White Paper

Enabling Cybersecurity in the Age of Digital Transformation

By Doug Cahill, ESG Senior Analyst; and Jack Poller, ESG Analyst

December 2017

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

Executive Summary

The various aspects of digital transformation are fundamentally changing enterprise IT, enabling greater business agility, but also creating a new set of cybersecurity challenges. The broad adoption of cloud services, knowledge worker mobility, and the explosion of connected devices are the core drivers of this technology shift. New methodologies such as agile software development and DevOps continuous delivery are also highly impactful aspects of this transformation.

These changes transcend technology and also impact IT business models. And many IT initiatives are decentralized—departments and business units often drive new technology adoption outside of the purview of corporate IT and cybersecurity teams. The combination of how digital transformation expands the attack surface area, the decentralization of IT, and the speed at which organizations are implementing new business applications in the cloud creates a new set of cybersecurity challenges.

The fundamental challenge is the gap between the rate at which companies are undergoing a digital transformation and their readiness to secure this new enterprise IT model, which is multidimensional, mobile, and decentralized, without context or consistent policies across the attack surface. This paper explores the impact of digital transformation on cybersecurity processes and technologies and offers a reference architecture for securing the foundational aspects of modern, enterprise IT.

The fundamental challenge is the gap between the rate at which companies are undergoing a digital transformation and their readiness to secure this new enterprise IT model.

Digital Transformation and the Expanding Attack Surface Area

ESG defines digital transformation (DX) as the profound and accelerating transformation of business activities, processes, competencies, and models to fully leverage current and future digital technologies. Digital transformation enables companies to better serve their customers, whether they are internal or external. Organizations are using technology to radically improve the performance or reach of their business, and digital transformation is transforming the IT landscape with a scale, speed, and breadth that has never been seen before.

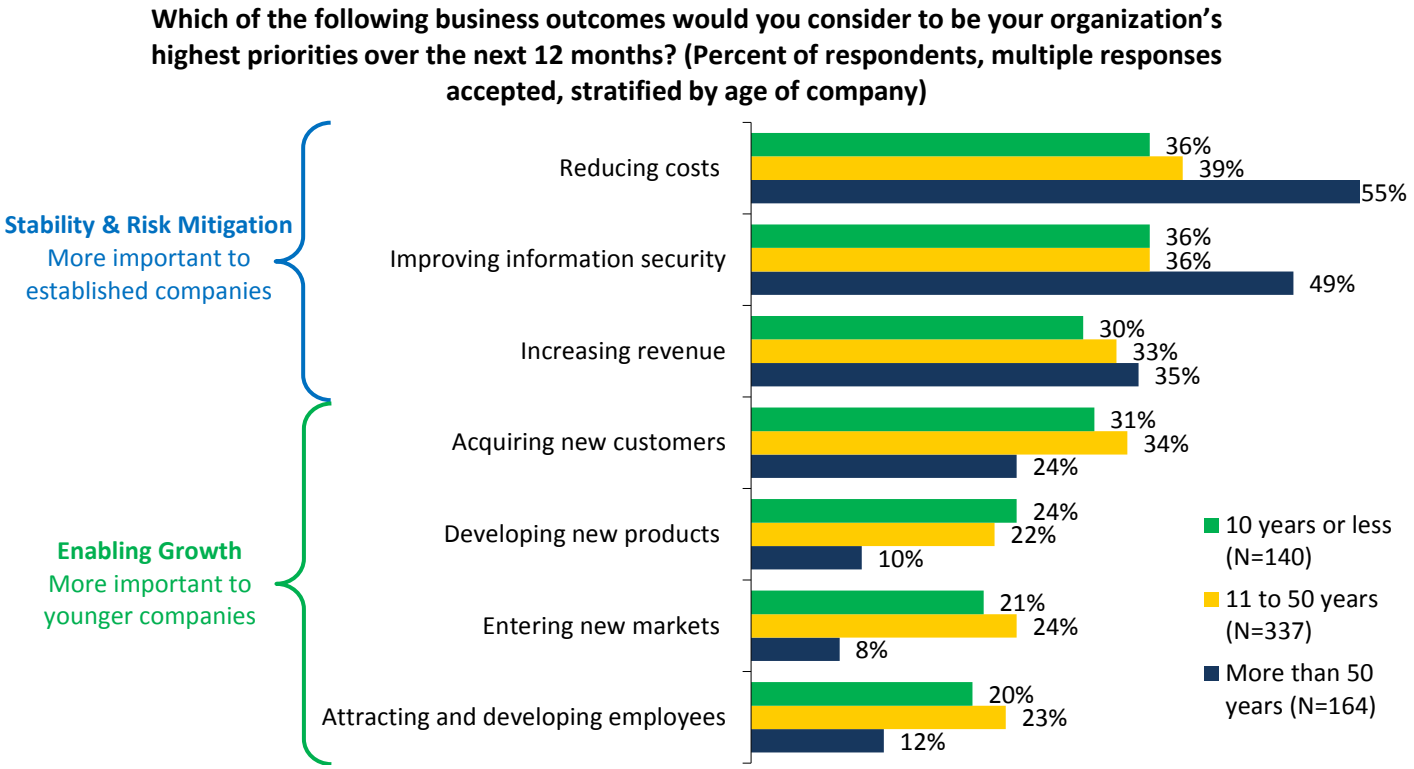
The Business Impact of Digital Transformation

According to ESG research, the age of an organization has an influence on its pursuit of modern IT strategies, including cloud, mobile, IoT, and digital transformation. Forty-five percent of companies 10 years old or younger have adopted a cloud-first initiative, compared with the 23% of companies older than 50 years that have done so. Conversely, 30% of older organizations are maintaining an on-premises-first strategy versus 11% of younger organizations.[1]

This is the result of business goals that drive IT strategy, which are also influenced by the age of the organization. Younger organizations tend to focus on goals that drive growth, such as acquiring new customers and developing new products. Conversely, goals that drive stability and risk mitigation, such as reducing costs and improving information security, are more important for established organizations (see Figure 1).[2]

[1] Source: ESG Research Report, *2017 Public Cloud Computing Trends*, April 2017.
[2] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

Figure 1. Business Outcomes by Age of Company



Source: Enterprise Strategy Group, 2017

Cloud adoption is one of the first steps organizations take on their digital transformation journey, and the increasing use of cloud services is an indication of the prevalence of digital transformation initiatives. According to ESG research, 78% of organizations use public cloud services today, up from 57% in 2013.[3]

The Hybrid and Multi-cloud Attack Surface Area

The main drivers for cloud adoption traditionally revolve around basic benefits such as transitioning from a CapEx to an OpEx environment. Cloud models are also disruptive and transformational, moving IT from a static architecture to a dynamic environment, providing scaling, efficiency, elasticity, and cost optimization, among many other benefits. Cloud technologies are catalysts for innovation, providing the scale and speed necessary for rapid experimentation, development, deployment, and distribution.

Successful digital transformation leverages key features of cloud architectures. Cloud scaling ensures that only the minimum necessary resources are dedicated to a workload at any point in time. This provides efficiency as well as elasticity. Cloud bursting, the practice of expanding or moving a workload from an on-premises data center to the cloud, or from one to multiple cloud service providers when demand spikes to consume all resources in the primary data center, provides additional elasticity and efficiency. Scaling, workload mobility, and cloud bursting ensure that organizations only use and pay for extra resources when they are needed.

Organizations are increasingly deploying multi-cloud environments. According to ESG research, three-quarters of organizations use between two to five IaaS or PaaS cloud service providers, and 19% use four or five cloud service providers.[4] The challenges of securing hybrid and multi-cloud solutions include:

[3] Source: ESG Research Report, *2017 Public Cloud Computing Trends*, April 2017.
[4] Source: Ibid.

- **Data security.** Maintaining control over data becomes harder as the data spreads across the cloud. In addition to ensuring data integrity, organizations need to prevent unauthorized access to data. Another challenge is preventing malicious actors from using an organization's cloud services to store and propagate malware internally, or to use the cloud as a launching point to attack others.

- **Data provenance**. Where data is stored becomes opaque in the cloud, increasing the difficulty of implementing data privacy and locality requirements, which can be critical for organizations operating internationally or globally. Even national organizations can be stymied when cloud service providers implement global data centers.

- **Data segregation**. Most public cloud infrastructures are architected with shared infrastructure to support multi-tenancy. Organizations need to ensure that cloud service providers guarantee complete data segregation to prevent malicious or inadvertent data loss.

- **Identity and access management (IAM).** Almost every SaaS application or cloud service incorporates its own user database. Cybersecurity professionals must maintain proper user identification, authentication, and authorization for each service and its associated data, as well as synchronize identities across public and on-premises cloud environments.

- **Expanded attack surface.** The number of points where an attacker can try to infiltrate the environment expands with the use of each additional cloud service provider or on-premises data center.

- **Amorphous perimeter**. The organization's perimeter becomes nebulous and fluid as the organization expands into the public cloud. Each public cloud and on-premises infrastructure has its own dynamic physical and logical perimeter. Organizations need to control access to applications and data from anywhere in the world.

- **Delegated authority and responsibility for cybersecurity.** The business delegates authority and responsibility for a subset of security to the public cloud service providers. This subset typically includes basic network security such as DNS, distributed denial of service (DDoS) prevention, and cloud service provider account identification and authorization.

- **Delegated infrastructure controls.** Organizations must establish a level of trust with their cloud service providers, who are responsible for hiring, oversight, physical security, and access control for the underlying infrastructure.

- **Expanded governance, risk, and compliance (GRC)**. Businesses remain accountable for their own data, even when stored in a public cloud. The effort to develop and maintain governance policies and procedures, ensure compliance, and measure risk grows with the addition of each cloud service provider.

Half (51%) of organizations surveyed by ESG said that the security risks associated with relying on a third-party cloud computing provider was one of the biggest impediments to their organization's use of cloud computing services. Additional security-related impediments to cloud adoption included the expanded attack surface area, cited by 37%, while 34% were concerned that cloud computing may not align with their regulatory compliance requirements.[5]

End-user Mobility

Companies are better able to serve their customers when employees can access data and applications from any device, anytime, anywhere in the world. And employees can make the best data-informed decisions by collecting and analyzing

[5] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

the most recent and pertinent data. This gives rise to organizations embracing user and device mobility in their digital transformation initiatives, but mobility increases the scale of the cybersecurity challenge. The problems include:

- Multi-device exposure. Each new endpoint presents a new set of attack vectors—points where an attacker can attempt to compromise the endpoint. In addition to traditional attacks, mobile devices expose additional communication channels, including SMS and MMS (text messaging), and Bluetooth, which are not afforded the same level of protection as traditional channels.
- Fluid and mobile perimeter. Mobile devices are continuously moving inside and outside of the corporate network. When outside of the traditional corporate network perimeter, devices lack the protections provided by corporate security controls. As with workload mobility, transient and mobile devices dynamically change the security perimeter.
- Insecure network. Users may access applications over insecure and potentially compromised networks. This can lead to man-in-the-middle and other sophisticated attacks to acquire user credentials and steal sensitive data. This can be an especially challenging issue for global employees operating in environments where corporate espionage is a constant threat and there is insufficient intellectual property protection.
- Expanded hardware, software, and application footprint. Each distinct device, operating system, and application requires its own security tools and controls, and has its own patch management requirements, multiplying the efforts to ensure device security.
- Loss or theft of endpoint devices. Mobile devices today have as much storage as PCs, and are troves of sensitive personal and corporate data. Most importantly, mobile devices are a key component in multi-factor authentication. Loss or theft of the device can potentially compromise identity, expose data, or prevent an employee from completing her work.

Shadow IT Visibility Gaps

Innovation in the consumer space is occurring at a rapid pace, with the guiding principle being simplification to drive adoption. This has led to the trend of consumerization of IT—the process whereby information technology emerging in the consumer market spreads to business organizations—and, by extension, the decentralization of IT.

Cloud services and knowledge worker mobility have accelerated the trend and amplified the implications. Easy-to-use services with one-touch provisioning, federated identification, and credit card billing have conditioned users to expect rapid progress in acquiring new technology, quickly transitioning from application evaluation to application deployment.

Motivated by the need for business agility to capitalize on an opportunity, some employees and lines of business are no longer willing to wait for corporate IT to deliver a new productivity application, opting to instead to bypass IT and, very often, using a cloud app they can easily enable on their own. This gives rise to shadow IT—technology acquired, provisioned, and managed outside of, and without the knowledge or approval of, the IT department. Even though 56% of organizations have a policy requiring prior approval before business units can use any cloud apps, and 40% require registration of cloud apps, unsanctioned IT app use is prevalent. In aggregate, 85% of organizations are aware of the use of a significant amount of (34%), a moderate amount of (31%), or a few (20%) unsanctioned apps.[6]

The lack of IT oversight and control of shadow IT presents a challenge to the cybersecurity team. Without visibility into which apps are in use, the team cannot apply threat detection, data loss prevention, access control, or other security

[6] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

policies. Shadow IT hinders the organization's ability to ensure compliance with recent and upcoming regulatory requirements that involve the entire business in data privacy and data protection.

The difficulty in securing corporate data becomes more pronounced for cloud apps, where there is a tendency to blur the lines between personal and business identities and activities. Employees may use a personal account to overcome corporate IT policies such as email attachment limitations. Or they may use their work accounts for personal activities. This exposes users to various avenues of compromise, resulting in potential inadvertent or malicious sharing and distribution of confidential information.

Lack of IoT Resiliency

Another step in the digital transformation journey is implementing the Internet of things (IoT), which is the concept of connecting almost any device to a network to obtain and exchange data and information. This can include devices that we already think about, such as mobile phones, thermostats, lights, and home automation devices, and things that we may not think about, such as medical devices, industrial sensors, and robots. IoT integrates the computer world with the physical world, enabling computers to sense and control the physical environment.

IoT creates opportunities for improvements in efficiency and efficacy, along with simultaneous reductions in human intervention and human-induced errors. Therefore, businesses see great value in IoT helping with their digital transformation journey.

Even though it is in the early stages of development, many industries are exploring IoT. A number of industries, including operational technology (OT/manufacturing), travel, energy, and health care, are actively integrating IoT into their business operations. According to ESG research, IoT initiatives are growing quickly, and a majority of organizations have already started implementing IoT initiatives or expect to do so over the next 12 months.

What's driving the adoption of IoT? Previously conducted ESG research indicates that organizations anticipate positive impacts from IoT, including:

- 45% say IoT will help their organization become more **operationally efficient.**
- 39% say IoT will help provide better and differentiated **customer service.**
- 39% say IoT will help develop **new products and services.**
- 26% say that IoT will enable the creation of entirely **new business models.**[7]

IoT devices present some unique security challenges. Many IoT devices run old versions of operating systems that have been discontinued, and there are no patches available to fix new vulnerabilities. Upgrading to newer operating systems and applications is hampered by a lack of resources, as IoT devices often have limited computing power, memory, storage capacity, or network bandwidth. This lack of resources often prevents IoT devices from implementing their own internal security controls.

According to ESG research, one quarter (24%) of organizations ranked securing IoT data as the biggest IoT technology challenge, tying it at the top of the list with integrating the data. Twelve percent of organizations said governing the data (i.e., applying corporate and regulatory compliance policies) was the biggest IoT technology challenge.[8]

[7] Source: ESG Brief, *The Intersection of IoT and Big Data*, March 2016.
[8] Source: ESG Brief, *The Intersection of IoT and Big Data*, March 2016.

The inclusion of mobile and IoT devices in the corporate environment is expanding the security practitioner's perspective from securing traditional desktop and laptop endpoints to securing "edgepoints"—devices operating at the edge of any network that are used to create, access, and manipulate an organization's data. Expanding the notion of what needs to be secured has broad implications for security policy, tools, personnel, and the volume of work.

Cloud computing is very important for IoT implementation. Many organizations use public and third-party private clouds to manage the IoT data stream and perform initial data aggregation and analysis. However, these cloud solutions represent a security challenge. Some IoT solutions hide implementation details, and IT may be unaware of cloud use or other attack vectors, further hampering the effort to secure their IoT environment.

The Cloud Security Readiness Gap Created by Digital Transformation

The drive to adopt cloud technologies as part of digital transformation initiatives is outpacing the development of technologies, processes, policies, and skills to secure the cloud, creating a cybersecurity readiness gap.

Cloud Security Maturity

Hybrid and multi-cloud services lead to a variety of security challenges, such as provisioning security controls, assessing security posture across heterogeneous cloud infrastructures, and monitoring cloud security for risk assessment, incident response, and regulatory compliance. Given the velocity of cloud computing adoption, cloud security challenges can lead to an inevitable increase in IT risk.

> This new enterprise IT model is multidimensional, mobile, and decentralized, without context or consistent policies across the attack surface.

Due to the prevalent use of cloud services, cloud security has become a strategic imperative. However, cloud security processes, policies, and technologies are still evolving. In fact, many cloud security technologies are adaptations of traditional on-premises security controls such as those that have been converted to run as virtualized instances in a cloud environment. This provides purchasing and licensing flexibility, and enables cybersecurity professionals to use the same tools, commands, and scripts on-premises and in the cloud. However, because these adaptations are not cloud-native implementations and are not always tightly integrated with cloud services, they are not always adept at addressing specific cloud security concerns.

A multitude of new cloud security tools have been developed to address the unique challenges of cloud security. Tools such as cloud access security brokers (CASBs), identity and access management (IAM) federated identity solutions, data loss prevention (DLP) tools, micro-segmentation with cloud adapters, cloud workload protection platforms (CWPP), and cloud-delivered secure web gateways (SWG) and proxies, among others, provide visibility and control over hybrid and multi-cloud environments.

As these cloud security solutions mature, so too must organizational readiness to secure cloud services. Indeed, according to ESG research, 80% of security professionals believe that their organization's approach—processes, policies, skills, and tools—for on-premises security is either much more (42%) or somewhat more (38%) mature than that safeguarding public cloud-based infrastructure and applications.[9] Irrespective of one's view of how secure public cloud services are, this research reveals that many organizations need to retool to meet the security requirements of hybrid and multi-cloud environments. Many organizations are responding to close this gap by increasing their cybersecurity investments: 41% are making their most significant investment in cloud security, and 39% in network security, both of which are required to secure hybrid clouds.[10]

[9] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.
[10] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

Clouds Obscure Visibility

Cloud-first is the new normal, and, combined with the consumerization of IT, IoT, and mobile-first initiatives, has led to the proliferation of shadow IT. Thirty-four percent or organizations state they are aware of a significant amount of shadow IT applications, and 31% indicated an awareness of a moderate amount of shadow IT.[11]

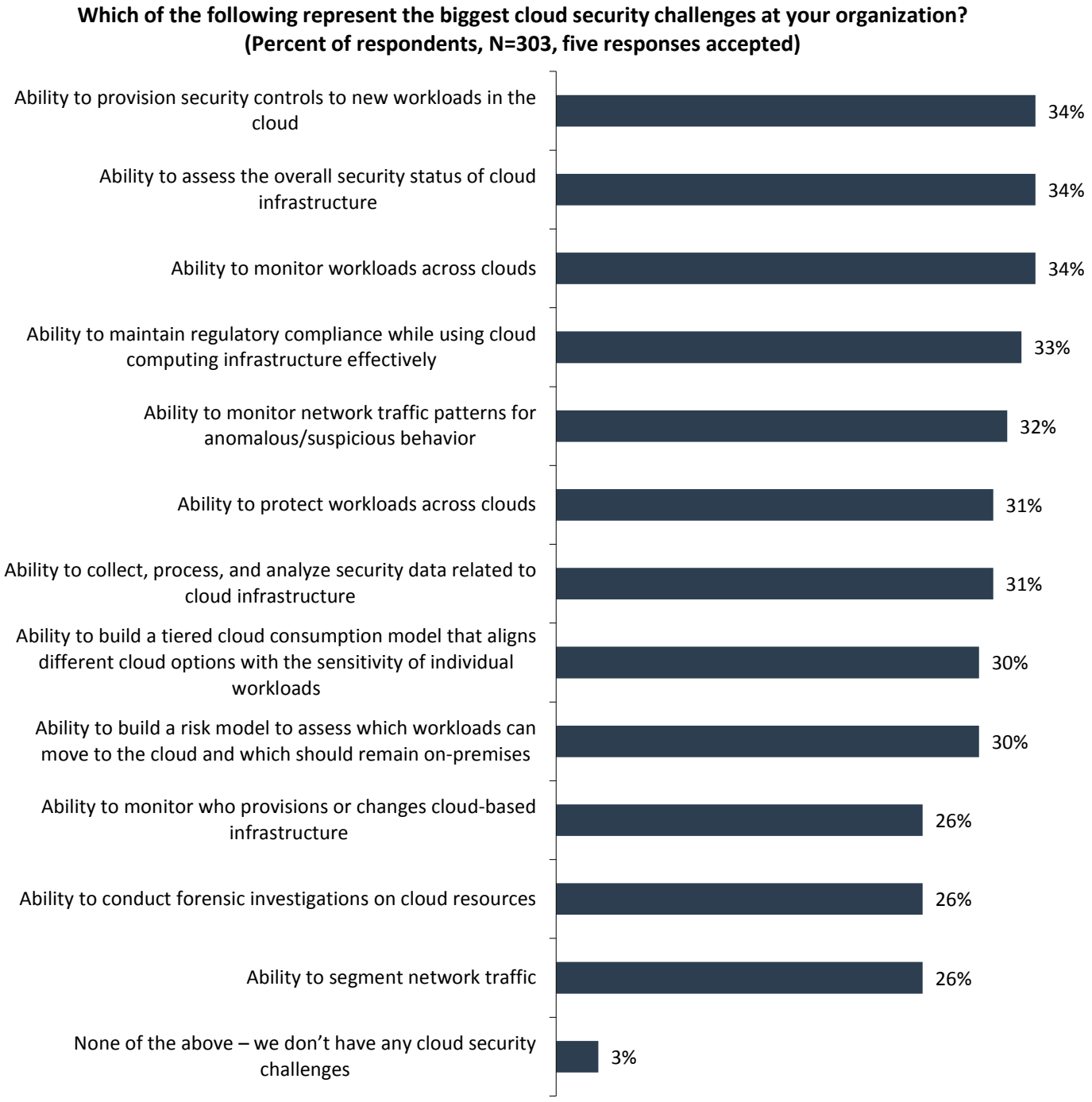
As cybersecurity professionals know, you can't secure what you can't see, resulting in some not trusting the security posture of cloud services. Yet unsanctioned cloud apps as well as the sprawl of cloud-resident workloads tend to obscure the critical information contained in the 5 Ws:

- What cloud services and applications are in use, what risks are associated, and what sensitive data (or malicious content) is stored with each service.
- Who is using the service and app, what data they are accessing, and how they are being authenticated and authorized.
- Where and when users are accessing cloud services and apps.
- Why users are resorting to unsanctioned cloud services and apps (i.e., shadow IT).

According to ESG research, 34% of organizations indicated that one of their biggest cloud security challenges is their ability to assess the overall security status of cloud infrastructure (see Figure 2). Concern with the ability to monitor workloads across clouds was also cited by 34%. Other visibility concerns include the ability to maintain regulatory compliance, the ability to monitor network traffic patterns for anomalous or suspicious behavior, the ability to collect, process, and analyze cloud security data, the ability to monitor who provisions or changes cloud-based infrastructure, and the ability to conduct forensic investigations.[12] This reveals that organizations understand that the cloud obscures visibility regarding critical security data.

[11] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.
[12] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

Figure 2. Biggest Cloud Security Challenges



Source: Enterprise Strategy Group, 2016

The Focus on Data Security

The use of public cloud services results in corporate data assets being stored with those cloud services. Many organizations consider this to be both a visibility and control gap. The increasing prevalence of shadow IT intensifies these security concerns.

Organizations have an especially acute concern for sensitive and strategic data, and it's not surprising that more than half (53%) of organizations are very concerned about storing sensitive data in the cloud. Shadow IT raises related concerns: In aggregate, 83% of organizations state they are either very or somewhat concerned with the use of shadow IT applications that could leak sensitive data. Forty-five percent are very concerned with maintaining a strong security policy in the context of the speed at which DevOps methodologies provision cloud services. The use of cloud applications as a threat vector is also a worry, with 43% of respondents indicating they are very concerned about the use of cloud applications as a means to distribute malware.[13]

In 2016, nearly half (49%) of organizations cited data security as one of three the cloud security areas in most need of improvement at their organizations in the following 12 to 24 months. Additional areas needing improvement were both process- and technology-related, with 41% of organizations citing a need to align existing security policies, processes, and technologies with cloud computing, while 35% stated a need to deploy a CASB solution coincident with a sanctioned IT application, and 32% identified the need to monitor and block shadow IT.[14]

Traditional Data Center Security Is Not Cloud-ready

Traditional data center security controls, like traditional data center management tools, tend to be hardware-centric, focused on protecting physical assets—compute servers, networks, and storage. Some network security technologies (i.e., physical firewall and IDS/IPS appliances, DLP gateways, switch- and router-based ACLs, Layer 2 VLANs, etc.) are a mismatch for cloud computing, but are still essential elements of a hybrid cloud security strategy. The same holds true with security monitoring, where cloud computing often leads to blind spots or data management issues (i.e., collecting the right data in a timely manner, normalizing different data formats, etc.) such as the monitoring of the use of cloud APIs, access to cloud management consoles, and cloud-resident workload activity.

Cloud bursting morphs the security perimeter, which grows and shrinks to accommodate growing and shrinking workloads. The required fluidity is changing IT perspectives around the security perimeter. With cloud architectures, security moves from focusing on the data center to focusing on the workload. Workload-centric security establishes a perimeter around the workload, and controls which, when, where, and how users can access the workload. This security perimeter moves with the workload, ensuring consistent security policies, attributes, and management regardless of the physical location of the workload.

Hybrid and multi-cloud environments challenge mobile workload security. Each cloud service provider has its own set of unique security tools and processes. This creates a complex IT supply chain that organizations must manage themselves to ensure the correct and consistent application of security policies across their entire suite of internal and external clouds, even as workloads move, applications scale, and policies change.

Once organizations understand the limitations of applying traditional security to the cloud, they adjust accordingly to meet the requirements and nuances of hybrid and multi-cloud infrastructures. Little wonder then that 74% of organizations are replacing traditional security processes and choosing extensible, scalable, and independent security technologies designed for cloud computing.[15]

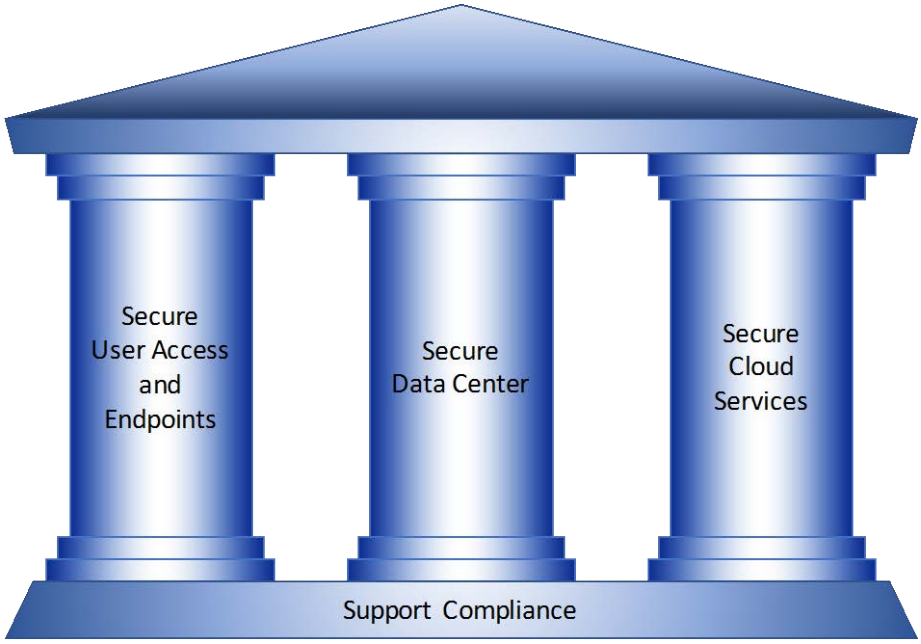
Requirements for End-to-end Security

The readiness gap, where security policies and controls are more mature for on-premises infrastructures than for the cloud, highlights the need for organizations to rethink cybersecurity for the new, software-defined, API-driven hybrid cloud

[13] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.
[14] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.
[15] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

world. Organizations need to maintain secure user access and endpoints, secure data center, secure cloud services, and support compliance. Taken together, these are the pillars of secure IT (see Figure 3).

Figure 3. The Pillars of Secure IT



Source: Enterprise Strategy Group, 2017

Secure User Access and Endpoints

Securing user access and the endpoints they operate requires gaining visibility into who is accessing what resources, understanding the business context of that use to determine whether it is appropriate, applying access control levels (ACLs), and performing ongoing monitoring for anomalous activity that could be indicative of a compromise. The cybersecurity best practice of least privileged access is the core construct of assuring secure user access, one that grants the least number of users the least amount of privileges to the least amount of resources, especially sensitive data. Access controls to protect data assets should be implemented as data loss prevention (DLP) policies to control not only which users can access which classes of data types, but what privileges they have for specific types of data. Creating least privileged access security policies for the digital workspace—comprised of mobile knowledge workers, endpoints, and things (IoT)—requires thinking of users and their devices as being a perimeter that needs to be secured to protect against both external and insider threats. Organizations should also employ a "trust, but verify" approach, which necessitates having sufficient context via monitoring who is using which devices to access what data assets, when, and from where. As such, there are two dimensions to access controls–devices and the users who operate them.

Secure Data Center

Most organizations operate in a hybrid cloud environment, maintaining their own physical infrastructure on-premises, or in a colocation facility, in addition to utilizing public cloud services. The data center portion of a hybrid cloud security strategy is one with a focus on protecting physical and virtual assets with a network-centric approach by employing highly performant firewalls, gateways, and intrusion detection and prevention systems.

While such an architecture protects the infrastructure behind the firewall, the security requirements specific to a new on-premises application are all too often implemented as, or after, that application is deployed to production. Cybersecurity

requirements should be treated as of equal importance to the functional requirements of applications so that security is integrated and not bolted on.

The principle of least privileged should also be applied to the data center. IT needs to control the level of privileges users, especially systems administrators, have to applications, data, compute, storage, and networking resources in the data center. Access to an organization's mission-critical resources and sensitive data assets should require a second factor of authentication and access should be audited. Least privileged access also applies to application workloads by leveraging micro-segmentation to assure that only authorized workloads in an application stack can communicate with each other. Furthermore, east-west traffic between workloads should be monitored for the possible lateral movement of threats.

Secure Cloud

According to ESG research, 36% of organizations have implemented a cloud-first policy, while 44% give equal weight to cloud or on-premises infrastructures.[16] As a result, more applications are being deployed in public cloud environments, requiring that organizations fully understand the shared responsibility security model, which depicts the respective areas of responsibility between the cloud service provider (CSP) and customer. Since the CSP is responsible for physical network security and customers do not have direct access to the network, a cloud security strategy must be grounded in a logical versus physical implementation.

The temporal nature of cloud-based infrastructure in which resources are automatically provisioned and de-provisioned requires an orientation around new conventions and methodologies. For example, cloud-resident workloads are addressed by tags based on key-value pairs and not names and IP addresses. As a software-defined environment that is API-driven, cloud infrastructure is code and managed by the DevOps methodology of automating the continuous integration and delivery (CI/CD) of code and infrastructure. Organizations should incorporate security practices and controls into their DevOps pipeline so that security is bolted in before new application stacks are deployed to production.

The principle of least privileged access should also be applied to workloads in cloud environments. In addition to the user-centric perspective that controls user access to data, IT needs to protect their cloud infrastructure with a workload-centric approach that limits an application's access to services and data to those that are minimally required. As discussed above, the use of micro-segmentation to create logical perimeters that control the east-west traffic between the various components of an application, such as between the control logic and the database server, is a least privileged implementation that also applies to cloud-resident workloads. In so doing, isolating and protecting east-west traffic prevents malicious code from snooping into conversations and gaining unauthorized access to sensitive data.

The change in perspective from the physical to the logical means that traditional network perimeter-centric security must be augmented with data-, workload-, and user-centric security. Security needs to be a primary concern during the design phase, ensuring that security can change with the cloud infrastructure being protected. Policies and controls need to be associated with, and move with, data, workloads, and users, all of which represent the new perimeter of cloud infrastructure.

Support Compliance

The heterogeneous nature of today's data center makes risk management and compliance increasingly complicated. In a cloud or hybrid cloud context, organizations delegate control over a portion of their infrastructures to third parties–their cloud service providers (CSPs). Risk management is especially important with public clouds, where data ownership and sovereignty are not always clear. For example, IaaS providers reference the shared responsibility model, in which the CSP is

[16] Source: ESG Research Report, *2017 Public Cloud Computing Trends*, April 2017.

responsible for security and compliance with regulations for the underlying infrastructure, up to the hypervisors. IaaS customers are still responsible for security and compliance for workloads, applications, and data.

Cloud environments are dynamic, and risk is a fluid concept. Cloud application risk considerations include provider reputation, adherence to security best practices, publication of security policies and audits, regulatory compliance, data-criticality, and business-criticality. Modern cloud security must build in continuous governance, risk management, and compliance (GRC) processes. GRC needs to extend from the edgepoint through the workload to the hybrid and multi-cloud infrastructure. This requires augmenting traditional hardware-based IT telemetry with modern software-defined, API-driven telemetry systems that instrument who is doing what to which data using which endpoints, along with the location of the data and the user.

Centralized Security Views of a Decentralized IT Environment

End-to-end security across the mobile, hybrid, and multi-cloud environment requires telemetry from any entity that has a risk of compromise. Organizations also require threat intelligence—evidence-based knowledge about an existing threat to any organizational asset. Threat intelligence provides actionable information regarding the mechanisms, indicators, and implications of the threat.

Integrating end-to-end telemetry with threat intelligence provides contextual connectivity. Cybersecurity professionals gain the ability to understand and provide context to what's happening as the organization's users make a connection between an edgepoint and a workload to manipulate data.

Hybrid and multi-cloud environments represent a decentralization of IT, and provide for the most efficient use of scarce and costly resources. Security operations and analytics platform architectures (SOAPA) wrap a unified security architecture across all assets in heterogeneous hybrid and multi-cloud environments. SOAPA integrates all security data and processes, and enables the security team to surface and address the areas with the most risk, those under attack, and those currently compromised. This requires automation and orchestration to ensure that security professionals are not overwhelmed by manual processes, alert storms, threat storms, etc., and is especially important given the global cybersecurity skills shortage and the ever-expanding cloud infrastructure and its concomitant attack surface area.

The Bigger Truth

Digital transformation, inspired and enabled by new technologies and the consumerization of IT, brings about profound changes to business strategy, business models, and business processes. Technologies such as hybrid and multi-cloud services, mobility, and IoT expand the attack surface area and increase the GRC challenge. There is a readiness gap, where cloud and modern IT adoption is much more mature than cloud and modern IT security.

A holistic and strategic approach is required to protect assets that comprise an organization's modern IT environment. The pillars of security in the modern IT environment provide a framework for such an approach. Secure access and endpoints have clear definitions of acceptable users, devices, and locations, and controls enforce the principle of least privileged access. Policies move in concert with these mobile elements. Secure data centers have network-centric controls on access to data, applications, compute, storage, and network resources. Secure cloud application infrastructures have policies and controls that are workload-, user-, and data-centric. Support compliance requires telemetry and risk management across hybrid clouds and all other assets in the environment.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188