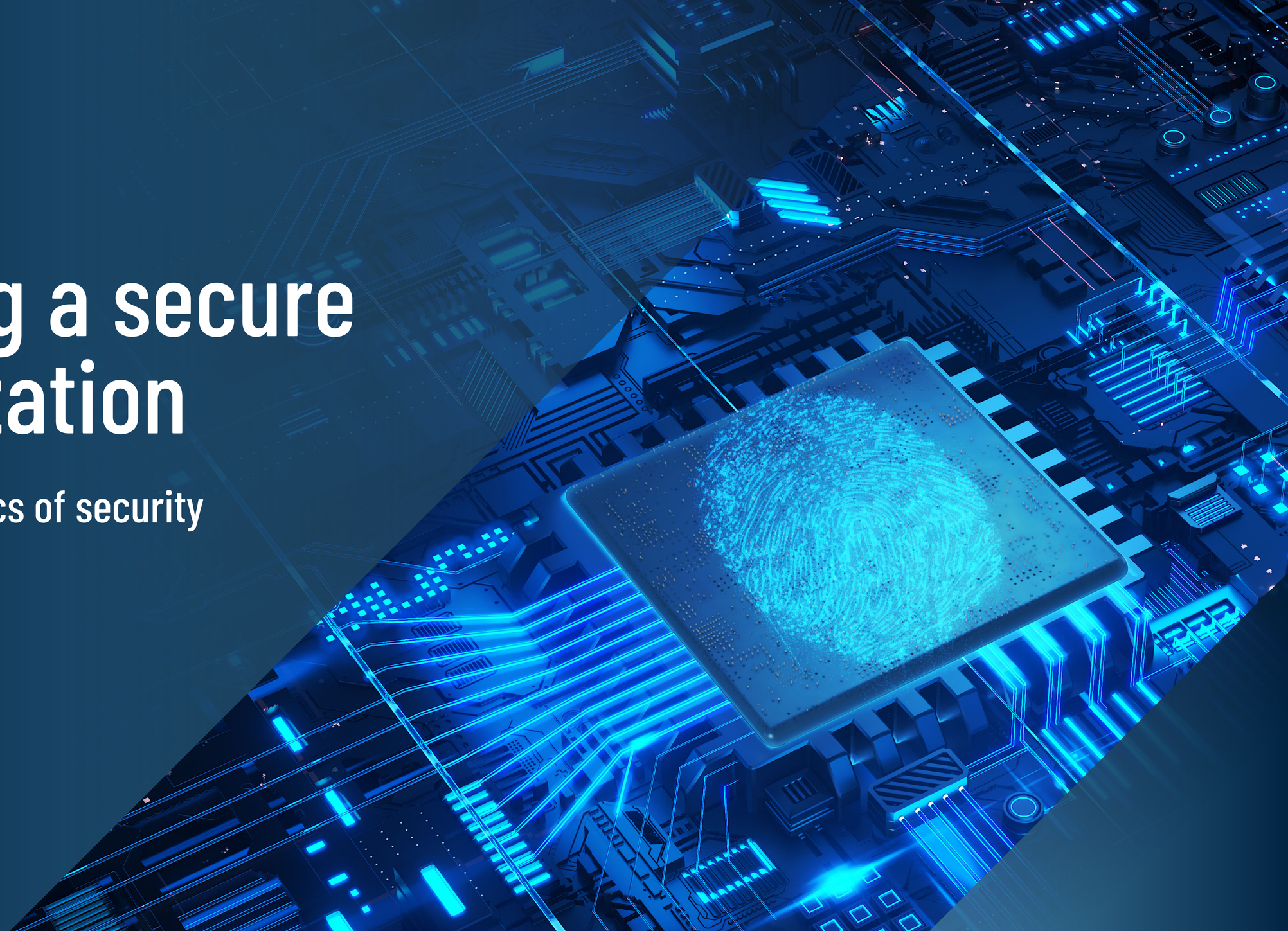
protiviti®
Global Business Consulting

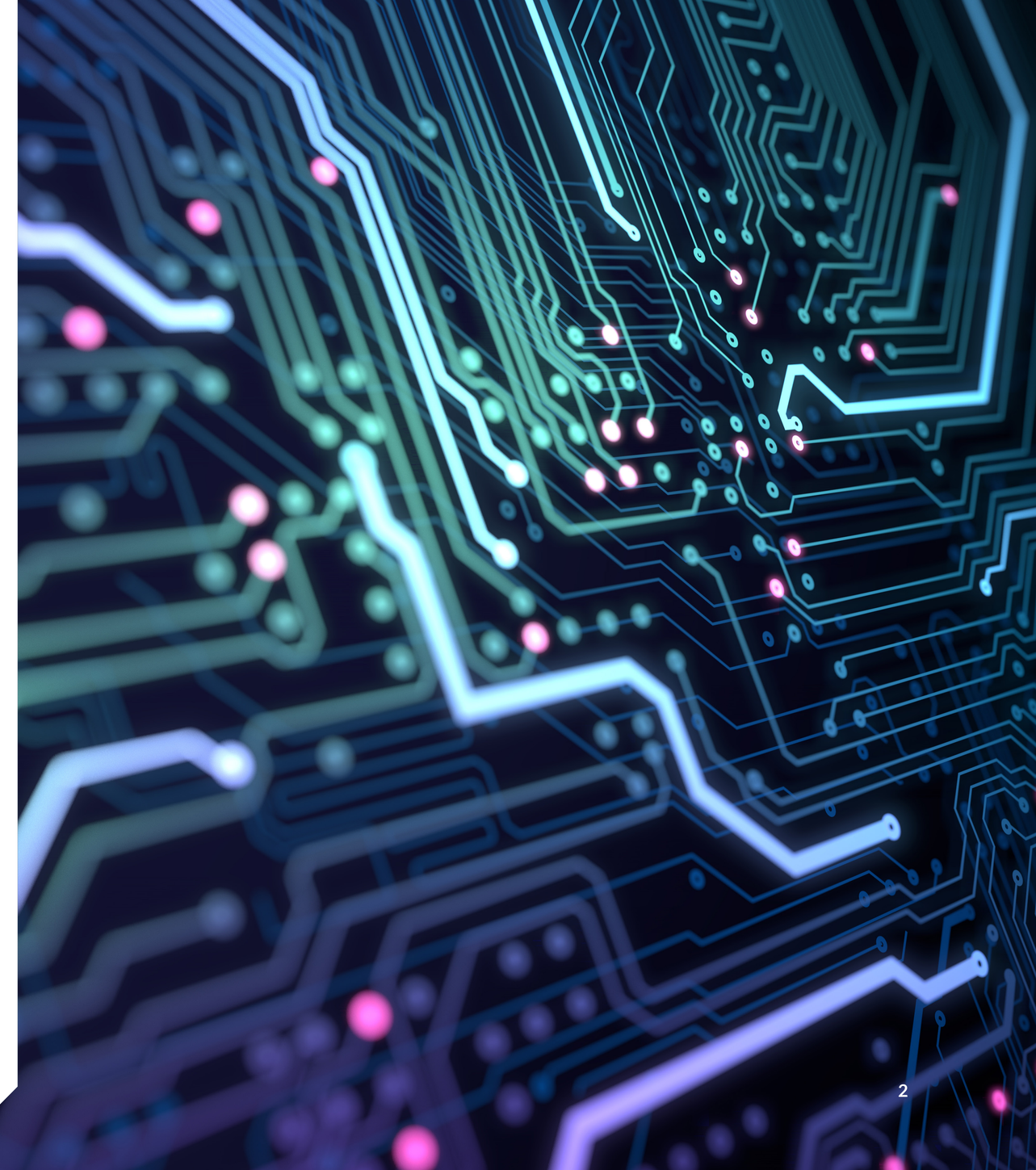
Building a secure organization

Beyond the basics of security



aws
PARTNER
Advanced Tier
Services

Contents



Building a secure organization: beyond the basics of security

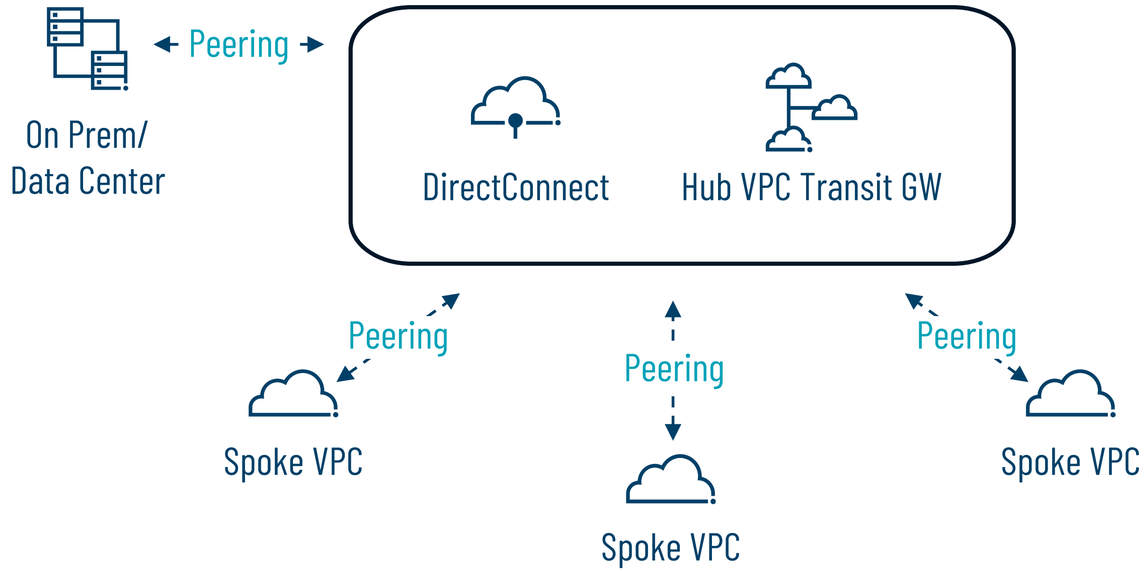
We've created this ebook to provide the reader with insight into what it takes to be a secure organization in the cloud. We will draw on our decades of experience to discuss what cloud security is, how to continuously improve and what an organization needs to do to become more secure. The ebook also addresses whether it was ever true that security for IT estates was simply a matter of applying the proper technology: It wasn't, and it certainly isn't true now. We will look at how to build a secure environment in the cloud — particularly on AWS — and at how organizational culture and technology work together to build a mindset of being secure.

Security starts with understanding

Security is one of those subjects where what you don't know can hurt you — a lot. To understand how to build a secure organization, it is important to understand what constitutes good security.

There is a lot of incorrect information circulating about cybersecurity. One of the most dangerous errors that organizations commit is relying on outdated knowledge. The best ways to protect on-premises systems aren't the same as what is needed to protect an organization's systems in the cloud. An on-premises model relies heavily on perimeter defense, with a firewall keeping out malicious actors. Once any attacker makes it through the firewall, segregation occurs by DMZs where email servers, web servers and other devices that need to be accessible to the outside world reside. An internal firewall isolates the network from the DMZ. The assumption is that anything that makes it through the internal firewall is authorized traffic. In an on-premises setup, where the organization has ownership of the infrastructure estate — both hardware and software — in the network, this is a viable solution.

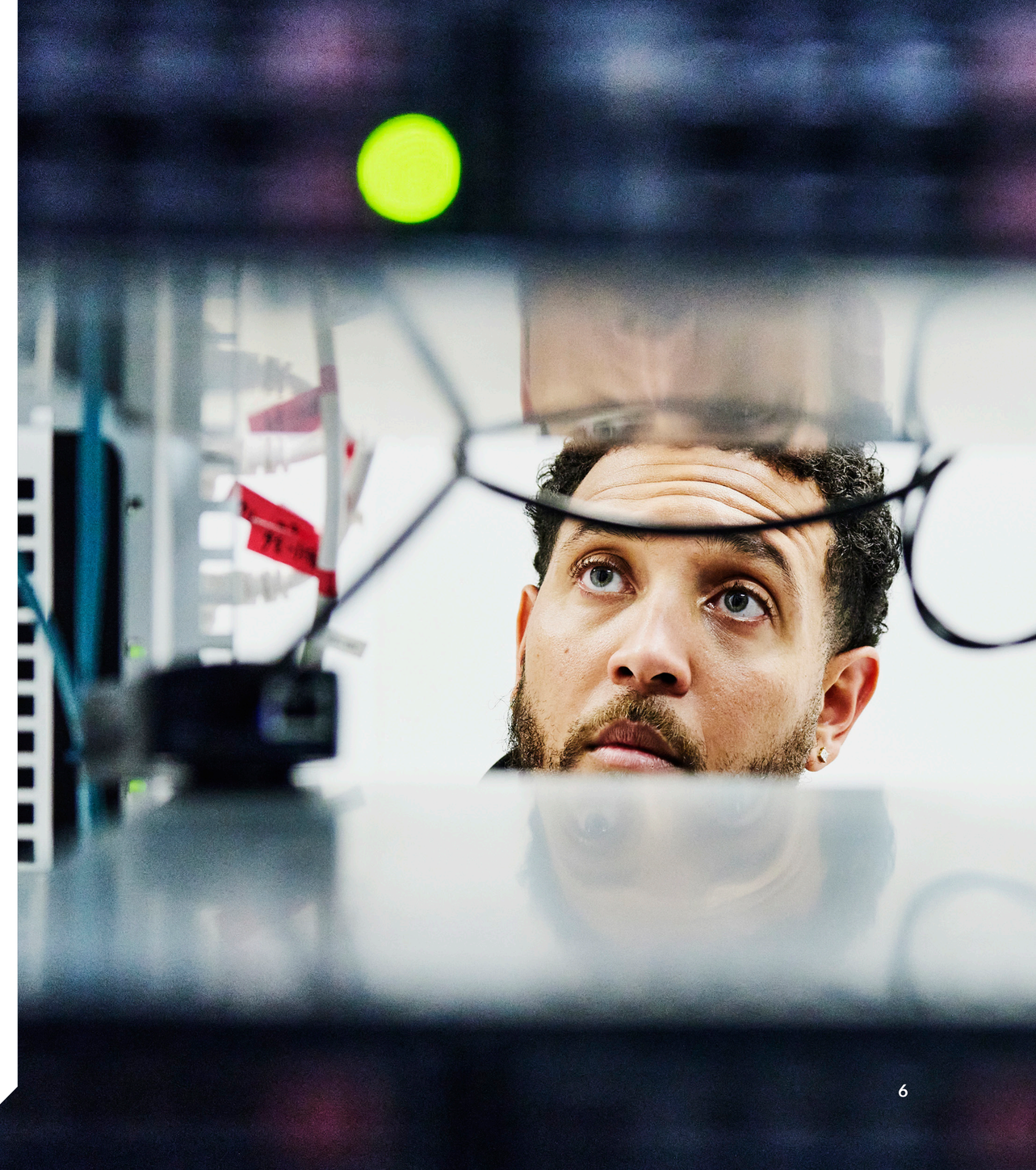
The perimeter model represented in most on-premises data centers doesn't reflect today's reality for security architecture in the cloud. Organizations may have many distributed networks, from regional offices to IoT devices in the field, to cloud footprints. The traditional perimeter defense designed for on-premises systems is ill-defined for the modern distributed network. Today, we're seeing hub-and-spoke models, with a central network hub acting as a control center that inspects traffic in and out of the network and between nodes on the spoke. This security architecture design provides your IT department with a centralized location from which to manage security, rather than trying to inspect a constantly expanding perimeter.



Internal security is important because external security can never be assumed to be completely effective. For this reason, zero trust network access (ZTNA) has risen in popularity. ZTNA assumes threats are present both inside and outside the network, limits all access to resources or zones to authorized *known* users/assets and limits those users/assets to a pre-defined level of access. Identity and access management (IAM) is a way for organizations to control access using both technologies and policies. Combined with ZTNA, this helps to ensure that authorized users and known assets have access only to what they need to do their jobs, while unauthorized parties may not freely move about within the network.

Why security is a business issue

Security, good or bad, can affect the business and must be a top-of-mind issue for the C-suite, not just for IT and not just for the CISO, CTO or CIO. Businesses increasingly operate in the digital realm, with both public-facing and internal systems connected to private and public networks, creating vulnerabilities. With a poor security program, it's not possible to do business with any level of confidence for either the business or the customer. For example, nobody would want to deposit funds with a bank known for poor security.



Businesses must protect against more than theft, however. They operate in a world of regulation and oversight. They must comply with laws and regulations and be able to prove that they do. Compliance has grown more important and complex, particularly for organizations that operate in multiple jurisdictions. The potential costs of security failures are too high to be ignored. The cost of remediation, fines, penalties and restrictions for security breaches can be severe. Some prominent compliance obligations — and these are just a few of many — that organizations face include requirements set by:

- **GDPR:** This European Union privacy regulation comes with fines that can reach €20 million or 4 percent of worldwide annual revenue, whichever is greater, for violations.
- **HIPAA:** This U.S. healthcare privacy regulation carries fines of up to $50,000 per incident and possible criminal penalties.
- **NYSDFS Part 500 Second Amendment:** Set by the New York State Department of Financial Services, this can apply to firms operating in New York as well as those based there. This set of regulations establishes strict guidelines for cybersecurity, including audits and documentation, and can impose multi-million-dollar penalties for non-compliance.
- **CCPA:** The California Consumer Privacy Act provides for fines of up to $7,500 per intentional violation and applies to the residents of the most populous state in the U.S.

Beyond losses due to theft and the increased risk of running afoul of regulatory and compliance requirements, security breaches frequently become high-profile news. The reputational damage of a breach or a ransomware attack, or even an interruption in service, can be significant. This may lead to a loss of business or a fall in share prices, with impacts that may persist for years.

To establish, strengthen and maintain governance, compliance and control — and to minimize risks to reputation — an organization must incorporate the cloud tools that enable it to ensure adherence to its policies and procedures. Employing proper IAM can deter intruders while ZTNA may additionally hinder criminals from gaining access if a breach does occur.

Why controlling users matters

When an attacker penetrates a firewall, the damage they may do depends on the degree of access they have. For example, hackers gained high-level access to a security vendor's network management software and, in what is described as a case of cyber espionage, created false credentials. These credentials allowed unauthorized access to thousands of the company's customers' networks, including U.S. government agencies such as the Department of Homeland Security, the Department of the Treasury and the Department of Justice. Many Fortune 500 private sector firms were also affected. The vendor later settled a lawsuit filed by shareholders for $26 million and faces penalties from the U.S. Securities and Exchange Commission (SEC).

Another prominent example is a U.S. retailer that was breached when an attacker gained entry into its systems after hacking into the systems of an HVAC contractor that worked for the retailer. That hack compromised the information of more than 41 million customers and resulted in an $18.5 million penalty.

These dramatic instances demonstrate the importance of limiting the movement and access that intruders can have in the event of a breach.

How the cloud can improve security

Organizations that move to the cloud operate within a shared responsibility model. Cloud hyperscalers are responsible for security *of* the cloud while organizations are responsible for their own security *in* the cloud.

What exactly does that mean? Hyperscalers, such as AWS, provide cloud-native services that handle traditional security tooling such as firewalls, end point protection and web application firewalls, etc. It is up to each organization to secure their environment and data. This can be done using cloud-native services and/or third-party security tools. The cloud hyperscaler provides the security services that both improve and simplify security for an organization's cloud operations. AWS, for example, is continually developing security services that are designed to enhance security of cloud-native applications. It can do so at a speed that traditional on-premises networks struggle to match. Although the shared responsibility model represents positive technical and operational advances, an organization must take an active role in securing their own environment and data.

Protiviti provides expertise and advisory services that support the design, architecture and operation of a continuously evolving cloud security posture program. Some highlighted elements include:

- **Infrastructure security:** This is the basis upon which you are building everything, and you cannot create a secure organization without a well architected cloud infrastructure. A great way to assess your readiness is to use the AWS Well-Architected Framework, which guides cloud architects in building secure, scalable, resilient and efficient infrastructure for a variety of applications and workloads. It assesses a number of pillars, including one focused on security and protecting information and systems. Our comprehensive security solutions include ZTNA, Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) to protect workloads from malicious traffic.
- **Threat detection and response:** We offer expertise, training and implementation of Security Orchestration, Automation and Response (SOAR), Security Operations Center (SOC), penetration testing and Security Incident and Event Management (SIEM) solutions.
- **Perimeter protection:** We provide protection for applications and origin infrastructure from threats like Distributed Denial of Service (DDoS), Structured Query Language (SQL) injection and cross-site scripting using AWS Shield, AWS Web Application Firewall (WAF) and AWS Firewall Manager.
- **Application security:** We assess code, logic and apps to detect vulnerabilities and threats in cloud environments, providing comprehensive security for your infrastructure and data.
- **Compliance and privacy:** We provide expert support and software for compliance and privacy in the cloud, including third-party certifications, Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) implementation.
- **Data protection:** We help clients secure critical information with robust solutions, including database security, Data Loss Prevention (DLP), email security, S3 file scanning and encryption key management.
- **Identity and access management:** We offer guidance, implementation and training for IAM solutions, including Cloud Infrastructure and Entitlement Management (CIEM), Identity Governance and Administration (IGA) and Privileged Access Management (PAM).

From security to secure

We have talked a lot about security to this point, and that is often how our conversations with customers start. But while Protiviti has deep technical and cloud security expertise, we believe that all organizations should focus on the larger picture of “being secure.” What does that mean — security versus being secure? Basically, security is something you do and being secure is how you behave. In a secure organization, the business understands the need for the organization to be secure and views security as an enabler and therefore acts in accordance with all security procedures. For a business to be able to embrace a truly secure posture, it requires some basics.

A business-enabling mindset and strategy: Although security is crucial to any business, it should not be a hindrance to business growth. Rather, good security is a partner to business growth. Therefore, a business-enabling mindset and strategy are prerequisites to developing a sound foundation. It's crucial to balance the need to be secure with the needs of the business.

A clearly articulated organizational risk appetite validated by leadership: Achieving the correct balance between security and business needs requires the business to determine its risk appetite. Senior leadership also needs to make the level of risk appetite clear to everyone involved in security, so that everyone can take appropriate steps to achieve a secure posture.

A governance framework and supporting processes: To create a secure organization, security must be a living program that is continually monitored and responds to changing needs. Being secure is not a "one-and-done" process. A great security foundation without proper governance will deteriorate over time. Worse still, the organization might consider itself secure because of security protocols that are collecting dust in a drawer. Proper governance processes help to maintain the relevance of the security foundation to the organization's business and risk profile. Such processes also help to enforce the security foundation and maximize its effectiveness. A good governance program should have not only a well-defined framework, but also a list of defined and enforced processes. These could include, for example, an AWS service review and approval, parameters for AWS control exceptions, and AWS security incident management, including escalation and AWS security remediation.

A set of business-validated and development-friendly AWS security requirements, reference architecture and blueprints: A common theme that we have observed when organizations are rapidly adopting AWS is the struggle to introduce security at the scale and speed of business. For example, security is often behind the curve of new AWS service adoption. Additionally, the adoption of DevOps methodology and the *shift-left* mindset — in which testing and quality control processes, including security testing, are moved toward earlier stages of development — push security responsibility toward the developer. This means that developers must be empowered to integrate secure solutions into their applications by following defined security requirements. The business should empower and enable those who are implementing security tools and make working securely an integral part of the business.

Being secure is about more than passing audits and assessments for compliance. *Secure* is a cultural mindset that must be embraced from the C-suite down to truly be successful.

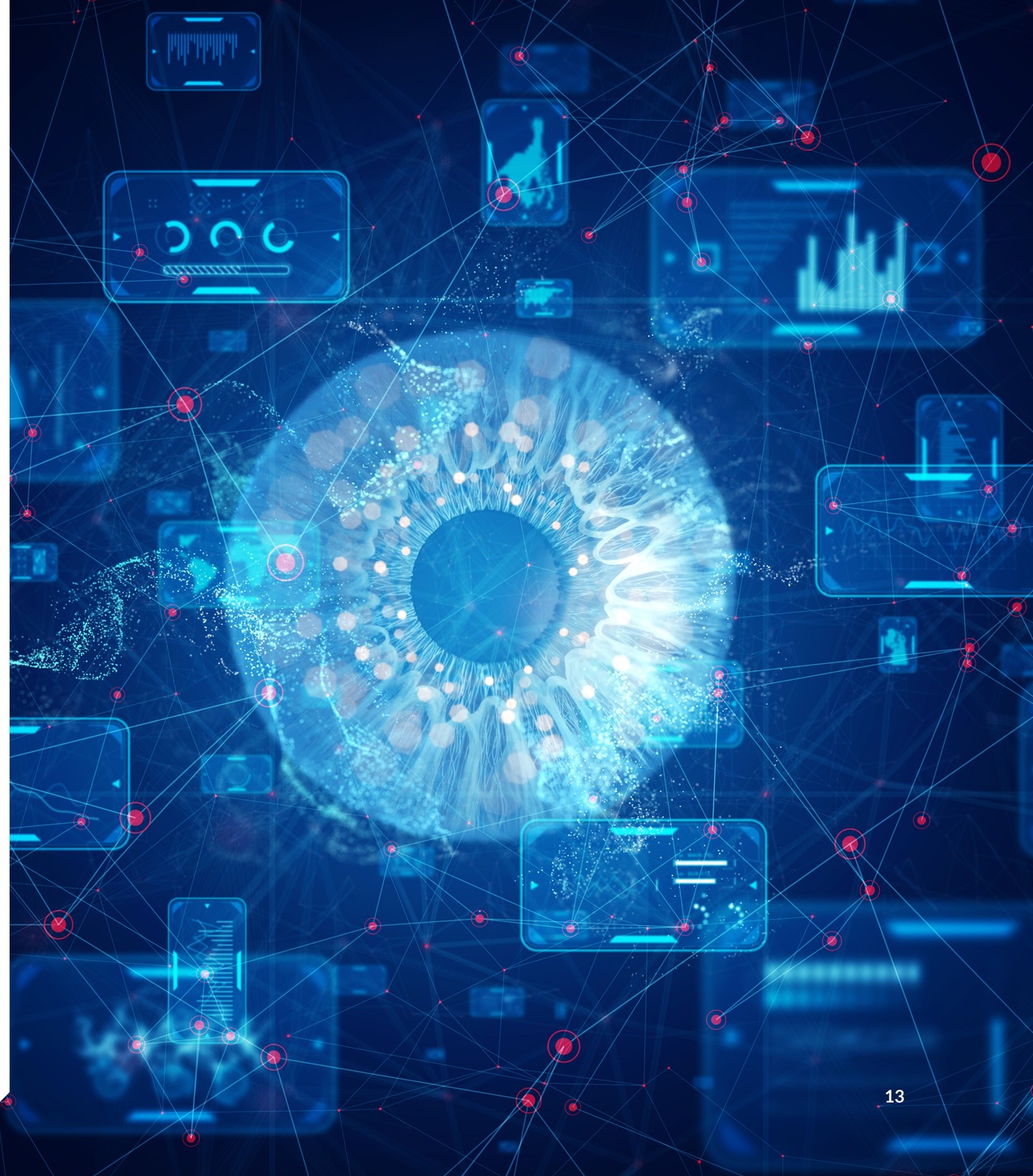
Being secure: we know what good looks like

As a firm with years of experience serving the world's largest companies, including many Fortune 1000 organizations, Protiviti understands that security — and specifically cloud security — varies amongst organizations and will always be fluid. We can help organizations with an unbiased third-party examination covering technical and organizational security readiness. Maybe you are migrating systems and security to the cloud for the first time, or maybe you have already established a mature footprint. In either case, Protiviti has the proper lens and guidance to help avoid costly and time-consuming mistakes.

Protiviti can help, whether it's guiding you on your cloud security journey or implementing a secure cloud environment together with your organization. We pride ourselves on meeting you where you are on your journey.

Cloud hyperscalers like AWS are constantly evolving and updating services, especially security services, in order to reduce and manage risk. Having earned the AWS Security Competency, Protiviti has demonstrated its security expertise and maintains a highly skilled team capable of navigating the challenges of being secure in a rapidly evolving cloud environment. If you'd like to know more, we're happy to have a conversation.

Wherever you are in your cloud security journey, we can help.
Learn more at protiviti.com/aws-security



About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI).

protiviti®

Global Business Consulting

aws PARTNER Advanced Tier Services

- Public Sector
- AWS Marketplace Seller
- DevOps Services Competency
- Security Services Competency
- Migration and Modernization Services Competency

Face the Future with Confidence®