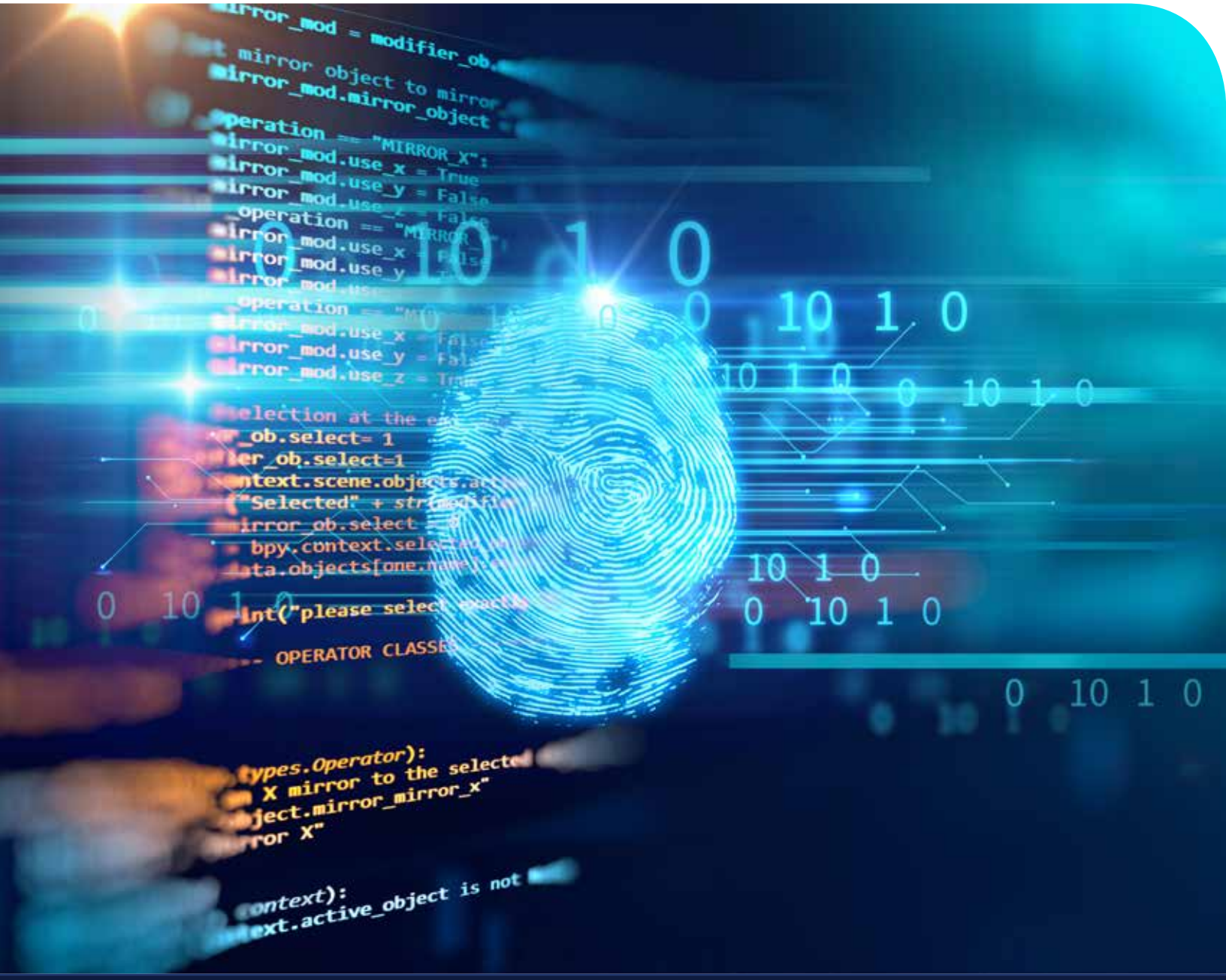
OneNeck®
IT SOLUTIONS
a TDS® Company



REPELLING CYBERTHREATS IN A MULTI-CLOUD ENVIRONMENT

What today's organization needs to know about maintaining security across multiple platforms and staving off cyberattacks

Repelling cyberthreats in a multi-cloud environment

Eager to reap the benefits of the cloud, companies everywhere are doubling down on their cloud strategies and turning to multi-cloud environments to handle their workloads and data analysis. Eighty-one percent of enterprises now have a multi-cloud strategy featuring an average of 2.7 public clouds and three private clouds to run essential workflows and applications.[1]

Cloud is no longer a matter of "if" for businesses, but "when."

But cloud is complex and still evolving. And as companies spread workloads among different cloud providers, they're faced with new challenges — namely, the difficulty in maintaining security across multiple platforms and staving off cyberattacks. And as cyberthreats grow in frequency, sophistication and malice, organizations also need a serious reality check to understand how multi-cloud environments open the door to risk and what can be done about it.

[1]RightScale 2018 State of the Cloud Report. Rightscale, Inc. January 2018.

OneNeck® IT SOLUTIONS a TDS® Company

Multiple deployments, multiplied risk

Effective cybersecurity requires extensive IT expertise and technological power that can dramatically compound both costs and risk for enterprises. And with each successive cloud deployment, the potential for vulnerability follows. As a company's cloud infrastructure grows and diversifies, added endpoints, APIs and integrations create more entry points for intrusion and risk—both from external and internal sources.

Over the past couple of years, cyberattacks ranging from DDoS and 51% attacks to targeted hacks and malware have more than doubled.[2] Factor in that internal security risks, whether an intentional act from a disgruntled employee or an accident like losing a USB drive, account for nearly three-quarters of new security threat instances,[3] and it's no wonder that IT leaders list security as one of their top cloud-related concerns in survey after survey.[4]

Where do cyber attacks come from?

Common Attack Vectors:

- Malware (27%)
- Vulnerability (10%)
- Targeted hack (13.5%)
- Account hijacking (17%)
- DDoS (3%)

June 2018 Cyber Attacks Statistics. Hackmageddon.com

[2]Seals, Tara. "Cyberattacks doubled in 2017."Infosecurity Magazine. Jan. 26, 2018.
[3]Schick, Shane. "Insider Threats Account for Nearly 75 Percent of Security Breach Incidents." Securityintelligence.com. August 28, 2017
[4]RightScale 2018 State of the Cloud Report. Rightscale, Inc. January 2018.

A large part of that concern emanates from simply not knowing what they don't know. IT executives who don't specialize in cybersecurity will have blind spots in their security plans and operations that can leave their organization exposed.

Addressing rapidly evolving external security threats and mitigating systemic internal vulnerabilities requires specific policies and procedures, specialized skill, and an intimate understanding of the strengths and weaknesses of an organization's infrastructure. Seemingly routine but essential tasks like managing user identities and access often lay outside the everyday skills of IT teams. And lacking immediate access to the proper resources — even just how-to guides — hampers the ability to act fast in the face of a threat.

Creating those policies, processes, and resources is the domain of a Chief Information Security Officer (CISO) and supporting staff, but not every organization has the financial resources to hire one. Nor do they necessarily have other staff who can take on those responsibilities, evidenced by the fact that more than 50% of IT leaders believe their organization suffers from a severe shortage of cybersecurity skills, up from 45% last year.[5]

This significant deficit in critical skills leaves many companies embarking on a multi-cloud solution without enough fortification — never an ideal situation when so much is at stake.

Six in 10 respondents in an ISACA study expressed difficulty in identifying the skills and knowledge needed to ward off a sophisticated cyberattack .

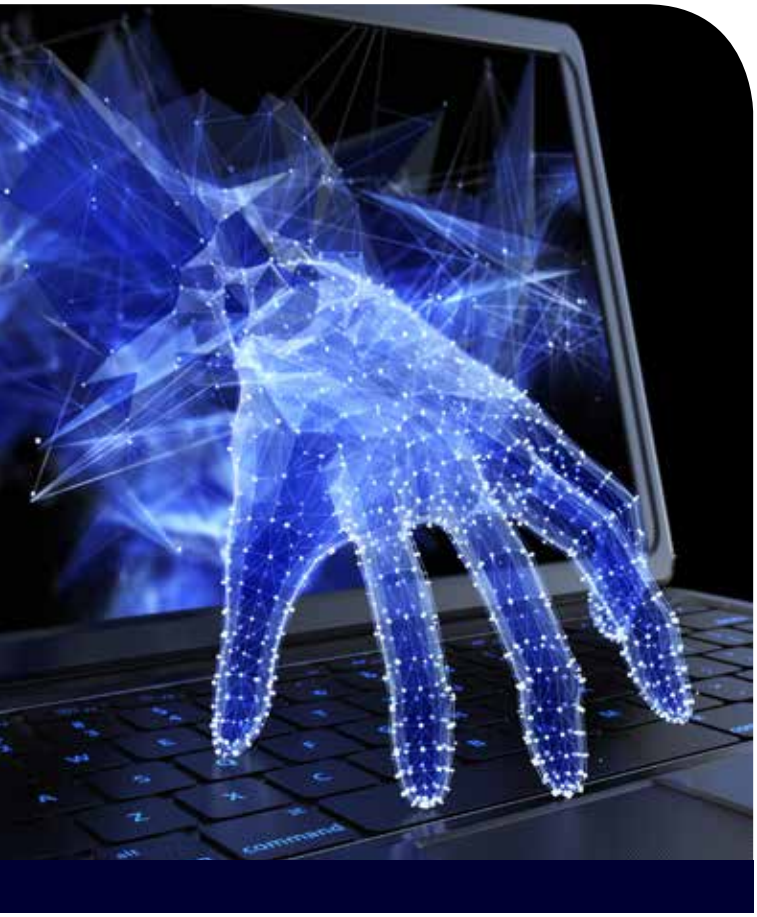
State of Cybersecurity: Implications for 2016. ISACA and RSA. January 2016.

Only 38% of cybersecurity staff believe they're getting enough training to keep up with IT risks.

Research Report: The Life and Times of Cybersecurity Professionals. ESG and ISSA. November 2017.

[5] "Research suggests cybersecurity skills shortage is getting worse." Jon Oltsik. CSO. Jan. 11, 2018.

What to consider when securing a multi-cloud environment



Organizations without a CISO or other security-focused leader onboard could be at greater risk for a breach. For enterprises in this position to keep pace with the level of cybersecurity needed to lock down data and applications, shore up vulnerabilities, and guard against threats, here are the most important security considerations when deploying a multi-cloud solution:

- **Security framework -** The average data breach costs as much as $5 million per incident.[6] Working with cloud providers to devise a comprehensive security framework that includes authentication parameters (single-sign-on or SSO) and data encryption in both software and hardware layers is a crucial step to keeping unauthorized users from where they don't belong. Lacking a strong framework usually means open season on highly sensitive user data.
- **Regulatory compliance demands -** Between state laws, specific industry regulations, and the European Union's sweeping new General Data Protection Regulation (GDPR), there's no shortage of data privacy and protection demands on businesses. Relying solely on cloud providers to support data governance principles and meet the latest regulatory compliance through regular system reviews, inventory audits, and risk assessments may not be enough to satisfy the myriad data management requirements.
- **Endpoint protection (servers and end-user devices) -** Any time a company's network is accessed remotely via laptops, mobile, or other devices, it's a potential entry point for a security threat. And if a device should get lost or stolen, the company's data is dangerously exposed. Managing network applications in the cloud means that endpoint protection has to be administered through security software, both on network servers and on each device.

48 states require individuals to be notified if their data is compromised.

"Reforming the U.S. approach to data protection and privacy." Nuala O'Connor. Council on Foreign Relations. Jan. 30, 2018.

[6] "How much does a security breach actually cost?" Michelle Drolet. CSO. Oct. 28, 2016.

OneNeck® IT SOLUTIONS a TDS® Company

- **Firewall / IPS / IDS requirements** - Firewalls and Intrusion Protection Systems (IPS) work together to block unauthorized network hacks, while Intrusion Detection Systems (IDS) detect and alert to any suspicious activity or data. But with so many outside devices being used for business, traditional detection systems are stressed when protecting against a bevy of internal and external threats. IT leaders must think about how to coordinate the various resources cloud providers have to meet firewall requirements effectively and neutralize threats that can literally come from anywhere.

- **Separation and segmentation of business applications** - Understanding how applications and other components are dependent upon each other — also called application dependency — is important when it comes to security updates. For example, knowing how data is shared between systems and how those systems are affected means foreseeing the potential ramifications when a new security feature is added to one app but not another. To avoid negatively impacting business, companies and cloud providers alike must be adept in discovering and configuring dependencies.

- **Security consistency and centralized management** - An attack in one form or another is nearly unavoidable. In response, companies need a two-fold approach to protect themselves: a universal security policy that governs all departments, partners, and customers, and cloud-based centralized security management to make it easier and quicker to deploy security measures to each server and device. Combining overarching policies with coordinated, on-the-ground tactics allows companies to respond to threats faster while actually reducing management efforts.

- **OpenDNS** - Since 2013, phishing scams have cost businesses $1.6 billion.[7] Which is why using OpenDNS is so critical to avoid the major impacts to productivity that can happen as a result of web-based threats, in addition to phishing, like untrustworthy websites, malware and ransomware. A cloud security platform tasked with running a company's internet has to secure web traffic and activity without impacting performance.

- Attacks targeting IoT technologies increased 600% in the last year.
- Ransomware shifts from big score to commodity, lowering prices while increasing variants.
- Malware attacks exploiting software vendors and supply chains grew by 200%.
- Mobile malware variants increased by 54%.

Internet Security Threat Report 2018. Symantec.

[7] "Phishing scams cost American businesses half a billion dollars a year." Lee Matthews. Forbes. May 5, 2017.

How to address essential security considerations

Even as cloud providers promise greater security than localized infrastructures, companies deploying cloud solutions are still ultimately responsible for their own data and operations. Here are five important steps organizations can take to address security considerations in a multi-cloud environment:

- **Follow public cloud best practices** - Public cloud providers like Azure, Google and AWS all outline their own best practices for utilizing their platforms and services, which include security. Additionally, identifying which applications can successfully move to the public cloud (i.e., which are "backward compatible") and whether a hybrid cloud environment makes sense helps companies stay abreast of cybersecurity concerns across the spectrum of their workloads and platforms.

- **Create a cybersecurity policy framework** - Developing a comprehensive cybersecurity policy framework can help accelerate a company's response to attacks and work to keep them from happening in the first place. A high-level map of cybersecurity outcomes — assessment, detection, mitigation and recovery — acts as a guide to managing those outcomes while also defining regulatory compliance demands and helping companies select the appropriate cloud services to meet security needs.

- **Approach shadow IT with caution** - Using IT tools and solutions without organizational approval can be both a blessing and a curse, depending on individual company culture. But while the use of shadow IT has led to flexible, fast and innovative approaches to today's business problems, it also poses significant risk. Over 50% of the consumption of enterprise applications is happening over sources that can neither be controlled or accounted for.[8] To help assure security and compliance company-wide, executive buy-in shouldn't be optional.

- **Emphasize automation** - At every turn, automating security workloads in the cloud takes the guesswork and human error out of executing a security strategy. Automating routine, day-to-day tasks — intrusion detection and prevention, endpoint monitoring, alerts to data breaches, log management and aggregation, and management of anti-virus and malware protection for hardware — allows companies to refocus valuable security expertise on higher-value activities and proactively thwarting cyber attacks.

62% of companies now have automated incident response processes .

"Security automation is maturing, but many firms not ready for adoption." Maria Korolov. CSO. May 2, 2017.

- **Seek outside support and expertise** - Even with a competent CISO at the helm, it's exceedingly difficult for any company to internally identify and manage every single aspect of cybersecurity. Instead, third-party cloud-managed security (CMS) services provide organizations with a comprehensive gameplan and staff to protect all systems, storage, data and devices from threats by tying together the best technologies, services, and expertise when internal IT teams may not be robust enough.

[8]"Shadow IT: it's not what you think." Jacek Materna. CSO. Dec. 5, 2017.

Multi-cloud is the new norm

As pressure mounts for organizations to cut costs, optimize performance, and improve reliability, businesses are increasingly moving away from their single-cloud infrastructure and employing a multi-cloud strategy.

They're drawn to the resiliency, flexibility and cost control capabilities multiple clouds provide. But they're quickly realizing that a one-size-fits-all approach to securing their infrastructure doesn't meet the growing complexities around running multiple environments for customer retention and data analysis and other high-value business activities.

To protect themselves, their business and their customers, enterprises must fully understand all the risks — and the rewards — that come with a multi-cloud infrastructure. They must commit to investing in the resources, technologies and partners to develop and deploy a robust cybersecurity program, complete with governance policies, automated task management and an enterprise-wide understanding of just how important it is to get every element right.

The companies that prioritize mastering the intricacies of cloud security can avoid the costly cyber attacks and data breaches that can impact a business for years to come.

Learn how OneNeck can help you address the challenges of a multi-cloud strategy and set you on the path to greater business agility, flexibility, security and success. Contact us for a free consultation at 855.OneNeck or www.oneneck.com

OneNeck®
IT SOLUTIONS
a TDS® Company

(855) ONE-NECK | www.oneneck.com