Trustwave®

CYBER RESILIENCY IN THE MULTI-CLOUD ERA

TABLE OF CONTENTS

CYBER RESILIENCY IN THE MULTI-CLOUD ERA

Introduction

The way business is being conducted today is rapidly changing. The evolution of handheld technology has resulted in consumer behavior that demands immediate, anywhere, anytime access. To meet these demands, enterprises are looking up to the cloud. This has propelled business leaders into migrating to multiple cloud environments that provide the speed and flexibility that business operations and processes require.

Now, organizations can cater to the needs of their customers, accelerating product and service deliveries, but also tapping into an influx of new data that can present additional revenue-generating opportunities. But with the benefits come the challenges, especially on the data protection front.

Working in multiple cloud environments introduces an added layer of complexity when it comes to locating and securing dispersed data housed in numerous environments. Additionally, making the decision on what security solutions best fit your organization's risk profile requires careful consideration, planning and communication. Then there's data privacy. The implications of the global data regulations have taken the privacy discussion to new heights. For large organizations, pinpointing sensitive data is difficult enough, but an added layer is introduced in the form of privacy laws that vary depending on whose data it is and where it's located.

Reaching a state of cyber resiliency in the multi-cloud era is one the biggest challenges a security leader faces today, which is why we've decided to cover this topic and provide actionable insight from Trustwave experts. The following articles will illustrate the biggest challenges you face today operating in multi-cloud environments, but most importantly, offer tactful instructions tied to:

- Vetting your cloud-based third-party provider;
- Determining if native or non-native cloud security tools are best for your organization;
- Navigating the challenges tied to data privacy in the cloud.

We hope you find this e-book to be informative and to serve you as a guide throughout your journey in securing your organization in its digital transformation journey.

PART 01

TAKE TO THE SKIES

CREATING A THIRD-PARTY RISK MANAGEMENT PROCESS FOR YOUR CLOUD VENDORS AND PROVIDERS.

As organizations rapidly transform their business processes and operations, leveraging cloud-based third-party services and applications, be it SaaS or infrastructure providers like Amazon Web Services (AWS), has become more commonplace.

Unfortunately, an organization's security department may not be properly equipped to vet these cloud providers. According to Netskope's 2019 Cloud Security Report, one of the top security headaches security operation centers are struggling with is the lack of qualified staff. Additionally, 49 percent of the cybersecurity professionals surveyed in the report indicated that cloud-enabled cybersecurity is the topic area they would find most valuable for ongoing training and education.[1]

A new set of challenges are presented by the services and platforms offered by these cloud providers which require security leaders to conduct thorough assessments prior to engagement.

[1] Netskope Report, "2019 Cloud Security Report," August 2019. https://resources.netskope.com/cloud-security-collateral-2/2019-cloud-security-report

Why might organizations feel so ill-equipped to vet cloud-based third-parties and manage ongoing cloud security? This can be due to a number of reasons. Security may not be a priority as organizations rush to migrate to the cloud or adopt new third-parties. Additionally, there may not be a proper third-party risk management process in place to account for cloud vendors. Or security leaders may not know what cloud vendors are entering their environment, which may be the case for third parties who come in via departmental channels and side-step traditional vetting processes. For example, social media management platforms and even communication platforms might be onboarded in a matter of weeks or days without the security function being aware.

Worse still, organizations who are reliant on cloud-based infrastructure providers such as Microsoft Azure, AWS, or the Google Cloud Platform, may not consider these cloud providers as third-parties and fail to vet them with the same scrutiny they deserve.

As Thad Mann, director of infrastructure and endpoint security at Trustwave says, “While cloud providers may be a bit more dynamic than other vendors, they should fall within the company’s defined vendor risk management process.”

Security leaders need to shift their third-party security approach intelligently and adapt to the rise of cloud vendors. This requires them to take the right security measures for their existing cloud-based third parties and put in new processes for new cloud vendors business departments are considering.

Find Your Blind Spots

Before applying a new third-party vetting process for any new vendors, you have to ensure your existing cloud vendors are also up to par. This means making an effort to identify all the cloud vendors in your organization.

Consider your visibility and monitoring tools – where are they lacking coverage? Is a department or new employee unaccounted for? There might not be a technical solution here – you may have to simply reach out to leaders of your organization and do some fact finding. Talk to your finance and legal department. Were there any approved contracts or charges for third-parties or vendors that you may have missed?

Due to the nature of cloud-based vendors, it's very easy to onboard them after a contract is signed. This means departments can quickly and easily implement a cloud-based vendor for a small function of their department such as calendar scheduling, social media, or even internal comms. These small partnerships are essentially a form of shadow IT and there's no guarantee that these tools are being properly vetted.

For small cloud-based vendors, decision-makers on both sides of the contracts often want to have these tools available immediately, making due diligence less of a priority. This means service-level agreements (SLA), contracts, and terms and conditions (T&C) often go unreviewed, potentially exposing the organization to unnecessary risk. This doesn't mean a security leader has their hands tied, however. Cloud-based vendors, especially if they're small or just starting out, are often willing to work with companies to stay in an organization's good graces. This means there's an opportunity to update contracts, SLAs, or T&Cs to ensure your organization's security is accounted for.

Know What's at Stake

When assessing third-party cloud vendors, you need to understand how they interact with your data and what kind of risk that poses to the organization. Are they handling sensitive credit card data? Personally identifiable information (PII)? Intellectual property or perhaps business critical assets? Is the data subject to specific compliance standards or regulations?

Answering these questions will help you prioritize and organize how you vet your potential cloud vendors. For example, depending on your industry and organization, a cloud-based social media management tool might require less vetting than a payroll or payment processor simply because the data stored in the cloud has a different level of associated risk. However, if you're adopting a cloud infrastructure provider such as AWS, that'll likely fall into high priority because of how much of your data and company's infrastructure will now live in the cloud.

Security leaders must also consider the regulation and compliance impacts that continue to put the pressure on organizations. Both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA), have far-reaching implications for organizations. According to Gartner's April 2019 The State of Privacy and Personal Data Protection report, "the California Consumer Privacy Act (CCPA) emerged on the legislative scene and passed in record time, paving the way for change across the U.S. privacy landscape. At the time of publication, 13 states have followed suit, introducing draft laws, some of which exceed the CCPA in scope. Cumulatively, they impact nearly 40% of the population in the U.S."[2]

Because cloud-based vendors often have a global footprint, their resulting customers assume much more responsibility surrounding the data itself. Even if data tied to the European Union isn't on your organization's radar (and neither are your cloud-based third parties), new regulations are being introduced around the globe in countries such as New Zealand, Brazil, and Chile that may affect you or your third-parties.

[2] Gartner Report, "The State of Privacy and Personal Data Protection," April 15, 2019. https://www.gartner.com/en/documents/3906874/the-state-of-privacy-and-personal-data-protection-2019-2

Use Your Existing Third-Party Risk Management Process

(IF YOU HAVE ONE)

If you already have a third-party or vendor risk management process in place, then that should be your starting point. Cloud vendor risk management is a subset of third-party or vendor risk management. While there are specific considerations when it comes to cloud-based third-parties, the fundamentals of third-party risk management still apply and go a long way in ensuring you're vetting your cloud vendors effectively.

Know Who's Responsible (It's Usually You)

Mattias Deny, vice president of Managed Security Services at Trustwave, offers the following question as a point of guidance: "If something goes wrong in your cloud environment and it's breached, whose fault is it?"

We've seen it time and time again. Many recent major data breaches involving retailers and financial institutions were the results of third-party exposure. But third-parties are hardly ever the ones suffering the consequences.

No matter the third-party, you should always assume you're the one carrying all the risk. Even if a data breach is the result of a third-party, whether cloud-based or not, the owner of the data is the entity that will suffer fines, reputational damage, or customer loss.

You're also responsible for communicating with customers, cooperating with any potential law enforcement investigations, remediating the issue and offering reparations to any affected parties, whether that's in the form of free credit monitoring or free services. Returning to business as usual is costly and depending on contracts and SLAs, cloud-based third parties may not have any responsibility other than alerting you to the fact that your data was compromised, leaving your organization to clean up the mess.

As you vet potential cloud vendors, make sure any security measures they have in place can and will ultimately affect you.

"Even if a cloud provider has encryption in place, you should make sure it's the right kind of encryption and that you still have done the basics, such as deploying the right network segmentation and access control," Mann says.

This mindset of assuming all the risk will help you vet potential vendors more effectively because you can approach cloud-vendor risk management with the understanding that your organization will be largely culpable in the event of an incident.

Getting To Know Your Cloud-Based Vendor

When you begin the vetting process, consider the approach as understanding your cloud-based vendor's relationship with you during three points within the vendor lifecycle: Pre-signing, post-signing, and incident response.

Note that all these aren't the times at which these considerations will come up. This should all be discussed and assessed prior to signing with a cloud vendor.

PRE-SIGNING

As part of your due diligence in this phase, you should ask what security measures your potential cloud vendors have in place, whether those security measures carry over to your data, and whether or not they're complying with standards required by your industry and theirs. You should also know where your data is being stored and how it's being secured. What kind of encryption is in place? Does the cloud environment provide access management capabilities?

If the vendor can point to any independent security validations, that's a good sign. If not, then you need to either validate their claims via your own means or a third-party tool. Only in extreme circumstances do you take their word for it (this can be the case with very reputable cloud vendors). If they're expected to interact with business critical assets, it's in your organization's best interest to take the time and resources to validate any of their security claims.

POST-SIGNING

Security considerations don't end once the contract is signed. Ideally, you'd want to apply any monitoring, visibility, and detection tools and processes to your vendor or at least to the cloud environment your data is being stored in. If you can't, then your cloud-based vendor should provide some kind of method of accountability. This can be in the form of reports, ratings, or a continuous feed of data monitoring tools that your security team can plug into. Third-party assessment tools can help here too.

While Deny is skeptical of some assessment tools, noting that there's "no silver bullet," he does concede that these tools can provide directionally correct data if used on a continuous basis. And, if used as part of a due diligence process, those assessment tools are helpful in rating a cloud vendor against another.

It's also important to know what kind of third-parties or subcontractors your vendor will be using and whether or not those third parties or subcontractors will interact or have access to your data. How deep do these relationships go? The more third parties your third party has, the less visibility you'll have so make sure it's something you bring up.

INCIDENT RESPONSE

This is arguably the most important consideration because it gets into the heart of risk management. You need to know what your vendor's incident response plan is, what happens to your data and their cloud environment in the case of a breach, and whether or not that aligns to your own processes.

Knowing their communication strategy during an incident is extremely important. You don't want to be in the dark about a breach longer than needed. It may affect your own responsibilities and exacerbate the consequences of the data breach.

For example, if a Service Level Agreement (SLA) between you and your customers requires you to disclose a data breach within a week, but your cloud vendor's SLA has a month-long notice, that time gap puts you at risk.

Knowing what your cloud vendor can be expected to do or provide during a security incident can help you identify new potential security gaps and will help you understand how you need to shift or adapt your security strategy to account for this cloud vendor. For example, you might need to consider new security tools that provide additional detection or monitoring capabilities, or you may need to change your organization's data infrastructure to prevent any malware from reaching your servers from a third party's cloud environment.

As you assess your potential cloud vendors, you're not looking for a right answer, you're looking for security compatibility and assessing whether any additional risk taken on by signing with a cloud vendor is worth the benefit. If you have an understanding of your organization's risks and security processes, as well as your security department's capabilities, you should have enough information to choose the right vendor, or to find an alternative if your initial choice isn't meeting your security and compliance requirements.

As you reach the contracting phase, you should have a clearer understanding of what kind of risk a cloud vendor brings to your organization and have plans to properly address it. For example, you may be able to change certain terms or contract details to reduce your risk and ensure your cloud vendor isn't leaving all the responsibility up to you.

"It's a shared responsibility," Mann says. "The cloud provider is usually responsible for network communications and systems, but they're not responsible for your data. You should be responsible for having the right protections."

Being able to change terms and conditions can be easier when it comes to startups and other smaller cloud vendors who are eager to get a deal signed. However, larger companies are less likely to budge.

When considering the cloud vendors that are already part of your environment, the considerations listed above will help you identify what risk these vendors have exposed you to and identify what clauses or terms in SLAs, contracts, or Terms & Conditions (T&Cs) need to change come renewal time. In the worst-case scenarios, you'll either discover that some vendor contracts need to be terminated immediately due to the risk exposure or you may have to make plans to find an alternative vendor come renewal time.

Cloud Providers Are Third Parties Too

Whether an organization has completely migrated to the cloud or taken a hybrid cloud approach, they're likely working with one of the three biggest players—AWS, Microsoft Azure, or the Google Cloud Platform. Due to the importance, pervasiveness and size of these companies, organizations often forget that these cloud providers are third-parties and they fail to properly vet them as such.

When making assessments, much of what's been discussed already applies but one significant difference compared to smaller cloud-based third-parties is contract inflexibility.

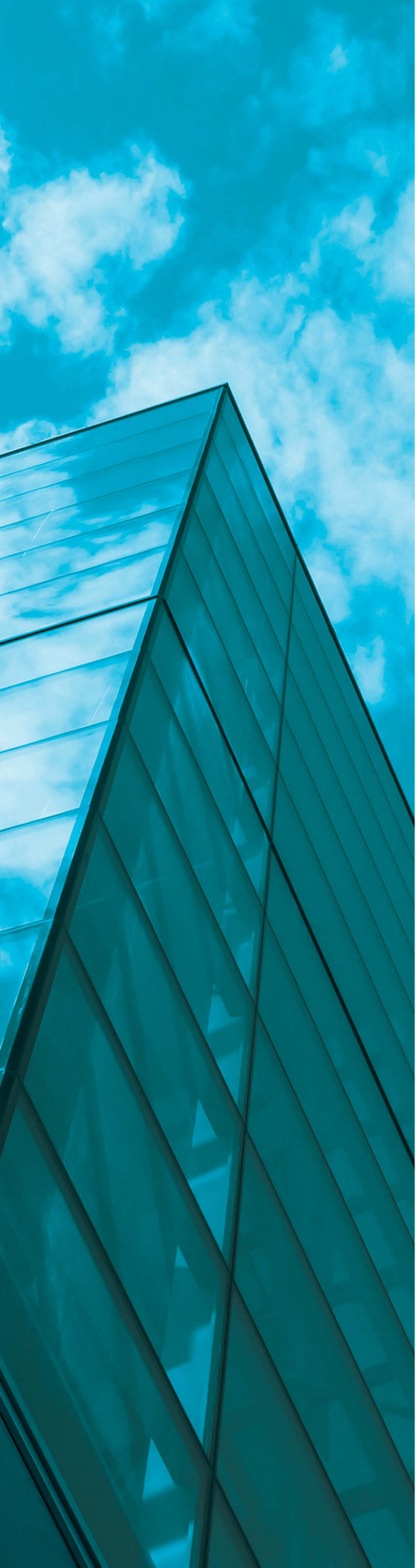
"Part of cloud vendor risk management is to accept the risk of not being able to change contracts," Mann says.

Smaller organizations will find it hard or nearly impossible to change T&Cs in contracts and SLAs. That means they have to pay very specific attention to their own environment and how its integrating with your cloud provider to ensure you have the right security measures and cloud architecture in place.

Ongoing security and risk management for cloud providers such as AWS can present distinct challenges. Given your infrastructure is so integrated with these cloud providers, or because they're providing the infrastructure itself, the kind of monitoring and ongoing detection required needs to either be done with the providers own native tools or third-party security tools. [See Part 2 for a deep dive in selecting the right tools for cloud provider security.]

The Risk of Improper Architecture Setup

Mann recalls a time when an AWS' service went down. Amazon's SLA only required them to communicate the problem and they did. However, some companies, due to improper architecture, ended up losing their AWS data. It's a costly lesson, so remember that the risk is always on the side of the organization.



The Aftermath: Ensuring Your Organization is Still Secure

If you ask yourself, “What happens when my cloud provider is breached,” you may as well be asking “What happens if my organization’s breached,” according to Deny.

He suggests organizations take a *when* rather than an *if*-based approach to breaches when it comes to cloud vendors. This means making decisions based on an assumption that a breach is inevitable, not an assumption that you can prevent a breach from ever happening.

This shift in security mindset allows organizations to take a more adaptive approach in how they can defend themselves and their environments. For example, Deny brings up how one organization’s CISO was less concerned about having their cloud environment being breached because their cloud only stored consumer product data, not intellectual property. Instead, the CISO was worried about malware infecting his environment and consuming CPU cycles, further increasing the cost of ownership.

By taking a more realistic approach and carrying out the thought experiment that one day you will be breached via your cloud-based vendor, you can better identify the threats that will impact your organization the most, helping you put more effective security measures in place.

“An attack is a mission,” Deny says, framing how threats should be considered. “It’s a project and it has a lot of different steps. Like many projects, there will be milestones, delays, and dependencies.”

There’s often a long period of time between when a malicious threat actor enters your cloud environment and when the attacker exfiltrates your data or leaves your cloud environment completely.

If detected early enough, this gives you and your cloud provider time to react to and put in additional measures in place to either mitigate the damage or outright eradicate the intruder. This is why it’s important to know and align with your cloud provider’s communications and incident response plan.

Your Strategy for Effective Cloud Vendor Risk Management

As organizations stack up cloud-based vendors and migrate to cloud or multi-cloud environments, security and risk management becomes its own challenge. With every new cloud vendor, your attack surface increases and your visibility is diminished. And with cloud-as-a-service providers, or infrastructure-as-a-service providers such as AWS, you may be faced with an entirely new set of challenges such as finding the right security tools for your new cloud environment, training your security department to properly understand cloud environments, and integrating your legacy monitoring and detection tools to a cloud-based environment.

Security leaders have to resort to a combination of using various tools available to them, either upskilling their team or staffing up with team members that have cloud-specific skillsets, and potentially consulting with a trusted security advisor or partner that's well versed in cloud security.

Again, you should approach cloud vendor risk management with the knowledge that you're assuming all the risk. As a security leader, your goals are to choose the right provider, vet them with proper due diligence, and take the appropriate internal actions to integrate them properly and patch any potential security gaps that might surface.

It's a lengthy process and you'll find nuances and differences depending on your vendor. Taking the time and deliberation now will keep your organization prepared during an inevitable security incident.

The Trustwave Cloud Vendor Risk Management Cheat Sheet

Cloud vendor risk management is a long arduous process that's constantly changing but it doesn't mean you can't get started. This cheat sheet provides you with the fundamentals needed to vet your cloud-based vendors effectively. As you perform your due diligence with this cheat sheet, you'll be able to adapt and shift your process depending on how integral a vendor is to your business and whether or not they're interacting with critical data. Be sure to answer the following questions:

1. WHAT IS YOUR VENDOR BRINGING TO THE TABLE?

While you should rightly assume the risk of a data breach, it doesn't let your vendor off the hook. Identify how your cloud vendor is addressing security and compliance concerns and make sure that they're validated by a party other than your vendor (this could include you). You should also find out whether working with this vendor will change any compliance standards you may have to now adhere to, given how new regulations cover more and more companies around the globe.

2. WHAT SECURITY RELATIONSHIP CAN YOU HAVE WITH YOUR VENDOR?

Depending on the vendor, you may have limited access to security measures on the cloud, especially if your vendor is working within a closed cloud environment (SaaS applications come to mind here). However, with some vendors, you may be able to apply your existing security controls (such as monitoring and visibility tools) to your vendors or you may have the option to use native or third-party security tools. It's important to know how well-integrated your security is with your cloud vendor so you can address any new security gaps.

3. WHAT'S THEIR PLAN IN THE CASE OF A SECURITY INCIDENT?

How soon will you know about a data breach? What happens to your data? Is your access affected? Does their incident response and communications plan align with yours? You have to be certain about the details here because you likely have your own disclosure requirements with customers or partners. You also want to know whether or not your organization's business functions are still able to be carried out in the case of a data breach or if a cloud provider's **incident response plan** will limit you.

4. HAVE YOU REVIEWED THE T&Cs, SLAs, AND BUSINESS CONTRACT?

There are a lot of details in this paperwork that point to the responsibility each partner has to each other. Review these agreements and flag anything that might expose you to unnecessary risk or liability. This might be a clause allowing unvetted third-parties to access your data, or a complete waiver of liability on the cloud providers' side. This is your chance to make sure you're not putting your organization in unnecessary risk.

PART 02

TO BE OR NOT TO BE (NATIVE)

ARE NATIVE OR NON-NATIVE SECURITY TOOLS APPROPRIATE FOR YOUR CLOUD ENVIRONMENT?

As multi-cloud environments become more of a norm for digital enterprises, security leaders are faced with a new challenge: choosing the right tools to address their cloud security concerns.

If that wasn't a difficult enough choice, CISOs trying to maintain security and visibility over their organization in a cloud environment also need to make the choice between using native or non-native tools.

Cloud providers like AWS, for example, have introduced a swath of native security tools for their users. However, leaders can also choose from third-party, non-native tools. This further complicates the decision for a security leader who already has to consider budget and team availability, among other things, before introducing a new solution to their security team.

The Rise of Cloud Providers

ACCORDING TO GARTNER'S FORECAST:

Public Cloud Services, Worldwide, 2016-2022, 4Q18 Update report, the worldwide public cloud service revenue market is expected to grow exponentially to USD$331B by 2022, up from USD $182B in 2018.

$331BILLION
2022

$182BILLION
2018

Gartner Press Release, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019," April 2, 2019. https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

There are pros and cons to native and non-native cloud security tools and these choices can have a long-term impact on an organization, shaping how a business approaches cloud security as it grows and continues to adopt new digital technologies.

Whether an organization is relying on a single, hybrid, or multi-cloud environment (or if it will in the future) is also an important consideration. Business departments may rely on different cloud providers depending on their needs and even geographical locations, which may affect which cloud environments are available.

To address these security concerns, and ensure they're making the right choice, leaders must understand their organization's internal risk, find the right cloud security approach that's best for their organization, identify what kind of security tools they need, consider their organization's roadmap, and then choose the right tools. It's a process that, if done with the correct approach, can have positive repercussions throughout the organization's digital transformation.

Looking Inward to Identify the Right Tools for Your Organization

How can a security department ensure their tools are just as effective at monitoring, detecting, preventing, and responding to incidents if their organization is cloud (or multi-cloud) based? Before you can properly make the decision between using native or non-native tools (and making a selection), you need to conduct a cyber risk tolerance assessment to understand specific security needs.

KNOWING YOUR ORGANIZATION'S RISK TOLERANCE

Determining the business's risk tolerance will help narrow the focus of your search, seeing as it can vary greatly depending on which organizational department is relying on a cloud provider, what cloud provider you're using, and what cloud-based assets need to be secured.

"A risk-based approach is absolutely needed here," says Chris Schueler, senior vice president of Managed Security Services at Trustwave. "This isn't a process to vet tools but a process to identify the tools. A risk-based approach guides you to the kind of categories and tools relevant to those cloud environments."

For example, payment card data is one of the most critical and high-risk assets in the hospitality industry. Whether or not that data is migrated to the cloud should inform what kind of cloud security tools an organization requires (likely visibility and detection). However, if credit card data stays within an organization's own database, and instead, supply chain partner data is on the cloud, then a different set of tools might be required for an organization's cloud infrastructure.

"This isn't a process to vet tools but a process to identify the tools. A risk-based approach guides you to the kind of categories and tools relevant to those cloud environments."

Chris Schueler
Senior Vice President of Managed Security Services, Trustwave

KNOWING WHAT NEW THREATS AFFECT YOUR ORGANIZATION

Cloud-based critical assets and cloud-based databases face a different set of threats compared to assets that are found on premise. According to Symantec's Cloud Security Threat Report, Adapting to the New Reality of Evolving Cloud Threats, the top three cloud threat categories include managing identity and authentication, phishing, and accidental insider threats.

These three categories offer just a glimpse into what the threat landscape has to offer in a cloud environment.

"Before [the cloud], attackers would hit the perimeter," says Matthew Lorentzen, principal security consultant at Trustwave SpiderLabs. "But now, with the cloud facilitating a single sign-on approach to many services, that attack surface spreads out."

Due to the flexible and accessible nature of the cloud, it becomes very easy to lose sight of what assets are moving in and out of cloud environments, what assets have accidentally been exposed, and who has access to what within a cloud environment. These primarily internal threats require a shift in how you approach security. Needless to say, the days of solely protecting the perimeter are long gone.

Security leaders need to be aware of how critical their cloud environments are to the business (a varying scale) and how that affects which cloud security threats your organization is most likely to face. Again, determining the risk tolerance level of the business will only help in painting that picture.

Ethereal Vulnerabilities

Lorentzen highlighted a vulnerability specific to cloud environments: "ethereal vulnerabilities." These are short-lived vulnerabilities that might have exposed some assets for a very brief period of time, putting your organization at risk. He stresses that the right kind of cloud security tools, whether native or non-native, should be able to detect these kinds of vulnerabilities before they lead to negative consequences like unwanted data exfiltration or public disclosure of the vulnerable assets.

"But now, with the cloud facilitating a single sign-on approach to many services, that attack surface spreads out."

Matthew Lorentzen
SpiderLabs Principal security Consultant, Trustwave

Knowing Your Organization's Needs and Capabilities

Once you have a better understanding of your organization's risk tolerance and the threats surrounding your critical assets, you're one step closer to determining what tools will best fit your security strategy.

Visibility is critical when it comes to cloud security, but it's important to know the extent of visibility you need. Will you need endpoint monitoring, basic log or database monitoring, or are your needs more specific and advanced? These answers will vary depending on what data is being stored on the cloud and should help you filter out what tools you may or may not need.

It's imperative to also consider the talent and skillset of your security team. Do you have a unit dedicated to AWS or just one individual? Are you planning to hire security personnel that specializes in protecting cloud environments? The size of your team should influence the decisions you make surrounding security tools.

For example, while 100 percent visibility is always the goal for any security department, it's always a moving goalpost that varies depending on your business's maturity level.

"One struggle organizations face is the need to have and see everything," Schueler says.

He and Lorenzten both stress that even if you have the right tools delivering complete visibility, you'd also have to ensure your team has the time and skills to use those tools effectively.

Cloud security requires specialized skillsets and many organizations may not have the right security staff capable of leveraging all the tools available to them by both cloud providers and third-parties. A knowledge base surrounding cloud governance tools, authentication mechanisms, encryption and data compliance are essential. As you determine your organization's cloud security needs, supplemental assistance provided by a trusted security advisor is a great option to steer you in the right direction.

"Even if you have the right tools delivering complete visibility, you'd also have to ensure your team has the time and skills to use those tools effectively."

Chris Schueler
Senior Vice President of Managed Security Services, Trustwave

Why Reducing Complexity is Key

Ultimately when it comes to choosing the right cloud security tools for your organization, it's important to remember why they exist in the first place. They're designed to make security easier for you and your team. However, there's no one approach to reducing complexity. Here, Schueler and Lorenzten lay out several options.

"Having a multi-cloud strategy is the first thing [your organization] should agree on as something that's vitally important for your security architecture."

Chris Schueler
Senior Vice President of Managed Security Services, Trustwave

Schueler recommends favoring non-native tools when possible if they have the ability of working across multiple cloud environments. Even if your organization is running on a single cloud, that likely won't be the case in the future. Using one tool for multiple cloud environments can be a huge time and cost-saver, especially in the long run, due to the flexibility and applicability it provides.

"Your business isn't going to stay in just one cloud", Schueler says. "Having a multi-cloud strategy is the first thing [your organization] should agree on as something that's vitally important for your security architecture."

This multi-strategy approach can help ensure an organization steers clear, or at least mitigates, some of the common issues having a multi-cloud environment brings up. This could include duplicating teams for different cloud environments, having to re-engineer architecture whenever data is moved from one cloud platform to another, and increasing the challenges presented by the industry's talent shortage, especially when it comes to cloud-specific skills.

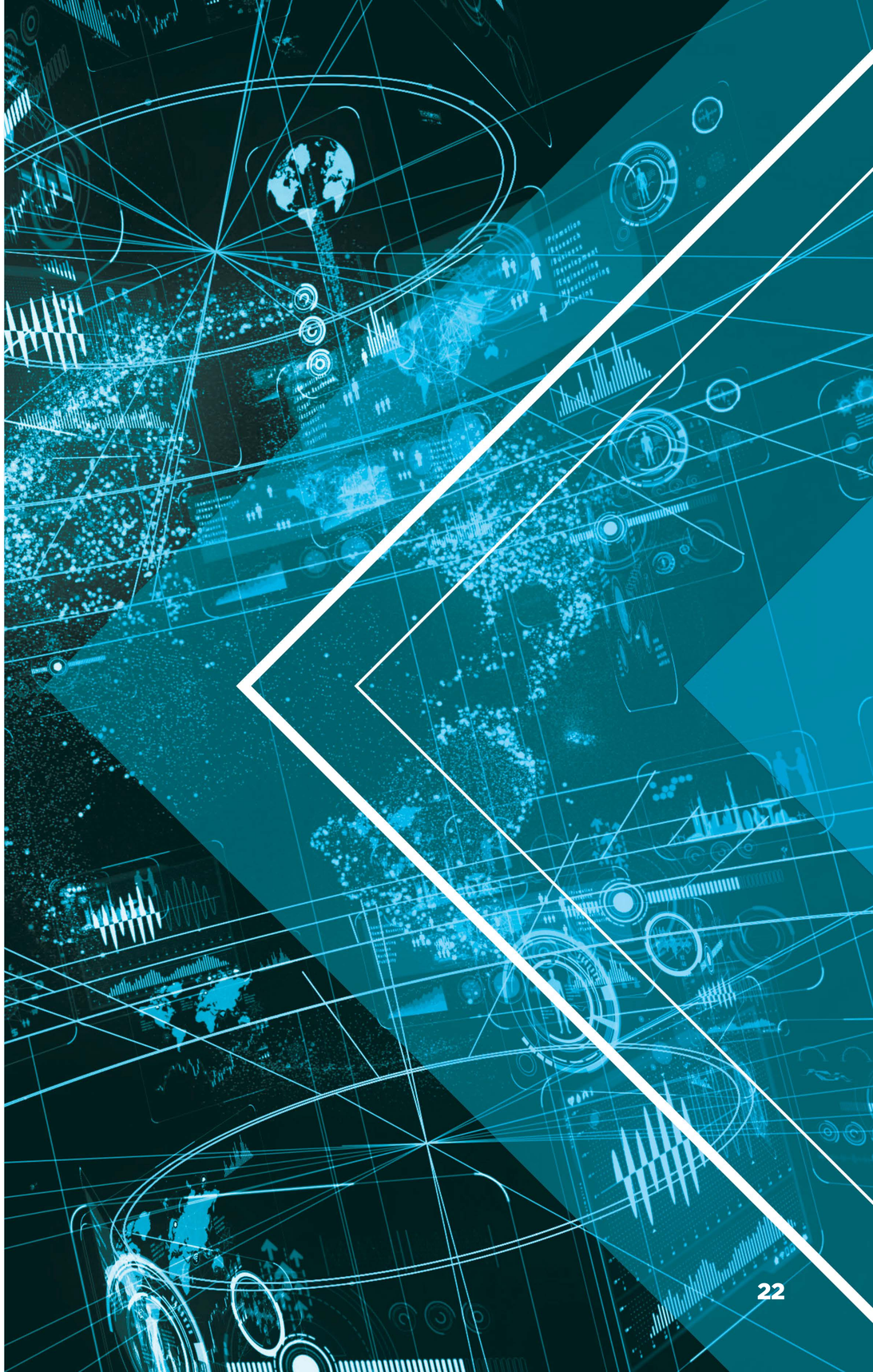
Even if certain tools can be used across multiple cloud environments, the benefits are minimized if individuals and teams can't work across different cloud environments.

However, that doesn't necessarily mean non-native tools are always the best way forward. Native tools help in reducing complexity for a security department because they keep a lot of the work and function of a team within the cloud environment.

Lorentzen sees having too many non-native security tools as increasing complexity and possibly the attack surface of an organization.

"Every time you enable or take on a new non-native security tool you introduce potential security considerations if you don't understand the impact on your environment," he says. "What permissions are you giving them? Does it introduce risk into your environment?"

Rather than having your current team grapple with the learning curve tied to new solutions, having everything housed under as few platforms and tools as possible is best for efficiency and risk management. Native tools don't add additional platforms and are designed to work seamlessly with the corresponding cloud environment, so a team well versed within that cloud environment is already equipped to maximize the benefits of that solution.



Regardless of the approach, both Lorentzen and Schueler stress the fact that enterprises with cloud infrastructure(s) have very different skillset needs and often need to hire for that specialty within cloud security or cloud optimization in order to have an effective security department.

“Skills and talent in the cloud are very different than traditional infosec skills,” Schueler says. “It’s difficult to find someone who understands cloud configurations and knows how security tools work within different cloud ecosystems.”

“Businesses have a wealth of information available in terms of security posture, but you need knowledgeable people who know environments and know how to take that data and make it actionable”

Matthew Lorentzen
SpiderLabs Principal Security Consultant, Trustwave

Lorentzen stresses that a well-equipped security department will help organizations make sense of the information cloud security tools provide.

“[Businesses] have a wealth of information available in terms of security posture, but you need knowledgeable people who know environments and know how to take that data and make it actionable,” he says. “They need to have a good understanding of cloud infrastructure.”

Depending on the approach that resonates with both your organization’s risk tolerance and environment, understand that these considerations must start at at the organizational level, not just the department level. Make sure you have the approval and budget required to staff your team up with the right skillset to leverage any new security tools. Otherwise, you may end up purchasing new security solutions, but lack the team or skills to maximize their use.

Making Your Decision: Native Tools Versus Non-Native Tools

Remember that considerations such as ease of use, available skillset, and which cloud vendors your organization is working with all need to be taken into account to help you make a decision on which route to take on native or non-native cloud security tools.

Before you make a final decision, Schueler recommends answering these three questions:

1. **Are you working within a closed cloud system?**
   This is often the case with SaaS companies and certain cloud infrastructure architecture setups. This also makes the choice easy—because of the closed environment, you don't have many options other than to use the cloud provider's native tools. Even if there are third-party tools available or native connectors for third-parties, they likely won't have the same functionality or provide the breadth of visibility or security required.
2. **Is the non-native tool applicable for multi-cloud environments?**
   As mentioned before, one of the major benefits to using third-party tools is their ability to provide multi-cloud support. Cloud complexity is its own challenge - using one tool to account for multiple cloud environments will reduce the load on your security team and prevent your organization from becoming siloed due to internal cloud segmentation, which can create problems as your organization grows. However, if a non-native tool only works on a single cloud environment, you may want to strongly consider the native tool as it might be more reliable, provide better visibility and detection, and garner better support given that it's tied to the cloud provider.

Pitfall to Avoid: Using Too Many Security Tools

Don't overload your security team with too many tools, whether native or non-native. This is an easy mistake to make - the market for cloud security tools has grown immensely. A forecast by Market Research Future has the cloud security market reaching USD$13B by 2022, up from USD$5B in 2016.

However, security organizations already struggle with a cloud security talent gap. Given the specific skillset required to properly handle cloud security and leverage relevant tools, an organization may not have the right team for their cloud security. This means stacking tools on your department won't necessarily solve the cloud security problems your organization is facing.

If your security department is inundated with tools, they'll likely be less effective, leaving your cloud environment and organization insecure at the cost of your company's valuable resources.

3. What's the business's roadmap look like?

This question applies externally and internally. Knowing whether or not your organization is planning to adopt more cloud providers and knowing what assets will fall under these new cloud environments will help you make a decision for the long-term. However, knowing the security vendor's roadmap is also important. Are they planning to add more multi-cloud support or integrate deeper with your current cloud environment? Do they have other technology partners that you're currently working with? Knowing this will facilitate better decision-making for your organization now and in the future.

Don't Overcomplicate Your Decision

Ultimately, if you're just starting out using cloud security tools, you should focus on making your team as effective as possible. This means taking an 80/20 approach to tool selection, starting off with tools that will have the most impact on your cloud security. Don't get overwhelmed by the selection and think back to security basics.

"Do you what you'd do in a non-cloud environment," Schueler says. "Stick to visibility, scan your data, harden apps, manage access. Remember, you don't have to recreate the wheel."

You can also look at partnering with a managed security services provider or consulting with a trusted security advisor that can provide supplemental assistance. This will save you time and money in the long run in case it's a challenge to find the personnel with the right skillset. These long-term partners are key in ensuring your multi-cloud environment is accounted for.

“An MSSP isn’t tooling or third-party,” Lorentzen says. “It’s more of a consultancy made to augment a department. While it expands the supply chain, it eases the burden on security.”

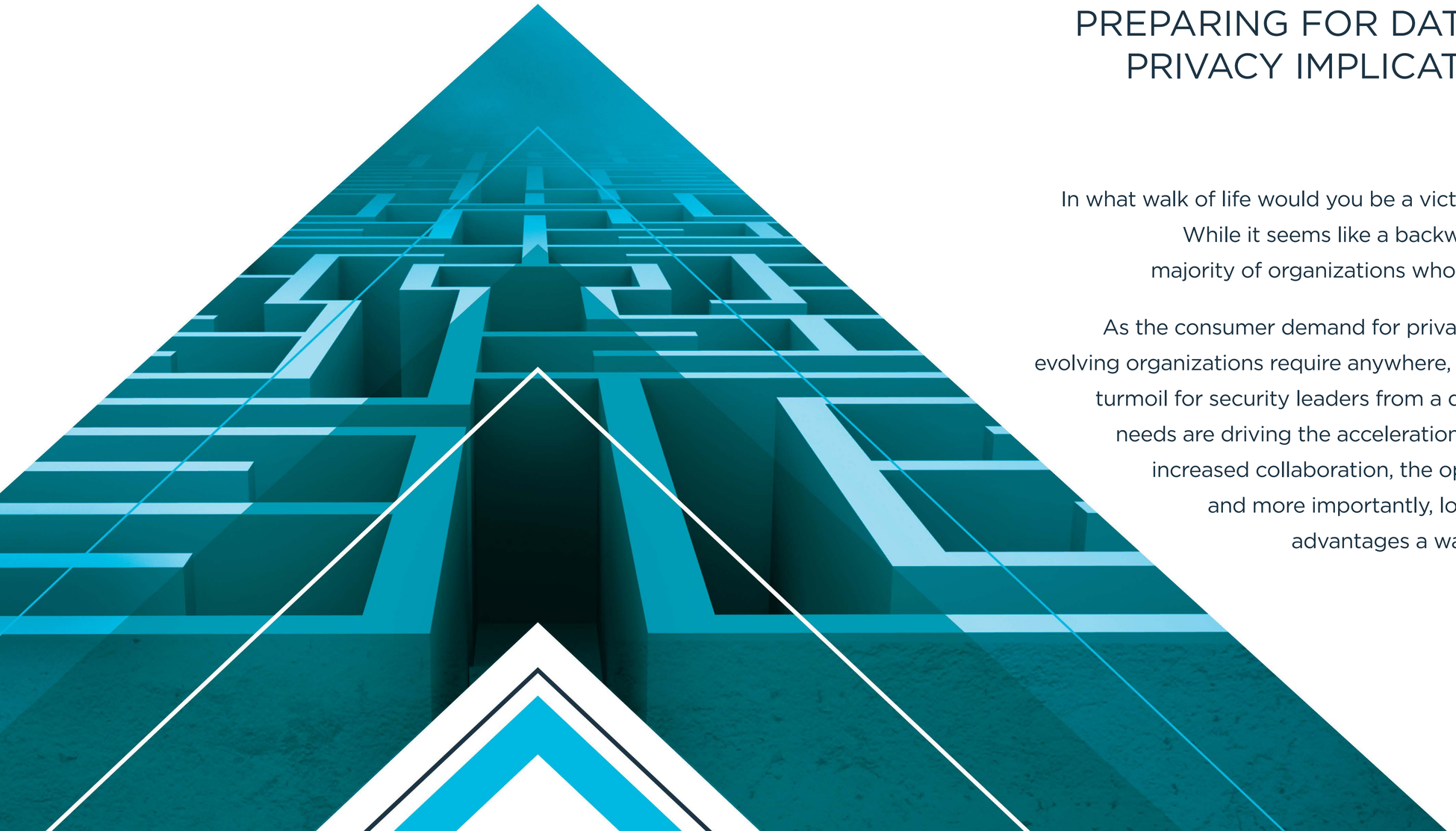
Both the approaches outlined by Schueler and Lorenzten have long-term advantages because they prepare an organization with the ability to take on new challenges as it grows and adopts new cloud partners or finds themselves needing to use more advanced visibility and security tools.

There’s no silver bullet when it comes to security. When it comes time to make a decision surrounding security, consider different strategies and approaches that fit the risk profile of your organization. Managing complexity and focusing on making your department as effective as possible is key, as is having a strong understanding of your organization from a risk and security perspective. By conducting some of this internal homework, you’ll be better equipped to handle this cloud security challenge now and for the coming years ahead.

PART 03

NAVIGATING THE PRIVACY LABYRINTH OF CLOUD DATA

PREPARING FOR DATA PROTECTION AND PRIVACY IMPLICATIONS IN THE CLOUD.



In what walk of life would you be a victim of a crime, only to get fined for it? While it seems like a backwards concept, it's a harsh reality for a majority of organizations who fail to protect the data they manage.

As the consumer demand for privacy continues to increase and digitally evolving organizations require anywhere, anytime access, this creates strategic turmoil for security leaders from a data governance standpoint. Business needs are driving the acceleration of cloud migration, with promises of increased collaboration, the opportunity to scale quickly and easily, and more importantly, lower technology costs. But with these advantages a wave of complexity presents itself from a cyber risk standpoint.

For organizations operating globally, these challenges quickly multiply as dispersed data located in multiple cloud environments makes it particularly difficult to locate, protect, and ensure its privacy given the varying laws and regulations that differ from country to country. This results in a risk labyrinth that security leaders need to navigate to effectively protect information and be compliant in a world where the data privacy discussion has been elevated to new heights.

As global businesses continue to transform digitally to increase revenue and exponentially grow their value, privacy and security need to be a part of that transformation conversation. Identifying who accesses data and when has always been a major focus for security leaders, but as digital transformation expands the availability and need of data, privacy and security are beginning to converge.

Gone are the days when discussions surrounding privacy and security are siloed. To successfully manage cyber risk within the business today, the understanding and internalizing of privacy regulations has to be seen through to the effective operations of the mechanisms put in place to be compliant and protect data.

Now more than ever, security leaders must ensure that the connected enterprise of today takes a holistic approach to being cyber resilient, one that takes into account the geographic implications of dispersed data the organization manages. The understanding of data ownership plays a central role in this cyber risk journey, especially as organizations are attached at the hip with cloud providers. To reach that ideal state of protection, security leaders must overcome three primary challenges that will present themselves along the way.

The Visibility Challenge

To protect something, you have to be able to see it. Although tangibility gets a bit diluted in the digital realm, the notion of visibility for security leaders plays a critical role in their overall purpose. The simple fact of the matter is, a majority of organizations don't know where their data is. This challenge grows in complexity as the environments and the surface of where the data is held changes—from different cloud environments and data centers, to endpoints. Migrating mission-critical applications to the cloud means losing a level of control and visibility.

If you also consider that databases can be hosted anywhere, securing the information housed in them becomes more challenging depending on the environment. More often than not, more than one cloud environment will be in play, meaning that reaching an ideal state of having a unified view of security, risk and compliance is much more difficult since there's a lack of security standardization in cloud environments.

According to Ixia's "The State of Cloud Monitoring" report, which surveyed 338 professionals who operate, secure, develop, deploy, or manage cloud applications or infrastructure, a majority of respondents (87 percent) shared a concern for a lack of visibility in cloud environments.[3]

Before tracking the organization's data gets out of hand, security leaders must ensure data migration by linking data assets and architectures as the organization grows, be it through a merger or acquisition, or a result of implementing new technology and applications.

"When you think about the different clouds that businesses are leveraging—be it AWS, Microsoft Azure, or basic applications that they've enabled in the Google Public Cloud—it's not the space they've acquired there that's the problem," says Bill Rucker, president of Trustwave Government Solutions, who assists government organizations in their data protection efforts.

"Product vendors are now cloud vendors, and cloud vendors are now product vendors, where do you draw the line on who's responsible for what?"

Bill Rucker
President, Trustwave Government Solutions

"The real concern is all of the different applications that they've moved or have enabled in the cloud, many times from a cost-savings standpoint."

This should immediately bring into question the level of trust that one would have to have for these multiple cloud environments to operate and be mission impactful, especially when those environments can't "talk" or are integrated with the entity's private cloud, Rucker adds.

"Product vendors are now cloud vendors, and cloud vendors are now product vendors," says Rucker. "Where do you draw the line on who's responsible for what?"

[3]Ixia Report, "The State of Cloud Monitoring," March 27, 2019. https://about.keysight.com/en/newsroom/pr/2019/25mar-nr19044-ixia-c-r-state-cloud-monitoring.pdf

The Ownership Challenge

So the big question is, when you're working with a cloud service provider, where do you draw the line when it comes to data ownership and protection? That's where the real complexity lies, in identifying where the responsibility for cloud vendors begins and ends. Needless to say, when it comes to your cloud adoption strategy, understanding vendor security and responsibility is paramount.

"I don't believe those 'lines' know what is in each other's area of responsibility," Rucker says of the ownership challenge when it comes to the role that cloud vendors play in security and privacy. "I think there's a pretty significant gap in that regard and it's an area adversaries will start to focus on."

The larger the organization, the more hurdles present themselves as more players are involved in the data game, leading to finger pointing when an inevitable security incident occurs. But before bringing the cloud vendors into the discussion, it's important to clearly identity the business owners of the data first, says Barry O'Connell, general manager, EMEA, at Trustwave.

"A lot of the data actually isn't owned by the security organization," O'Connell says. "The core data shouldn't be owned by the security organization. Even though defining the business owners of the data may sound bland, it's quite the challenge when you understand large organizations, corporations and government departments."

A City Cloaked in Secrecy

More than 77 years ago, the U.S. federal government took over 60,000 acres of land located near the border of East Tennessee. This was the birthplace of Oak Ridge National Labs, the facility where tens of thousands of people—many unknowingly—helped build the world first atomic bomb. Both residents and workers were preached privacy, with some billboard signs located nearby reading, "Loose Talk Helps Our Enemy, So, Let's Keep Our Trap Shut."

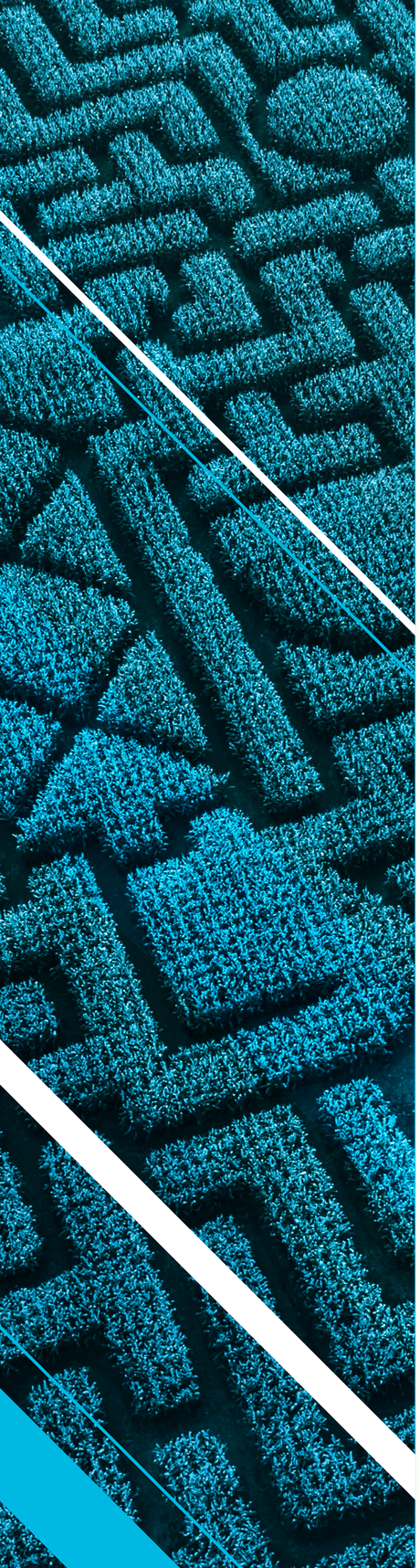
From scientists to traditional factory workers, all were sworn to secrecy inside the facility.

"You had your swim lane and you stayed in it," Bill Rucker, president of Trustwave Government Solutions says. "You didn't ask your colleagues what they were working on and they didn't ask you because it would be deemed a 'spill.'" A spill amounts to data, likely classified, ending up in a non-classified place.

In these types of secure work environments, everyone had their own independent tasks, and only as you moved up layers in the project did people understand what those independent tasks meant in the overall picture. Given the increased risk oganizations face today, Rucker believes that we could be seeing more of this disconnection in the future, only because it reduces risk.

Given the intricacies tied to protecting cloud data, both from a security and compliance standpoint—and the varying global regulation implications in play—many public cloud providers have drawn a line in the sand, indicating that they're in charge of securing the cloud, while their users are to protect the data itself. This shared responsibility model allows the organization to focus on protecting applications and the data themselves. When it comes to software-as-a-service providers, however, organizations are responsible for protecting just the data, not the applications and infrastructure.

Understanding and clearly articulating the ownership of the data you're trying to protect gets you one step closer to establishing a unified approach to securing critical assets in multiple cloud environments. The biggest mistake a security leader can make is to assume their cloud provider will address their privacy and security needs. Taking the same security measures to protecting data in the cloud as you would on-premise is the most successful path to take. Part of that journey should include a data strategy to meet the demands of current and emerging regulations surrounding privacy.



The Privacy Challenge

From Facebook's Cambridge Analytica scandal and the introduction of the European Union's General Data Protection Regulation (GDPR), to security breaches that impacted millions and dominated headlines, the privacy discussion was elevated to new heights in 2018. Events like this prompted a domino effect that have made governments, citizens, and businesses much more privacy-aware, resulting in increased attention into how personal information is stored, managed, and protected.

Many are beginning to think that the challenges data privacy present today are on par with those of the threat landscape, which begs the question: are privacy and security converging?

"When you get into cloud environments and privacy, it absolutely will start to tie into your traditional cyber threat landscape and it will be just as relevant," says Rucker. "In the privacy world, your data puts your organization and your customers at risk. It's absolutely on par with the threat landscape and it will be one in the same if not a higher area of risk."

"When you get into cloud environments and privacy, it absolutely will start to tie into your traditional cyber threat landscape and it will be just as relevant"

Bill Rucker
President, Trustwave Government Solutions

Ultimately, privacy will be a means to discussing the level of impact that something has, Rucker adds. The more impactful that data could be from a privacy or business perspective, the more it will be seen as a potential threat.

With the roll out of the GDPR in Europe, New Zealand's Privacy Bill, Chile's Privacy Bill Initiative, Brazil's General Data Protection Law, and California's Consumer Privacy Act, governments are waking up to the immense impact technology has on user privacy. But is this a question of privacy, or data protection? Rucker believes that at the end of the day, the ladder is what's really being focused on.

As President of Trustwave Government Solutions, Rucker has had his fair share of conversations surrounding privacy with U.S. government agencies in both civilian and defense. In his world, it always comes back to protecting the data.

“When you start talking about systems and how that could impact more than just the mission of the agency, but the people and national security tied to it…it’s almost always about data protection,” he says.

While security and privacy may be converging, O’Connell believes that the two are still pretty far apart and not as conjoined as they should be, an unfortunate symptom of the cybersecurity conversation of today. He says that from a risk register perspective, privacy should be at the top of any CISOs list. It’s the risk that should be managed against any privacy obligations that present themselves from a regulatory standpoint, all the way through the continuum, down to the tools, processes, and technology that’s deployed in the organization.

“From a purely risk and financial position, taking privacy more seriously and then implementing the mechanisms to ensure the privacy and protection of that data exists should be top of mind,” O’Connell says. “Because it will be a financial challenge, not just a regulatory challenge.”

If you’ve enlisted the help of a trusted security advisor to guide you through the protection process, security leaders must ensure that the outcome is consistent with the risk the organization bears around privacy. This is especially the case when working with security partners on the cloud security front.

A Different Era, Similar Goals

If the notorious 1920s bank robber Willie Sutton, aka “Slick Willie,” were still around today, he’d most likely be a cybercriminal setting his sights on compromising databases. Instead of being armed with a Tommy Gun, a laptop would likely do the trick.

Why would he focus on compromising databases? Well, according to an apocryphal story, he’d give the same answer he gave a reporter when asked why he robbed banks… “Because that’s where the money is.”

When you consider high-value assets and privacy, that privacy is meant to protect whatever’s located in the database—or the bank vault in his case. Sutton robbed banks because the benefit of the return on investment was much higher.

This is exactly why digital thieves opt to go after data stores, because of the valuable information they could benefit off of monetarily. And this is also precisely why privacy regulations are being introduced from country to country.

A Compass for Success

As a guide for security leaders aiming to navigate the risk labyrinth presented by multi-cloud environments, O'Connell has outlined four key areas of focus that will help them overcome the challenges presented from a visibility, ownership and privacy standpoint.

1. Locate Assets and Where They're Moving To

As the business digitally evolves, data environments will be going through changes along the way. It's important to understand where data is residing today, where it will migrate to tomorrow, and what the risks are in each of the environments it traverses. This is very much a planning and mapping exercise that organizations must work through. The larger the organization, the more challenging this can be, so many have opted to consult with security advisors that provide supplemental assistance with in-depth planning and help them identify current, target and future security states.

2. Map Out a Governance Structure

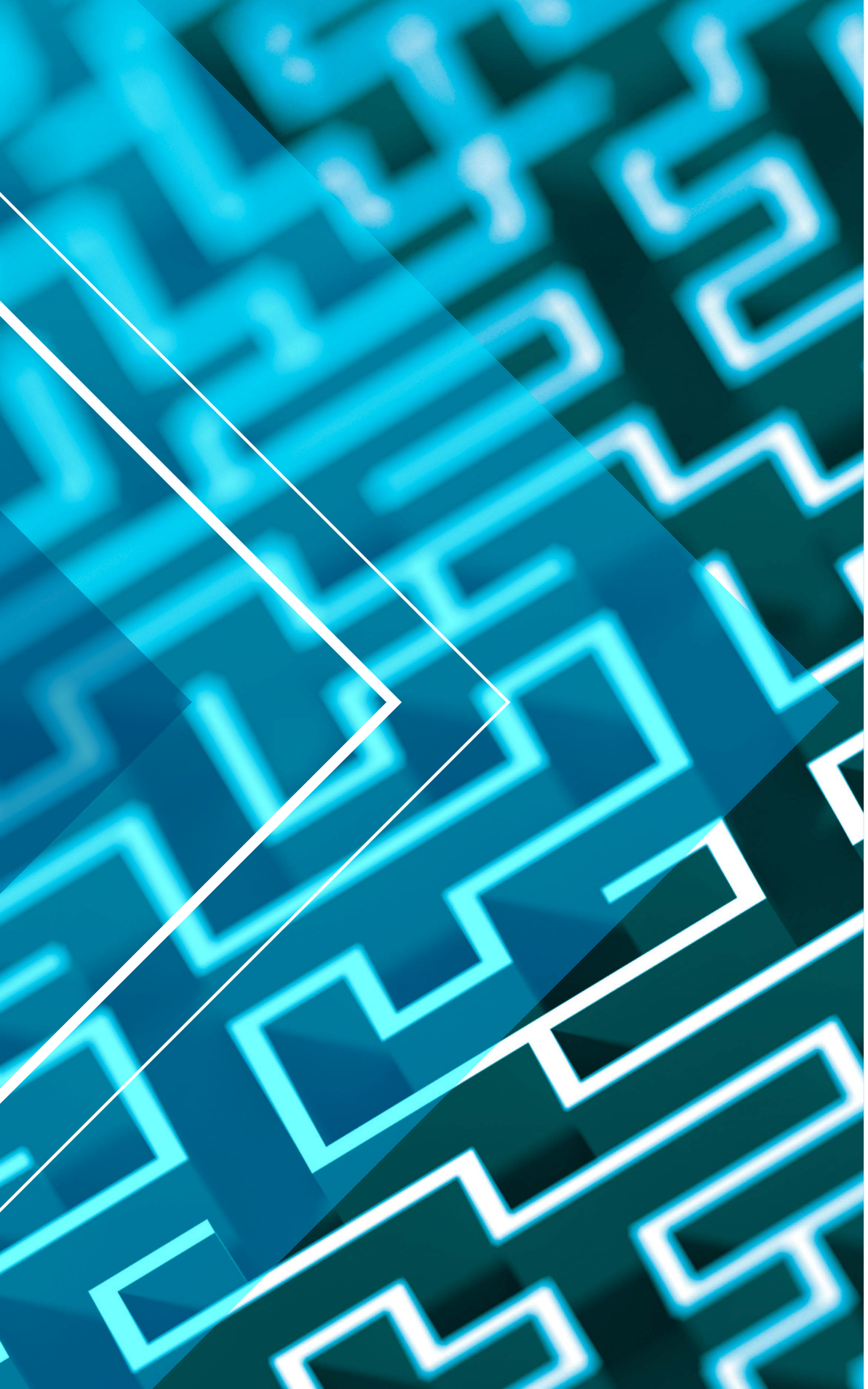
The first step of this process should be building and plotting out where the data ownership resides within the business. Security leaders must first assess the organization's overall risk tolerance, then make sure that the individuals in the business have a commitment to the company and regulators that those data sources are secure. As O'Connell states, "it needs to be a business decision to make those things happen, not just a security decision."

3. Create a Set of Metrics

It's important to have a strong security awareness and data protection program in place that aligns with the regulatory obligations the business faces. Make sure that the activities you're plotting together are integrated into one program and not run separately. Once these are in place you can then develop a privacy metric program that establishes evidence of compliance with said legislative requirements. As a board activity, this allows you to start talking about the organization's privacy program.

4. Develop a Response Plan

We know you've heard this time and time again, but as they say in information security, it's not a matter of if, but when. So what does happen if and when part of the mechanisms you put in place fail? How will you respond to that as an executive team both internally and externally so you're well prepared? The combination of working in multiple cloud environments, an increased attack surface, and a constantly evolving threat landscape can almost assure that you'll have an incident to respond to in the future, so it's imperative to have a response plan in place. Working in red teaming or purple teaming exercises is a great way to prepare your organization for the approaches their adversaries would take, which sharpen your defenders' skills and increase security maturity in the business.



As you maneuver through the challenges presented by multi-cloud environments, reaching a state of cyber resiliency that integrates tools, processes and people is obtainable. Understanding the looming challenges you face as a security leader will allow you to adjust your approach to data privacy and protection and enlist supplemental assistance in the areas that best your service organization.

A proactive, forward-thinking approach to privacy will allow you to introduce tangible controls around the organization's data, but most importantly, keep you one step ahead of the difficulties presented by both the threat landscape and expectations set by regulatory bodies.

Trustwave®

Trustwave is a leading global cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses navigate the digital transformation journey securely.

As organizations continue to evolve their processes and operations, leveraging multi-cloud environments, Trustwave can help ensure they protect where their data resides and where it's migrating to through a variety of services that include:

INFORMATION SECURITY ADVISORS

A dedicated security advisor with deep security expertise adds value for your team by serving as a single point of contact for technical escalations, guiding the development and implementation of security policies, and providing context to alerts and escalations.

CONSULTING AND PROFESSIONAL SERVICES

Our Intelligence Security Operations (iSecOps) consulting team helps you create an agile, go-forward plan to improve security maturity as you migrate mission-critical data to multi-cloud environments.

THREAT DETECTION AND RESPONSE

Trustwave Threat Detection and Response services provide quick and effective response to cyber-threats to minimize—or even eliminate—potential damages from malicious activity.

Trustwave®

www.trustwave.com