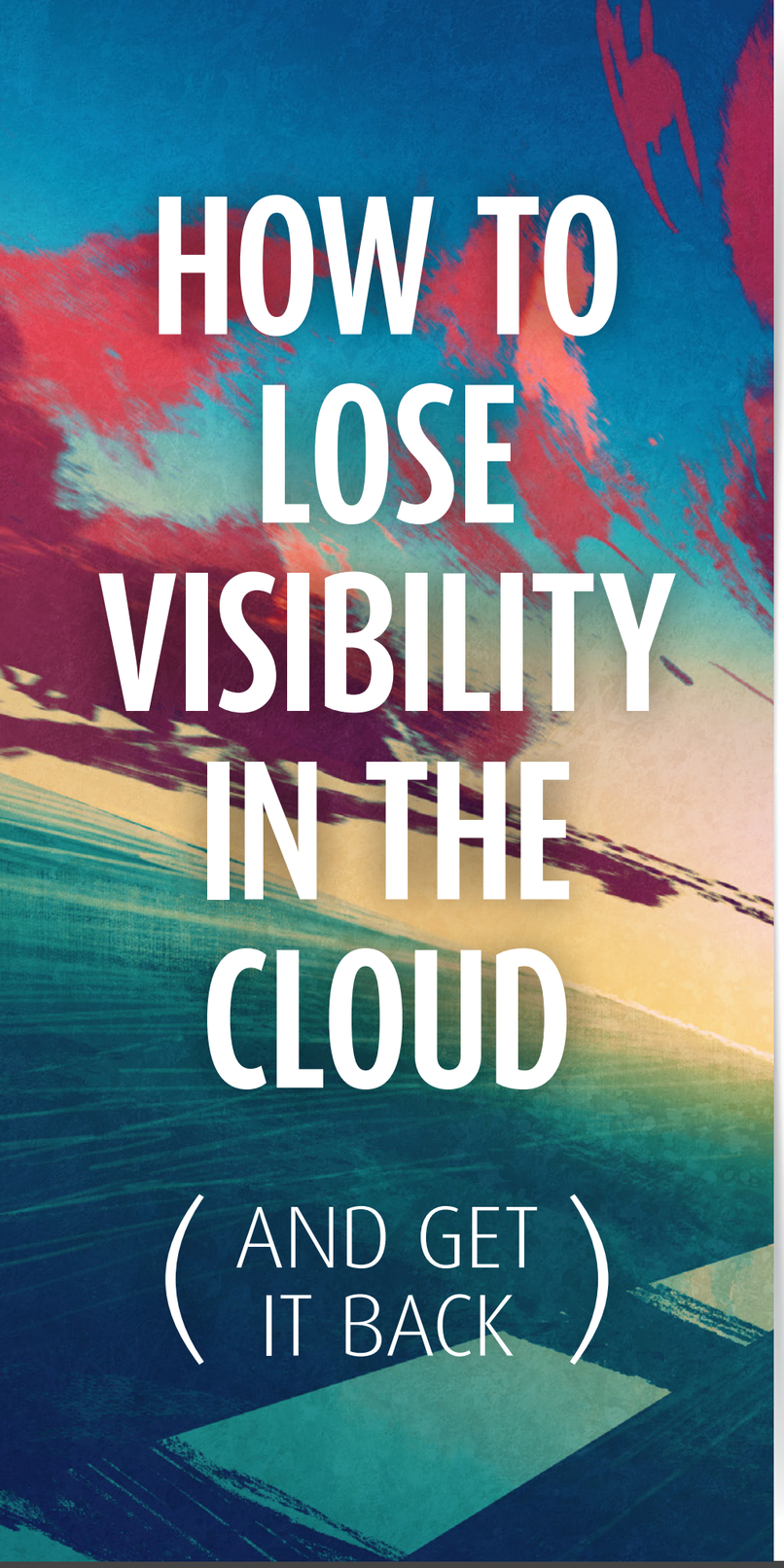
Moreover, companies shouldn't see the installation of an AI/ML platform as an opportunity to relax. Analysts need vigilance to avoid spending their time investigating false positives. As well, they need to stay up to date on emerging threats that could evade their fancy new platforms. Finally, IT and security teams need to ensure that employees are maintaining basic security hygiene.

NEGATIVE 2: The AI Arms Race

Anyone interested in security needs to know that the use of AI/ML isn't limited to the good guys. Hackers can use these technologies too. With AI/ML, hackers can automate labor-intensive, personalized attacks like spear phishing. Also, it's possible that AI/ML attacks could end up bringing down AI/ML security. Malicious actors could fool these programs with faulty test data. Or they could run AI/ML security programs in the cloud and attack them in an automated, intelligent fashion to find chinks in their armor.

The upshot here is that the introduction of AI/ML into security isn't an exclusively positive development. Like just about every development in the security landscape, it's a double-edged sword. It's another step in an ever-evolving battle between white hat and black hat hackers.

The negatives here don't mean that the positives are meaningless. Rather, that while AI/ML-enabled security is a positive step, it's not clear how long it can hold off the forces of darkness. This is just another exciting chapter, not the end of the story.



HOW TO LOSE VISIBILITY IN THE CLOUD

(AND GET IT BACK)

The cloud is now one of the basic facts of life. To achieve efficiency and flexibility, many teams within your organization will use the cloud services of their choosing, whether or not they are given permission to.

This is truer than many people imagine. IT and security departments often underestimate the extent of cloud use and have no idea which cloud providers are being used throughout their organization. Essentially, IT and security are often in a state of denial. They tell development and operations teams that they should stay away from the cloud, or only leverage the infrastructure of their choosing. But those commands are ignored. Business units wanting to deliver applications are driven by time to market concerns and have no incentive to obey, will continue to leverage the cloud without security's knowledge. Your developers will smile, nod, spin up an unapproved workload on AWS, if that's what they need for their specific purposes.

This is how visibility issues start, according to Wendy Moore, Director of Product Marketing at Trend Micro. Many IT departments do not know where cloud infrastructure is being used in their organization, because they assume that they are only using infrastructure sanctioned by the organization. They are not aware of how extensive their cloud security needs actually are. Meanwhile, their organization's attack surface expands, and they have no visibility of it.

Generally, business units are not worrying about security either. Many assume that built-in public cloud security is adequate, but cloud service providers have a shared responsibility model where they secure the infrastructure but you are responsible for securing what you put in the cloud. Alternatively, they may just not be security-minded people. Nobody is aware that there is a problem, which is the very definition of a poor visibility situation.

> IT AND SECURITY DEPARTMENTS OFTEN UNDERESTIMATE THE EXTENT OF CLOUD USE AND HAVE NO IDEA WHICH CLOUD PROVIDERS ARE BEING USED THROUGHOUT THEIR ORGANIZATION.

"It's actually kind of shocking," Moore says, "particularly in large enterprises. We will talk to a security person at an organization where we know teams are using the cloud, and say 'what's your cloud strategy?' They'll say, 'oh we're not doing cloud, we're sticking purely in the data center.'"

Moore and others at TrendMicro see this frequently. It's common enough that they have names for the usual stages of cloud development. The first stage is "cloud birth": the time when business units are first adopting cloud. The second stage is "cloud chaos." This is when the cloud has become widespread, but there is no central control: nobody has a clear policy, processes or tools about how to monitor and secure cloud use. In fact, nobody is even sure which cloud providers are being used. Then, as Moore puts it, "IT and security realize that this is going on, and they go, oh my gosh."

What follows is a scramble for control. Moore says this can go one of two different ways, depending on the mentality of IT. Some security teams resist the change. "There are those who come along and say 'thou shalt.' You are going to use the security tools that we have been using on-premise in the data center. And you are going to deploy them in the cloud."

But these tools aren't designed for the cloud. They aren't able to scale up and down with workloads in the cloud or automate to fit into cloud operational processes. So cloud teams become frustrated because security is slowing them down, which is exactly the reason they went to the cloud in the first place.

However, there is another way. IT and security can embrace what Moore calls the unique security and operational requirements of the cloud. This means using hybrid cloud security solutions that secure and create visibility in any environment whether it be on-premises in the data center or in the cloud with any service provider. With a solution like the one TrendMicro offers, enterprises can have it both ways. Cloud teams can use their own blend of cloud technology and tools, but the security team can provide security tools that fit the cloud environment, and integrate with the automated cloud operational mode. While security gains visibility into what was once the "wild-west" of the cloud and is able to ensure their organizations' security while gaining visibility of what is happening in the cloud.

The key to making these solutions work is keeping ahead of the needs of teams that want to leverage the cloud for business advantage. For example, TrendMicro adopted support for containers before they became a popular deployment model. Their Deep Security package can inspect containers as they are created. This maintains developer freedom while ensuring visibility in new environments.

In a sense, freedom is the central concern. Security teams need to acknowledge the fact that teams have up-to-the-minute needs that IT will not always be able to predict. Innovative information workers will adopt whichever cloud service they feel will improve their work. To pretend otherwise is to continue living in denial, which is the best way to increase risk and lose visibility.

5 COMMON CLOUD SECURITY PITFALLS

The cloud represents a new era of agile computing. But, equally, it represents a new era of security woes. The adoption of cloud means the disruption of the traditional security perimeter, which calls for new policies and mindsets. This is hard to do. Alex Hanway, Business Development Manager at Gemalto, sees clients falling into similar pitfalls again and again. He shared his expertise with us, in hopes of improving the state of cloud security education.

THINKING THE CLOUD IS A CURE-ALL

The most basic issue Hanway sees is a lack of willingness to acknowledge the cloud's faults. "The cloud is in that phase where it's still a bright shiny object." In other words, companies think that adopting the cloud is a problem-free way to make everything cheaper, faster, and more scalable. And, while that can be the case, it's important to be aware of the caveats. "They need to approach the cloud with a healthy level of skepticism." So, what does that actually entail?

One big, basic thing to remember is that the cloud is still a data center—it requires a basic level of security awareness. This is a consideration that's been ignored by many enterprises. For evidence of this, look no further than research conducted by Croatian security firm NVTEH in 2017. They discovered that an alarming number of AWS customers were accidentally sharing private data in the form of public Elastic Block Store snapshots. With little effort, NVTEH was able to extract security credentials belonging to an unnamed Fortune 100 company, as well as patient data drawn from health care researchers at a number of major universities, including genome sequences.

Moreover, Hanway says, companies forget that the cloud is a new kind of attack surface, which makes old-school perimeter security infeasible. "Customers can build walls that are higher and thicker," he says, "but the cloud's distributed nature means that this line of thinking no longer works."

NOT USING MULTI-FACTOR AUTHENTICATION

People are lazy. This is no less true when it comes to passwords. According to SplashData, the most common password in 2017 was "123456," edging out contenders like "password" and "12345678," which came in second and third place, respectively. In these dark times, it's simply wishful thinking to count on passwords to protect your data. "Multi-factor authentication isn't a luxury," Hanway says, "it's a requirement."

If it's such a no-brainer, why doesn't everyone adopt it? Well, it's often for the same reason that weak passwords are used: convenience. Many multi-factor authentication systems are cumbersome to use. But Hanway is quick to note that engineers working on authentication systems know this, and are making the processes more streamlined. "It's easy enough to just get a message on your phone you can tap."

TAKING A BLASÉ ATTITUDE TOWARDS ENCRYPTION

Lots of cloud service providers offer built-in encryption. And Hanway says that these services are a good start. "We'd much rather see a customer adopt the native solutions instead of doing nothing." (Which, he adds, he sees distressingly often.) However, not all encryption services are created equal.

For example, many native solutions don't offer granular access control. As a general matter, it's obvious that employees should only have access to the specific data they need, at the precise time when they need it. Alice from accounting might need financial data throughout her work day, but not during off-hours. Bob from marketing might need it once a month. A third-party solution is sometimes required to facilitate these specific permissions.

Also, even the best cloud-native encryption can be supplemented with third party features. Gemalto's Safenet Protect V enhances AWS by offering a full-disk encryption of EC2 instances.

FRANKENSTEIN KEY MANAGEMENT

One of Gemalto's central offerings is centralized crypto key management. This is important, Hanway says, because of the increasing number of crypto keys that companies work with, and the high costs of mismanaging them. Lost keys translate into lost data, as do compromised keys. Failure to produce the right keys can create auditing issues. In short, lacking a united key management system quickly creates a shambolic mess. But these problems can be solved in one fell swoop by adopting a visible, unified system, which allows administrators to track keys and dole them out as needed.

ASSUMING THAT BREACHES WON'T HAPPEN

These days, it's common to hear that data breaches are a matter of "when" and not a matter of "if." Hanway agrees, in spite of himself. "I hate to try to scare people into feeling like they need to do something. But the reality is data breaches are happening to everyone." According to Gemalto's research, 2.6 billion records were stolen or compromised in 2018. Companies with compromised records ranged from mom n' pop shops to giant multinational corporations.

So, if data breaches are inevitable, what's to be done? The first step is prevention of the kind outlined above. Correct encryption policies could mean that stolen data is useless, either in whole or in part. And, while multi-factor authentication won't protect against every breach, it's the single most important preventative tool.

After that, acceptance is necessary. That involves coming up with a data breach protocol in advance—knowing which consultants to contact, and how to proceed with legal counsel. As well, companies need to be committed to customer transparency. In the case of a data breach, telling customers that they've been exposed might be painful upfront, but everything comes out eventually, and a gradual release of information will erode consumer trust.

ARE WE SEEING THE DEATH OF PERIMETER SECURITY?

Often, people adopt new fashions before noticing their implications. We all got smartphones, and marveled at having email everywhere, as well as fun games. Then, we noticed that they were bad for our concentration, and we uninstalled some of our apps. Meanwhile, cool companies embraced open concept offices, expecting easier collaboration and increased happiness. Now, studies are showing that they're bad for productivity. Some executives are opting for walled offices again.

This pattern is true of the cloud as well. The upsides of the cloud are extraordinary. Speed, convenience, scalability, savings: it's all there. But the cloud also requires a new security mindset. Specifically, it requires supplementing perimeter security with other solutions.

Matthew Balcer, National Sales Engineer at Kaspersky Labs, explains this cogently. "By definition," he says, "the cloud is perimeter-less, so I certainly can't use perimeter security to defend it."

Balcer says that a surprising number of companies haven't grasped the ramifications of this. "Cloud technology moves so fast, and I can't say that the wheels of the security machine have rolled at the same speed."

Companies of all sizes bought into the cloud, but still thought their old security was enough. They thought of "security" as a static concept, not a concept that could change. As a result, they thought they had achieved security forever by buying nice firewalls.

HOW TO BECOME A TARGET

There's another, related blind spot that Balcer often notices. He finds that small companies don't think they're targets in the cloud. As a result, they stick with their old perimeters. "But you don't necessarily have to be a target," Balcer says, "you became a target by using a cloud service. It doesn't matter that you're not a big enough organization. You're just going to fall into the mass attack." If you put your data on DropBox, for example, you're now a casualty of potential DropBox breaches. (Such as the one that occurred in 2012, which lead to 68 million leaked user passwords in 2016.)

It's true that cloud service providers have excellent security, Balcer says. But it's excellent security that all the malicious actors in the world are trying to breach. And some succeeded. "You name it—iCloud, Yahoo, DropBox, LinkedIn—these are some of the biggest names in the cloud space. They've all been breached." There's no such thing as impermeable security. Especially not under those circumstances. Also, in the case of cloud providers like AWS/Azure, the customer is ultimately responsible for their data. If you suffer a breach because of your own security practices, that's on you.

But moving beyond perimeter security can be tricky because a lot of companies don't know where their assets are. In the rush to adopt complex arrays of cloud services, it is easy to lose track of the finer details. Says Balcer: "The first question I ask when I go into a company is 'Where is your data?' It's a question that gets harder to answer every year." Even if they know which cloud services they're using officially, their staff are probably using a bunch more unofficially. Company data and assets become distributed without their knowledge.

HOW TO PROTECT YOURSELF

Firms that fall into this bucket- and there are many- need companies like Kaspersky to help out. The challenge is it can be hard to hear that the nature of security has changed after you've invested heavily in perimeters. As a result, a lot of companies wait until they have a breach to make the jump. Which is unwise, according to Balcer. "The most expensive time to put security measures in place," he says, "is when you're already responding to an incident." Moreover, adopting cloud security gets more expensive over time. This is owing to the fact that cloud use tends to become more complex rather than less. Companies use more apps, and data gets more spread out. So, the sooner you move beyond the perimeter, the better.

Does all this mean that perimeter security is, strictly speaking, 'dead?' Of course not, says Balcer. "We always preach a layered approach. Although something like a next-gen firewall might not help you that much in the cloud workload space, it can still play a role. It can still give you good network rules, control traffic, solidify access policies, and so on." There is still a place for old-fashioned perimeter security, and Kaspersky's solutions can work with it.

However, it's clear that cloud workloads will continue to become the norm. "We might get to a point very soon where even large organizations are looking at a 50-50 balance of cloud and on-prem," says Balcer. "Many small businesses will become almost 100% cloud-based." So, while perimeter security isn't dead, it may be in its autumn years.

THE SECURITY REASONS
FOR MAKING THE WINDOWS 10 MOVE

BY NOW, YOU'VE PROBABLY HEARD THAT WINDOWS 7 GOES "END OF SUPPORT" AS OF JANUARY 14, 2020. UNLESS YOU'VE ALREADY MADE THE LEAP, YOU'RE LIKELY THINKING ABOUT WHEN TO UPGRADE. PERHAPS YOU'RE PUTTING IT OFF, FEARING THE ASSOCIATED INCONVENIENCES AND COSTS ASSOCIATED.

Well, here's a sentence you don't hear every day: you don't want to end up like the US Navy. In 2015, due to nothing more than inertia, they were still using Windows XP, which was then 14 years old. This had obvious security implications. So, to avoid their warships being hacked, they had to maintain a private security support contract with Microsoft, to the tune of $9 million a year. A fine use of taxpayer funds, don't you think?

Like many enterprise horror stories, the intuitive reaction is "this kind of thing would never happen to my company." But it actually could. Procrastination is a brutal master. It can engulf small enterprises (or large ones, like the navy) with ease. And, while Windows 10 migration can be easy enough with proper guidance, it's still a process. It often involves significant device replacement, accommodating legacy apps, and so on. Initiating it too late could mean incurring surprise costs based on chaotic purchasing, as well as creating other issues. Or it could mean hanging onto Windows 7 for far too long.

Which shouldn't even be an option. It won't be safe. After end of support, Windows 7 will be open season for malicious actors. And they'll be highly motivated, because, if other Windows updates are anything to go on, millions of users will fail to upgrade for years.

But ensuring a smooth transition isn't the only reason to start migrating to Windows 10 immediately. There are also security concerns. While Microsoft is continuing to offer excellent security support to Windows 7 users, there's no way to give them the enhanced security features available in Windows 10. This means that updating to Windows 10 could save you from a devastating breach.

This is not a hypothetical scenario, in any way. Thanks to its improved security, Windows 10 was the only Windows safe from WannaCry. It's true that Windows 7 was considered safe if patched correctly. But correct patch use is surprisingly rare. This is why Windows 10's anti-malware features update automatically by default.

It's for these reasons that the National Health Service of the UK, in May, struck a deal with Microsoft to adopt Windows 10 two years before end of support. WannaCry had a literally life-threatening effect on them, resulting in 19,494 canceled appointments, which includes at least 139 patients who had "an urgent referral for potential cancer canceled". If they had adopted it earlier, a large number of health scares could've been avoided.

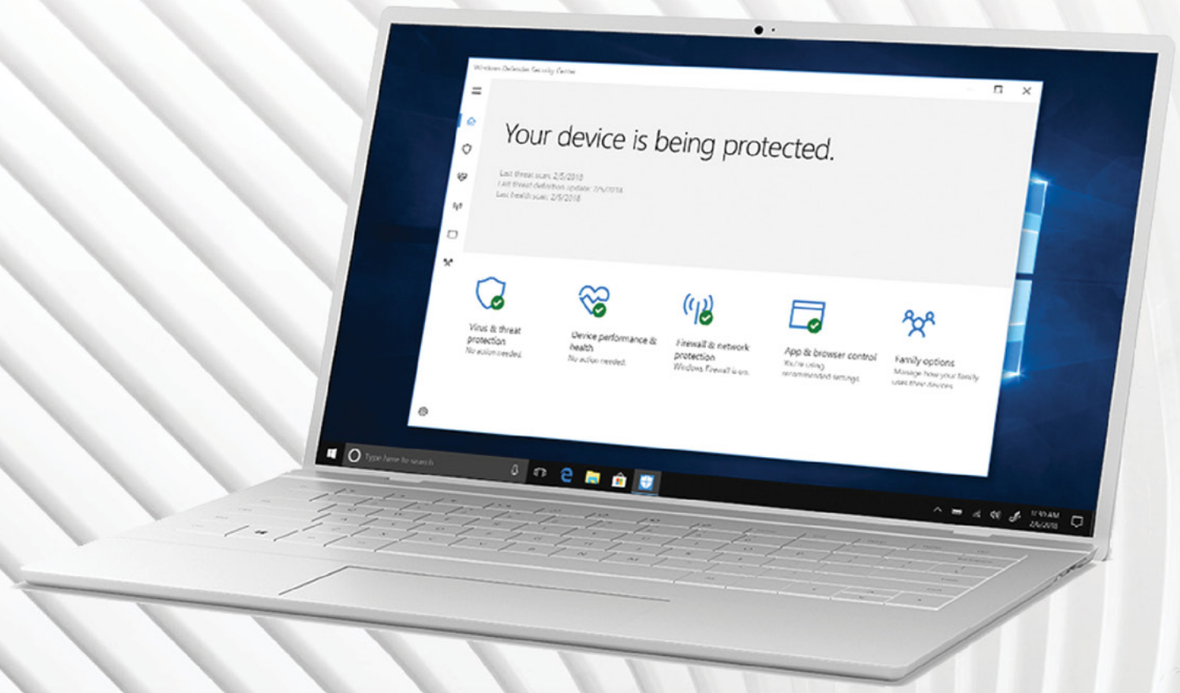
Given the worldwide upswell in malware, it's unlikely that this will be the last attack that falls somewhere in between the security capabilities of the two operating systems. Malicious actors learn from what works and what doesn't. Having learned that Windows 10 is a harder target, it only stands to reason that hackers would take more interest in a softer one.

The counter-argument here is that migrating to Windows 10 can be expensive. That's true, it can be--If you don't have a clear strategy and you do it in a rushed fashion. Or if you procrastinate, and, during the procrastination period, invest in systems you'll have to discard when you make the move. However, proceeding in the near future with a well-thought-out roadmap will reduce costs significantly. Also, consider whether you'd like to deal with the indefinitely expanding price of suffering a data breach. Better the inconvenience you know than the devil you don't.

Microsoft | softchoice

DETECT AND RESPOND TO DATA BREACHES.

Learn how to make the shift to Windows 10 Pro before January 2020.



MAKE THE SHIFT

CONQUER THE CLOUD

Download our eBook to learn how to build your own cloud strategy or optimize your existing one.

Download Now

softchoice

www.softchoice.com/cloud-accelerator

softchoice