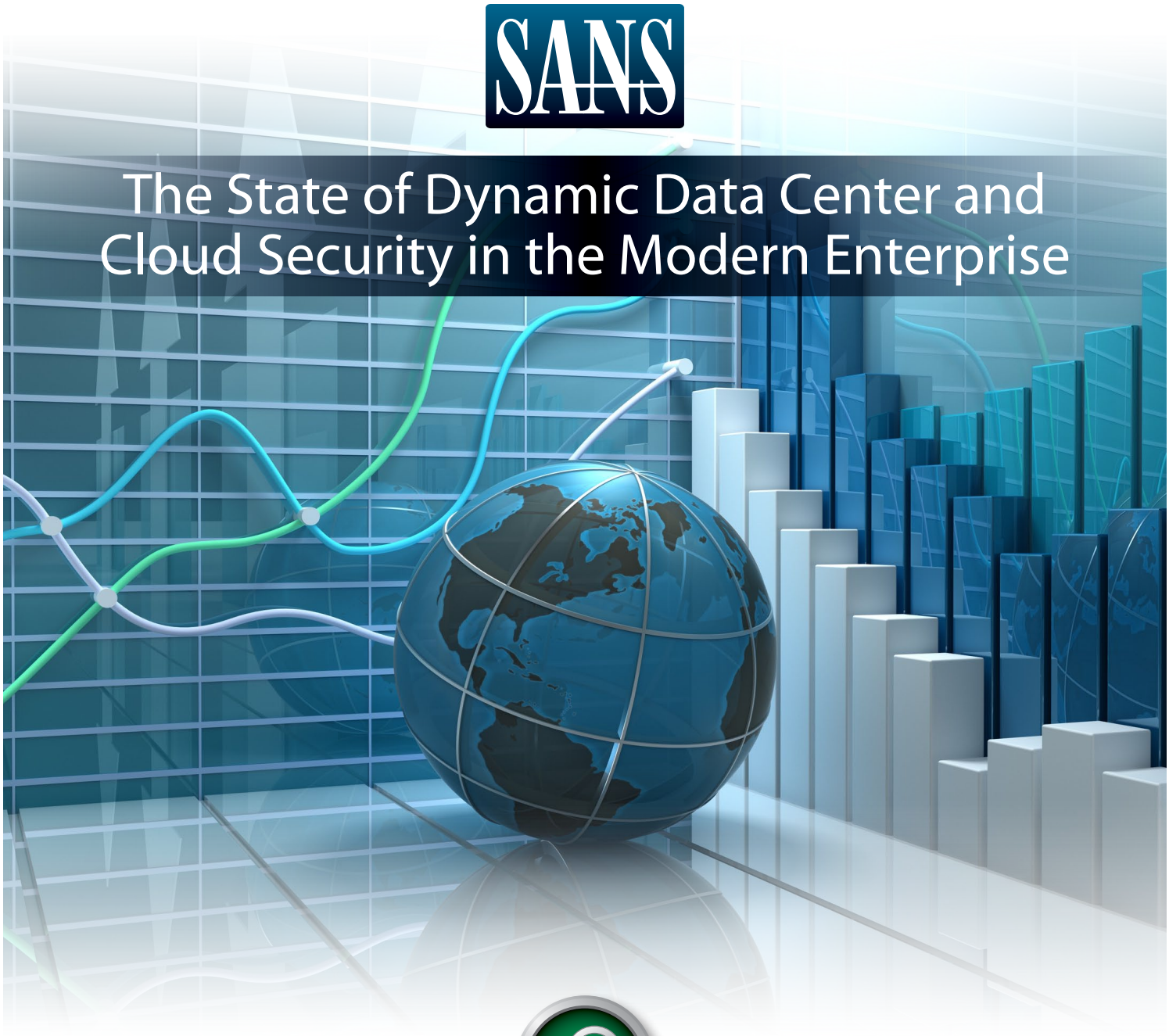


The State of Dynamic Data Center and Cloud Security in the Modern Enterprise

A SANS Survey

Written by Dave Shackleford

October 2015

Sponsored by
Illumio

Executive Summary

The variety of architectural options available to corporate data centers has grown enormously as organizations have moved workloads from traditional data center deployments to hybrid cloud infrastructures that can be managed dynamically among internal and cloud-based data centers. In the SANS Dynamic Data Center Survey, respondents reported a variety of data center structures, including traditional proprietary data centers, traditional multitenant structures, as well as private and public cloud infrastructures. As a result, the connections between corporate information systems have become more complex.

Many of the security concerns that kept enterprises from embracing earlier cloud computing models still remain, ranging from account and identity management to application flaws and malware. Application flaws and malware are the biggest threats, with 50% reporting system and data compromises due to application flaws and 45% attributing compromises to malware. Visibility is a problem for 44% of respondents, who said their cloud providers don't allow them to see into those environments well enough to protect users or data. Public cloud providers also don't offer insight or access to tried-and-true security technologies that enterprises have come to rely on, according to 19% of survey takers.

Enterprises seem to be evolving from traditional IT infrastructure models to a range of newer, often more complex structures, and both enterprise security and distributed computing appear to be at an evolutionary crossroad. Breach and incident data reported by IT teams suggest that traditional security strategies and controls struggle to keep up with the risks facing traditional enterprise models and are inadequate for the challenges they face in trying to address dynamic computing environments.

Fully 80% of respondents polled by the Cloud Security Alliance (CSA) for a recently published report[1] said their security concerns are serious enough that they are pushing cloud providers for more transparency and improved auditing controls; 57% said they are asking for more and better encryption tools as well. Nearly one in five (18%) use only private cloud deployments. Of those, 86% said the decision was due primarily to concerns such as threats to data confidentiality and loss of control over enterprise data.

Key Findings

of those able to share their breach history have experienced a breach resulting in the loss of sensitive data

are concerned with access management and privileged account management vulnerabilities in their data centers and in the cloud, with 64% concerned with application vulnerabilities

have no visibility into East-West traffic in their data center or cloud environments (or know whether they do)

use network IDS/IPS, malware detection tools, and access control lists (ACLs) on intermediate routers and switches to secure their East-West traffic

revealed it takes more than two weeks to implement security change controls

have experienced attacks against workloads in their data center or cloud environments, and 25% don't know whether they have experienced attacks

are dissatisfied with their current attack containment and recovery times

[1] https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

The potential risk from cloud services or providers represents just one set of elements in an increasingly complex picture. The real problem is that security concerns grow along with increases in complexity. According to this survey and other SANS reports,[2] many organizations are concerned about how to react to increasing pressure to scale their data center and IT architectures, adapt to new computing models and quickly embrace complex architectures.

As organizations' data centers become more dynamic and the need to scale quickly in complex architectures grows, security will need to adapt accordingly. Based on feedback from this survey, the following seems clear:

- Most organizations' computing surfaces are expanding, with the majority reporting a mix of traditional data center and cloud service infrastructure in place. They use a broad array of traditional security controls, many of which don't work well (or at all) in the cloud. Huge changes are being made to computing infrastructures, which include the addition of more dynamic data center processes such as DevOps and expansion into clouds; however, organizations are not adding technologies that respond to security challenges created by these major shifts in computing.
- The top types of attack vectors concerning most enterprises are access management flaws, application vulnerabilities, malware, advanced multistage attacks and poor security habits of employees. In the case of this survey, 44% of respondents willing to share their breach experiences have faced at least one breach in which sensitive data was accessed by attackers.
- Among the key security capabilities missing in modern dynamic data centers and clouds are visibility, rapid attack identification, and fast, accurate and automated containment. As the data shows, many organizations have experienced attacks both in the cloud and in their own data centers.

[2] "Conquering Network Security Challenges in Distributed Enterprises," July 2015, www.sans.org/reading-room/whitepapers/analyst/conquering-network-security-challenges-distributed-enterprises-36007

"Enabling Big Data by Removing Security and Compliance Barriers," September 2014, www.sans.org/reading-room/whitepapers/analyst/enabling-big-data-removing-security-compliance-barriers-36017

"Data Center Server Security Survey 2014," October 2014, www.sans.org/reading-room/whitepapers/analyst/data-center-server-security-survey-2014-35567

"The Case for Visibility: SANS 2nd Annual Survey on the State of Endpoint Risk and Security," March 2015, www.sans.org/reading-room/whitepapers/analyst/case-visibility-2nd-annual-survey-state-endpoint-risk-security-35927

"SANS Analytics and Intelligence Survey 2014," October 2014, www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

"SANS Ninth Log Management Survey Report," October 2014, www.sans.org/reading-room/whitepapers/analyst/ninth-log-management-survey-report-35497

About the Respondents

Most enterprises rely on a variety of time-tested, best-practice information security practices and policies to secure their computing environments, according to respondents to the SANS Dynamic Data Center Survey, completed by 430 IT professionals working in security-related disciplines. Respondents are less clear about whether these traditional approaches can work in a much more dynamic computing environment with a heterogeneous mix of bare metal and virtual servers and data centers and clouds.

Respondents represent a variety of industries. The largest overall category, represented by 18% of respondents, was government. Banking and finance was the next largest category, with 14%, followed by information technology (10%). A mix of other industries including manufacturing, health care, consulting, telecommunications and many others responded to the survey, lending credence to the reality that all types of industries are using or planning to use dynamic data centers. The top 10 industries represented are shown in Table 1.

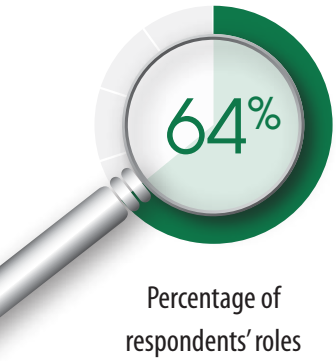
DYNAMIC DATA CENTER
A scalable data center that uses automation and virtualization to meet the demand for IT resources provided by private and public clouds, SaaS, mobile and terrestrial networks, and other sources

Table 1. Top 10 Industries Represented

Rank	Industry	Percent
1	Government	17.5%
2	Banking and finance	14.2%
3	Information technology	10.2%
4	Manufacturing	7.7%
5	Education	7.4%
6	Health care/Medical	7.2%
7	Consulting	4.9%
8	Telecommunications	4.7%
9	Insurance	4.4%
10	Retail	4.0%

The majority of the respondents (64%) worked in organizations with more than 1,000 workers, and 23% worked in large enterprises of more than 15,000. Another 23% worked in smaller environments with 100–1,000 staff, and 13% had fewer than 100 employees.

Most respondents (77%) have some presence in the United States, and 58% are headquartered in the United States. More than a quarter each operate in Europe (29%) and the Asia-Pacific region (25%). Slightly fewer than 22% have a presence in Canada, with the remaining regions represented by fewer than 20% of respondents.



Percentage of respondents' roles focused on security and compliance

Security administrators/security analysts made up 39% of the respondents. Security managers and executives came in at 15%, and IT managers and executives as well as network operations and system administrators both came in at 11%, as illustrated in Figure 1.

What is your primary role in the organization?

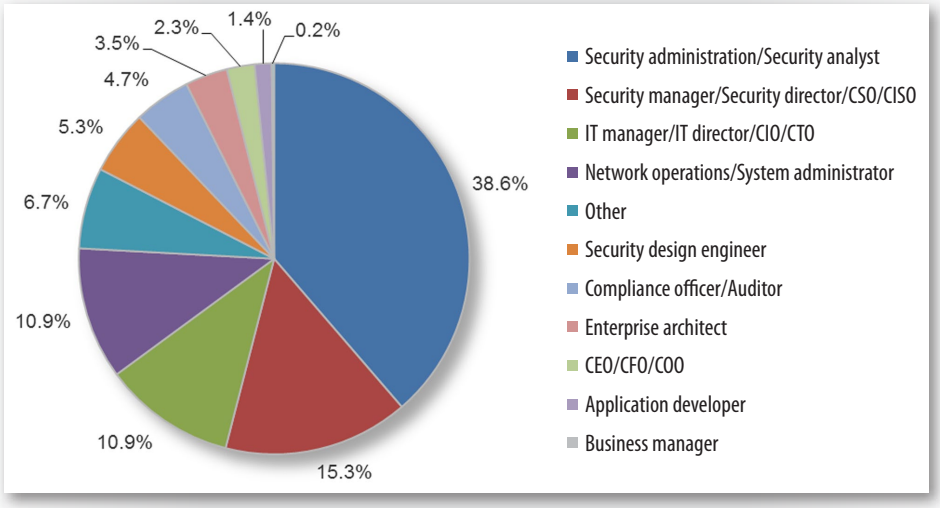


Figure 1. Respondent Job Roles

Overall, this survey garnered attention from organizations of all sizes, predominately in the U.S., but with some international representation. The sample represents a broad spectrum of IT and security professionals in both engineering and management positions, all of whom are concerned with the security of cloud services and hybrid data center deployments.

Security teams are decidedly still concerned about attacks and security issues. In this survey, 68% of respondents cited access and privilege management events, and 64% highlighted application vulnerabilities, both issues that could easily affect internal data center infrastructures and applications as much as cloud deployments. In fact, one respondent stated that assigning too many permissions and privileges in one major cloud provider's portal was a big concern, emphasizing both of these issues.

Advanced multistage attacks and malware infections continue to be key concerns in enterprises of all sizes, at 62% and 61%, respectively. Figure 2 illustrates the attack vectors of greatest concern.

What type of attack vectors are you most concerned about with regard to your data center or cloud infrastructure?

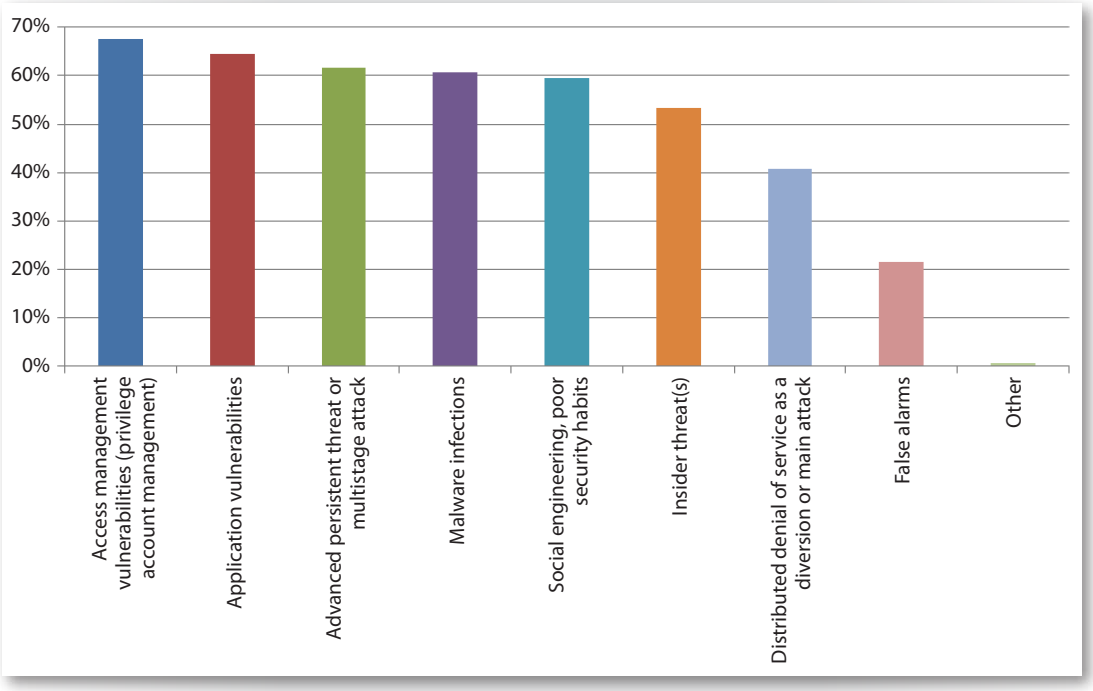


Figure 2. Today's Top Security Concerns

Respondents could choose more than one attack vector to be concerned about. Still, it is surprising to see that the six most often-cited issues were a concern to more than half of all respondents, highlighting the significant concerns these vectors present to dynamic data centers.

Even with these defined attack vectors, 37% of respondents indicated they had experienced a compromise of some sort, an equal percentage said they had not, and 25% weren't sure. Of those who had experienced attacks, 50% blamed exploits of application vulnerabilities; 45% blamed malware; 33% fell victim to social engineering techniques; and 31% said they'd been hit by a distributed denial of service (DDoS) attack. Figure 3 provides a breakdown of the sources that result in compromise.

What types of attacks have actually resulted in the compromise of a server, system or workload inside your data center or cloud-based deployments?
Select all that apply.

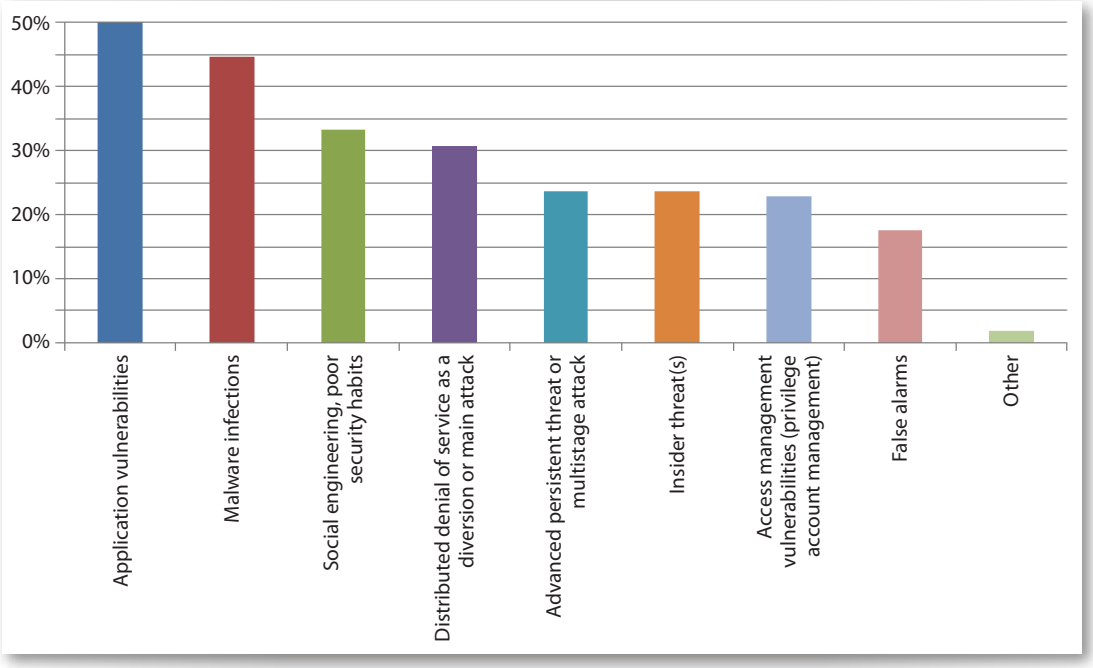


Figure 3. Root Cause of Compromise

TAKEAWAY:

Organizations need to focus on privileged account management, advanced malware detection and response, and security awareness training. These security control areas can help reduce some of the top avenues of potential compromise today.

Advanced multistage attacks and insider threats were responsible for compromises for 24% of respondents. Interestingly, although access and privilege management issues were the top concern for respondents, they blamed that vector for only 18% of successful compromise scenarios.

It's not surprising that many of the root cause scenarios were related to application flaws or malware of some sort, as these tend to be the most prevalent direct attack models today. User involvement in attacks is also increasing, usually through social engineering, so its positioning as the third most common compromise vector is also expected.

Containment and Recovery

Time to containment and recovery from attacks is crucial to limiting loss of data and the costs of a breach. With regard to containment, 37% of respondents were able to get their incidents under control within 8 hours, which reflects the nature of application-centric or malware-based infections. Usually systems can be quarantined, and the malware can also be cleaned or quarantined in some cases. In application attacks, development and security teams can remove attacker data or take applications offline temporarily.

Another 21% of respondents contained the issue(s) within 8 to 24 hours, and an additional 19% contained the problem in less than a week. Unfortunately, 17% took more than a week to contain the attack. See Figure 4.

TAKEAWAY:

Take steps to cover the major avenues of compromise, including application flaws, malware and social engineering. Invest in controls that can isolate threats and contain potential attacks, providing more time for analysis and recovery without affecting the rest of your environment.

In general, how long from the time the attack was detected has it taken you to contain the attack and fully recover from its effect?

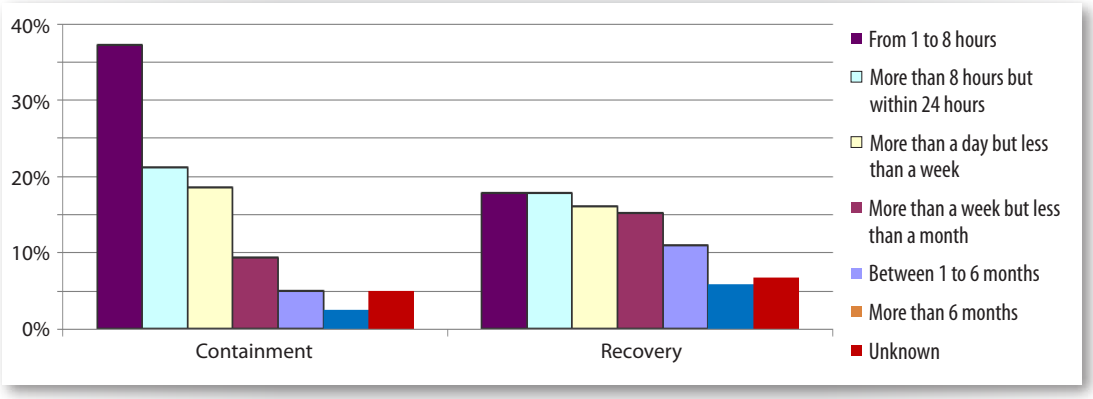


Figure 4. Containment and Response Times

Recovery times were much more evenly spread out, which may reflect the larger scale or severity of the incidents some respondents faced. Just under 18% of respondents recovered within 1 to 8 hours. Another 18% took 8 to 24 hours, and an additional 16% took up to a week.

In both the containment and recovery phases of incident response, a small number of respondents stated that they didn't know how long the containment and recovery times took during these incidents. But most (55%) were dissatisfied with the amount of time containment and full recovery took.

Just over half of enterprises are able to contain incidents within 24 hours, which leaves many open to continued damage. More than 9% of respondents took between a week and a month to contain incidents, and another 5% took between one and six months, which may demonstrate that traditional security tools are not helping organizations get a handle on attack scenarios. During attacks, time is of the essence. If enterprises are alerted to attacks without the ability to contain and respond to them rapidly, the security program's overall effectiveness is diminished.

Data Compromise

Simply experiencing an attack or incident doesn't mean that sensitive data was accessed or stolen. Unfortunately, of those able to share their breach experiences, 44% reported having sensitive data accessed by the attackers in at least one attack. Looking at the entire data set, 20% experienced one or two breaches as a result of the attacks, another 8% reported three to six breaches and less than 1% noted experiencing more than six breaches. Another 17% didn't know if they had been breached, and 17% declined to answer. This may indicate that even more breaches actually occurred and that respondents chose not to respond. See Figure 5.

TAKEAWAY:

Most organizations have experienced at least one breach that led to data theft or exposure. Operate under the assumption that you will be breached, and put more effort and investment into security controls and processes that enable rapid detection, containment and response.

How many times, in the past 24 months, have attacks resulted in a breach that led to theft of your customers' regulated data or your intellectual property?

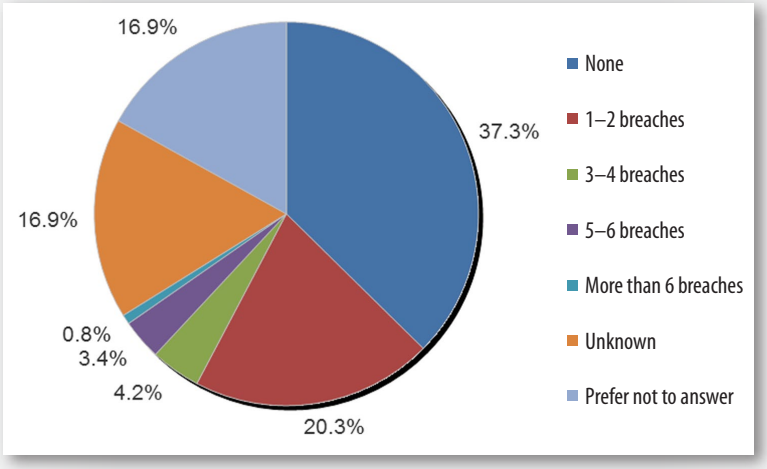


Figure 5. Attacks Leading to Breaches

How often an attack results in a breach varies among the top 10 industries included in this survey. Respondents from education, government (nondefense) and IT have the highest level of attacks, accounting for 12% of the reported attacks. Each attack appears to result in the compromise of a server, system or workload inside the respondent's data center or cloud-based deployment. Considering the ratio of breaches to attacks, however, these industry segments have a moderate to low level of actual breaches, with 36% of attacks turning into breaches for education and IT, and just 7% for government (nondefense). On the other hand, the banking and finance sector accounts for only 8% of the attacks, but 60% of those attacks are converted to breaches. Consulting has a similar breach-to-attack ratio. And, for the relatively small number of retailers participating in this survey, the retail industry has a very high breach-to-attack ratio, at 75%. This raises the question of whether preparedness against attack/compromise may be different from preparing for a breach once a compromise has occurred. See Table 2.

TAKEAWAY:

Organizations of all sizes and from all industry sectors must prepare not only to prevent attacks but to have containment and remediation plans and technologies in place when a breach occurs.

Table 2. Comparison of Breach-to-Attack Ratio by Industry

Industry	Attack	Compromise	Both	Ratio of breach to attack
Education	11.5%	11.5%	4.1%	35.7%
Government (Nondefense)	11.5%	11.5%	0.8%	7.1%
Information technology	11.5%	11.5%	4.1%	35.7%
Health care/Medical	9.0%	8.2%	2.5%	27.3%
Manufacturing	9.0%	7.4%	1.6%	18.2%
Banking and finance	8.2%	8.2%	4.9%	60.0%
Government (Defense)	6.6%	6.6%	1.6%	25.0%
Insurance	4.9%	4.1%	0.0%	0.0%
Telecommunications	4.9%	4.9%	1.6%	33.3%
Consulting	4.1%	4.1%	2.5%	60.0%
Retail	3.3%	3.3%	2.5%	75.0%

Organizational size appears to have some effect on how many attacks result in breaches. Looking at the ratio of breach to attack, organizations of 2,000 or greater experience a breach 30% of the time or more when they are attacked. For entities with 5,001 to 10,000 employees, that ratio increases to 50%.

Although most organizations are combating sophisticated attacks and data compromise incidents, the design and function of today's data centers is changing dramatically. Many organizations are moving assets to the public cloud, and the nature of security controls may need to change to accommodate this as well. In fact, some types of security controls may not even be available in all cloud architecture models.

Data Center Architecture and Deployment Types

In the past, the majority of organizations either built their own data center infrastructures (usually only large enterprises) or leveraged multitenant data center environments (co-location facilities or colos). Today, with the addition of multiple cloud service deployment scenarios, the lines are blurring between where and how organizations create and maintain their data center infrastructure and computing assets. Organizations have been steadily moving away from a single type of data center deployment for quite some time, and both private and public cloud services and technologies have become more integrated into complex application and server architecture designs. The survey results confirm this trend. Figure 6 shows the breakdown of different infrastructure types respondents' organizations are currently using.

Does your organization currently have any of the following?
Select all that apply.

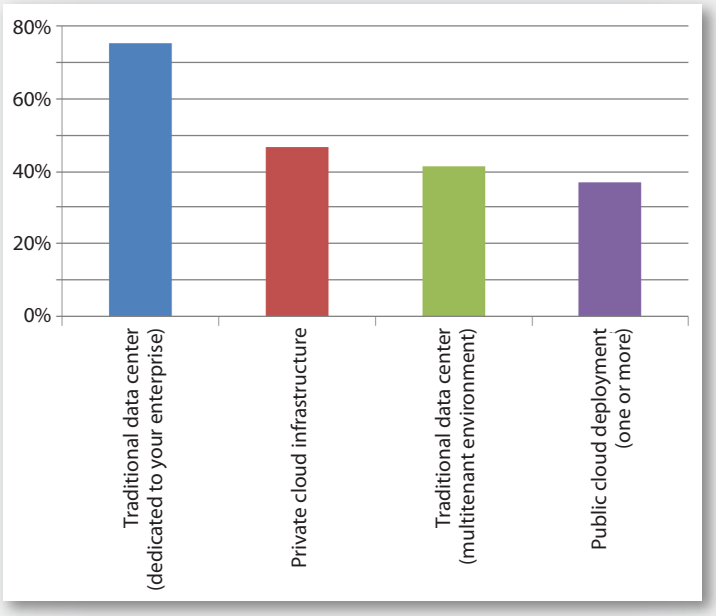


Figure 6. IT Deployment Types

SANS analyzed the number of breaches by the type of data center deployment, and the results seem to indicate that organizations that experienced up to four breaches are still seeing more breaches occur in their own data center environments than in the public cloud. Those who experienced five to six breaches in the past 24 months saw just as many in the public cloud as in other environments. This result may speak to the comparative amounts of data housed in the traditional setting as opposed to the public cloud setting. However, given that the majority of respondents either did not experience breaches (that they know of) or chose not to answer, these results are somewhat inconclusive.

Deployment Types Defined

Public and private clouds for servers are commonly called *infrastructure-as-a-service* (IaaS). Private cloud implementations can be located on-premises (private data center or colo) or situated within a public cloud provider environment (often referred to as a *virtual private cloud*, or VPC). *Platform-as-a-service* (PaaS) clouds and *software-as-a-service* (SaaS) models can also be set up on-site or in public environments, but tend to be deployed in public cloud provider environments. Table 3 breaks down the components in each deployment, as well as the most prevalent risks.

TRADITIONAL DATA CENTER

A standalone building, often owned and operated by the organization, designed and engineered to support a single organization's computing assets. Some organizations may use several floors of an existing structure instead of building a separate facility.

CO-LOCATION FACILITY

A similar facility, but the sites are subdivided into multiple tenant areas, usually via provision of separate racks, cages surrounding multiple racks, or even separate rooms or access-controlled spaces within the facility.

For more in-depth information on risks associated with cloud deployments, review the research from the Cloud Security Alliance Top Threats to Cloud Working Group.[3]

Table 3. Deployment Models, Components and Risks

Deployment Model	Components Installed and Maintained by Organizations	Top Risks
Private data center	All hardware, systems and applications	All infrastructure and apps are maintained by the organization, so all traditional IT and physical security risks apply.
Co-location facility	Most network devices, all servers and applications	Physical security is run by the colo provider, other tenants also host infrastructure and applications there. The primary risks are that physical security is breached by other tenants or insiders at the colo provider.
IaaS Private cloud (on-site)	Virtualization hypervisors or container platforms, virtual machines and applications	All virtualization components and systems, apps, and data are maintained by the organization, so all traditional IT and physical security risks apply. New risks may arise from the use of new technology, such as virtual machine escape or role/privilege misuse within virtualization and cloud tools.
IaaS Private cloud (VPC)	Virtual machines and applications, possibly virtual appliances and networking	The cloud provider maintains all hardware and physical security, as well as most networking functions and storage infrastructure. Risks from this may include exposure of sensitive data to the cloud provider personnel or other tenants. Some risks may still exist from other tenants, even though VPCs should be isolated, due to virtualization platform vulnerabilities.
PaaS (public)	Application components and data	The cloud provider maintains all hardware and physical security, as well as most networking functions and storage infrastructure. In addition, the provider usually maintains all control of the OS configuration within virtual machines. Risks include insider threats, configuration errors and risks from other tenants due to virtualization platform vulnerabilities.
SaaS (public)	Data	The cloud provider maintains control of all components. Only software-based controls within container or virtual machine instances are made available to providers. Insider threats, configuration issues and code flaws are the most prevalent risks in these environments.

[3] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

In this survey, 93% of respondents indicated they are deploying servers using virtualization tools and technology, with 68% using traditional (bare metal) server installations and 23% leveraging container technology.

A variety of different cloud services are in use today. Based on responses, 63% of enterprises surveyed are currently using SaaS offerings, with over half (51%) using IaaS for server deployments and one-third (33%) using PaaS. In addition, 39% are using cloud storage, 15% are implementing cloud-based desktops (DaaS). Two write-in responses also indicate the use of security-as-a-service (SecaaS), and six use no cloud services at all. Figure 7 shows the breakdown of different cloud services in use by survey respondents.

Which of the following types of cloud deployments are you currently using?
Select all that apply.

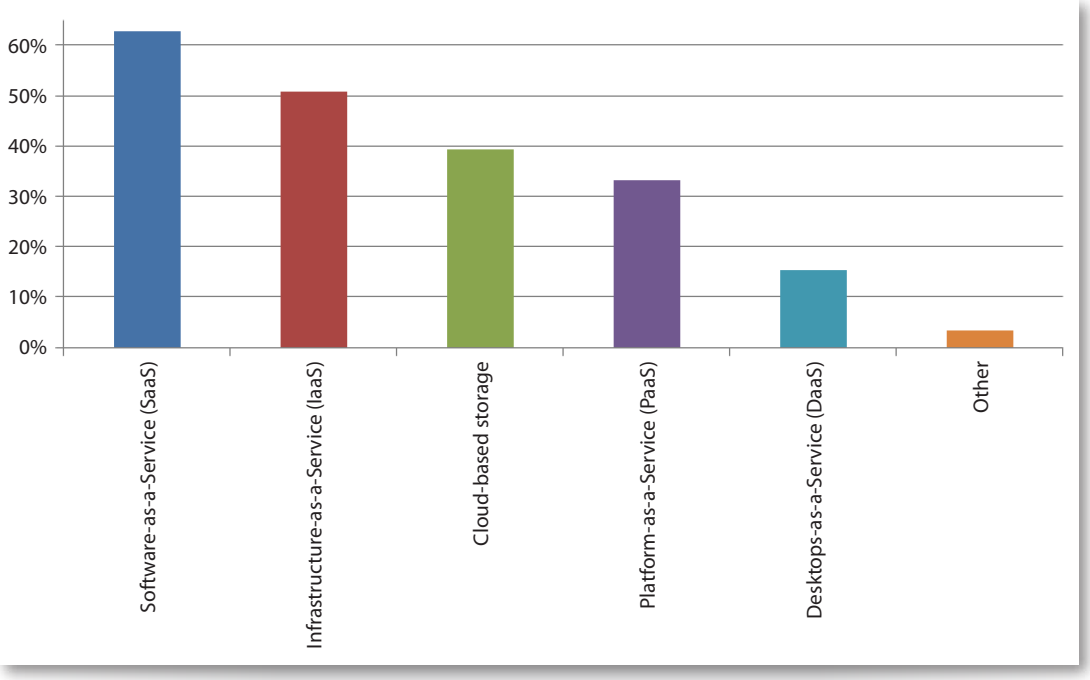


Figure 7. Cloud Service Use

SECURITY-AS-A-SERVICE (SecaaS)
A cloud business model in which the service providers or other vendors integrate their security services into the client's infrastructure on a subscription basis

When any of these services are deployed in the public cloud, organizations are putting their data and systems into environments where they fundamentally cede control of their infrastructure to cloud service providers (CSPs). To some, this is a reasonable risk to take, based on the attractive cost savings and business advantages. However, there are many hurdles to overcome.

Deployment Types and Compliance Initiatives

Love it or hate it, compliance is still a factor in organizations today. Most survey respondents are required to meet one or more compliance mandates, ranging from the PCI DSS, chosen by 56% of respondents, to HIPAA (36%) and various privacy laws, including the EU Data Protection Directive (15%) and Canada's PIPEDA (15%). Figure 8 shows the full list of compliance requirements organizations are responsible for in both data center and cloud deployments.

What are the applicable regulations or standards with which you must comply?
Select all that apply.

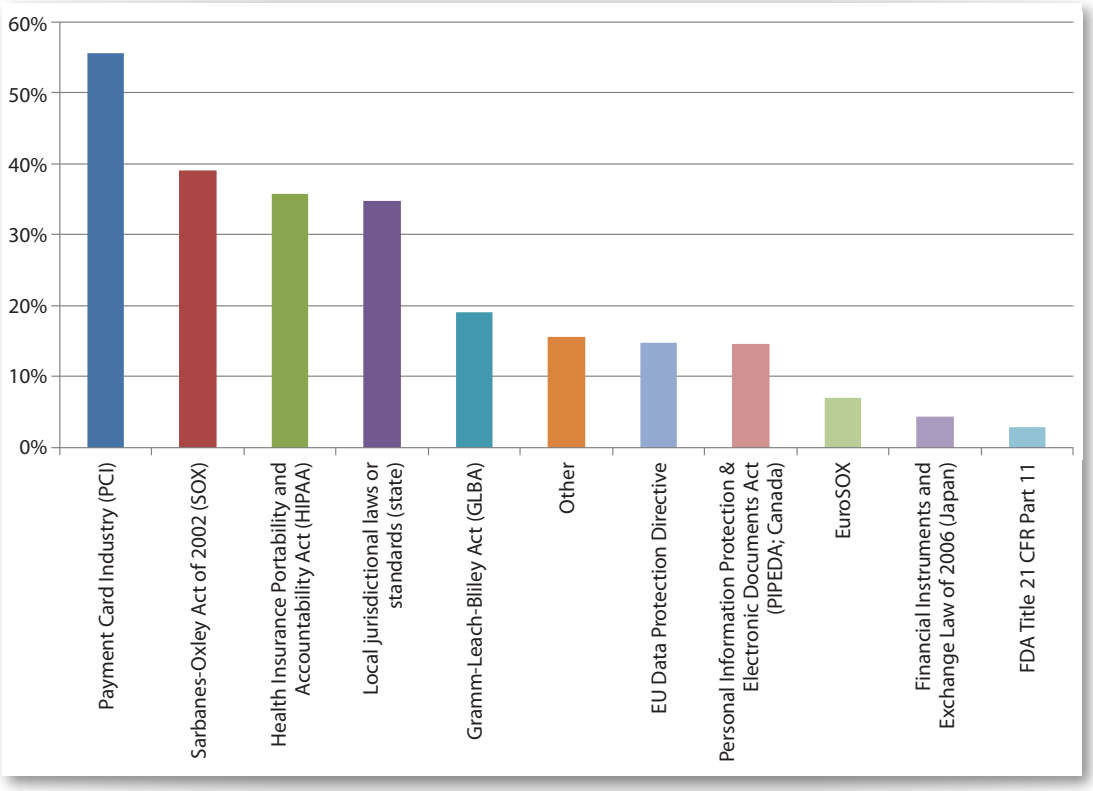


Figure 8. Regulatory Requirements of Enterprises Today

In the "other" category, organizations listed an array of other requirements that included military requirements for the U.S. Department of Defense (DoD) and others, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Family Educational Rights and Privacy Act (FERPA), ISO 27001, Australian privacy directives and more. All industry verticals are hoping to leverage cloud services more than ever, and the cloud providers are rising to the occasion with compliance-specific environments. In August 2014, for example, Amazon Web Services became the first cloud provider approved to handle sensitive DoD workloads.[4]

[4] www.nextgov.com/cloud-computing/2014/08/big-win-amazon-first-provider-authorized-handle-sensitive-dod-workloads/92069

Many of these regulatory and industry compliance requirements include specific security technologies and governance needs such as change control. In fact, based on experience, many organizations SANS works with are moving resources to cloud environments in an attempt to reduce the amount of time it takes to implement changes.

Deployment Types and Security Controls

Currently most respondents are using more security controls in traditional data centers than in the cloud. Figure 9 illustrates the use of security technologies and techniques.

Which of the following security technologies and techniques are you actively using in your organization's data center or cloud deployments?

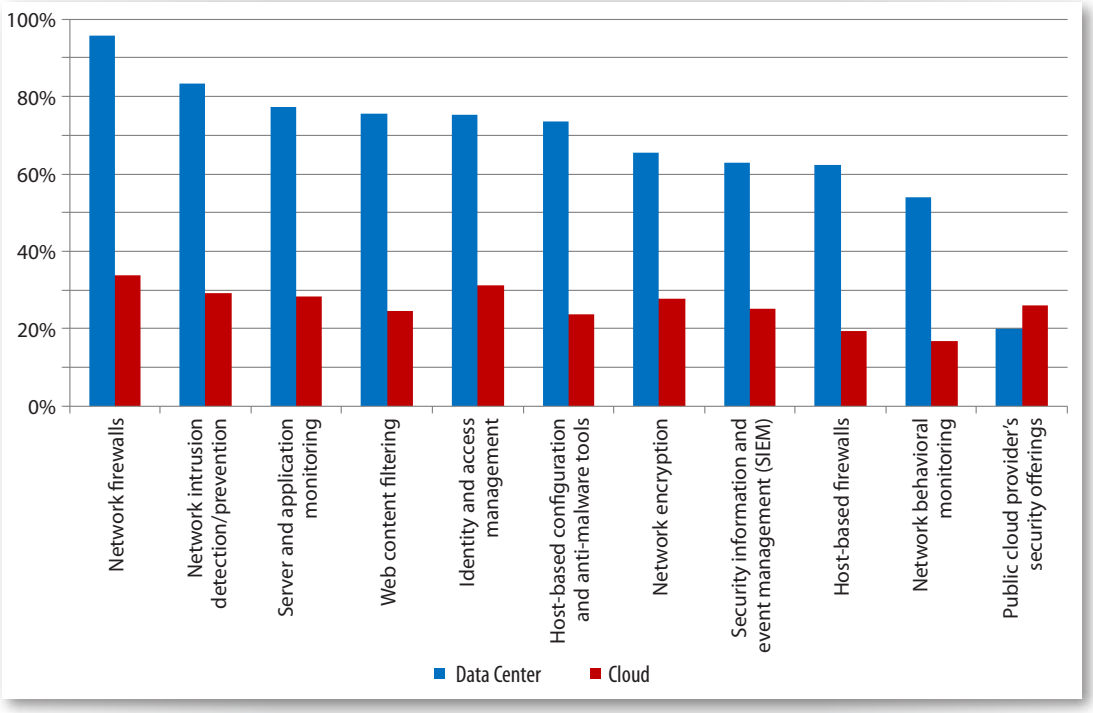


Figure 9. Security Technology in Use In-house and in the Cloud

Within the data center, the vast majority are employing network firewalls, network IDS and IPS, and server/application monitoring, selected by 96%, 83% and 77%, respectively. In addition, 75% use web content filtering, 75% use identity and access management tools, and 74% use host-based security and anti-malware tools. Roughly two-thirds are using network encryption (66%) and SIEM (63%).

However, the numbers drop sharply when we examine the tools in use within the cloud. Just 34% make use of network firewalls, 29% rely on network IDS and IPS, and only 28% monitor servers and applications. Web content filtering fell off considerably, with only 25% taking this approach. Only 31% use identity and access management tools, while 24% deploy host-based security and anti-malware tools, 28% incorporate network encryption and 25% use SIEM.

This seeming reduction in use of security tools is a huge issue for many organizations today, given the fact that many public cloud providers don't currently offer or support many security tools considered standard by most security teams. While some cloud providers do have security offerings available, they fall far short of the security stack used by most survey respondents.

TAKEAWAY:

Work with cloud providers to enable the security tools, such as network firewalls, network intrusion detection and prevention, and identity and access management, but realize they are often significantly less effective in securing hybrid and dynamic workloads. New tools that enact policies closer to the workloads themselves, regardless of where they're running, may prove more effective in dynamic environments.

Making changes to security controls requires implementing change controls required by many regulatory groups. And, security changes do take a long time to implement, as shown in Figure 10.

From initial change request to final implementation, how long does it take for your security change controls (firewall rule changes, VLANSs, security zones, etc.) to be configured, approved and applied into production within your organization?

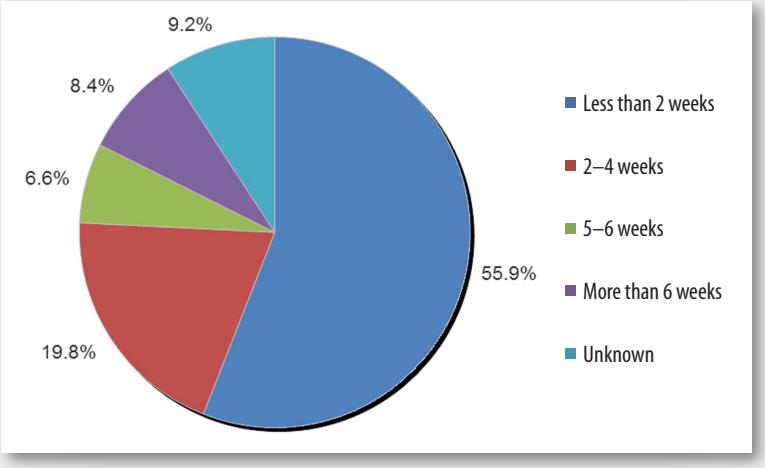


Figure 10. Security Change Control Timeframes

While 56% of respondents said they are able to implement changes in less than two weeks, many are still finding that security changes and updates take much longer, with 8% taking longer than six weeks to implement security changes. These kinds of changes are taking a long time with security technologies that are currently running in our own data centers and co-location facilities. The larger the organization, the longer it takes to implement changes. And, although the differences in the time to implement change in traditional and cloud environments in this survey are not significant, it is worth considering whether that will change as more technologies are migrated to cloud deployments.

The Next Phase of Network and Security Monitoring and Protection

Network security monitoring has proven to be a huge challenge for many organizations in the data center and in the cloud. As noted previously, fundamental network security technologies such as firewalls and intrusion detection/prevention platforms have significantly lower adoption rates in the public cloud. While this may be partially due to lack of provider support for tried-and-true in-house network security technologies, security personnel face a number of challenges, one of which may be the lack of security planning for dynamic and hybrid workloads in private and public cloud environments. Only 32% of respondents have a formal cloud security strategy in place. Security of cloud-based data centers cannot be a chance occurrence.

Organizations must envision strategies and implement policies to ensure security of their internal and cloud-based assets, design a formal hybrid security strategy and operationalize it with a series of policies governing what can be stored on the cloud and in the data center, who has access to it and what technologies should be deployed. In addition, it is essential that organizations continually update strategies and policies to keep pace with evolving attacker strategies.

Lack of visibility, cited by 44% of respondents, is the primary hurdle in setting up network security in the cloud, followed by the lack of cloud provider support for security technology at 19% (see Figure 11).

TAKEAWAY:

Ensure that security controls and protection are applied unilaterally. Security should be in place regardless of whether the system runs internally or in the cloud, and the controls in use need to protect assets wherever they're located.

What has been your biggest challenge in setting up network security in the cloud?

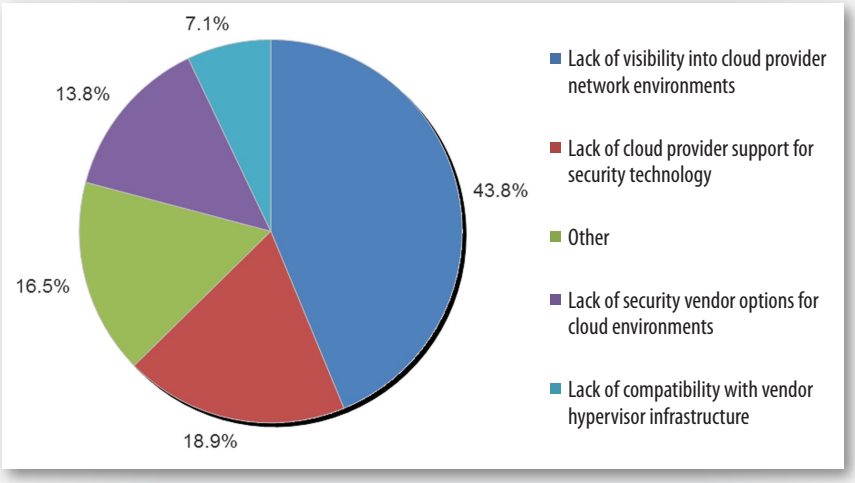


Figure 11. Cloud Network Security Monitoring Challenges

TAKEAWAY:

Visibility is a concern in the cloud and the data center. Investigate and implement tools and processes that improve visibility in your computing environments.

Other challenges include a lack of vendor options for cloud environments and a lack of virtual appliances that work with chosen cloud service provider hypervisors. SANS received a number of responses for the "other" option, including licensing challenges, operations delays, lack of management support, lack of funding, and a knowledge gap preventing expansion into new options.

But the challenges are not limited to the cloud. The SANS Data Center Security Survey[5] found visibility a concern in data centers as well. This suggests that tools and processes that can enhance visibility in cloud and data center environments should be a high priority for organizations.

[5] "Data Center Security Survey 2014, www.sans.org/reading-room/whitepapers/analyst/data-center-server-security-survey-2014-35567

EAST-WEST TRAFFIC
The traffic between applications, systems or VMs within both data center and cloud environments

While much has been said in the past several years about monitoring and protecting data moving from our data centers to cloud service provider environments, there is also a need to carefully monitor traffic between systems or virtual machines in both data center and cloud environments, commonly called *East-West traffic*. Currently, only 43% of survey respondents are monitoring East-West traffic in their data center and cloud environments, with 36% not monitoring this traffic and 21% unsure whether they are or not.

The finding that 21% don't know their monitoring status certainly speaks to confusion about the need to secure East-West traffic. If one in five respondents doesn't know his/her organization's own monitoring posture, certainly a problem exists that must be addressed.

For those that are currently monitoring East-West traffic, 69% use network IDS/IPS or malware analysis tools to accomplish this. The same percentage of respondents uses access control lists on routers and switches. Some enterprises are using East-West internal firewalls (53%), and 18% are using or considering software-defined networking (SDN) options. Some enterprises did not know how they were monitoring such traffic or were looking at host-based solutions to monitor activity. Unfortunately, these tools are static and unable to keep up with the pace of dynamic data centers. It's no surprise 35% of respondents revealed it takes more than two weeks to implement security change controls. Figure 12 illustrates the strategies respondents are using to secure East-West traffic.

TAKEAWAY:
Begin monitoring East-West traffic to enhance your data security. With the advent of dynamic, hybrid data centers and the increasing frequency of intrusions and data breaches, East-West monitoring should be done as close to the workload as possible, implying that monitoring on individual systems and virtual machines may make more sense both now and in the future.

What strategies do you use to segment applications and secure East-West traffic inside your data center?

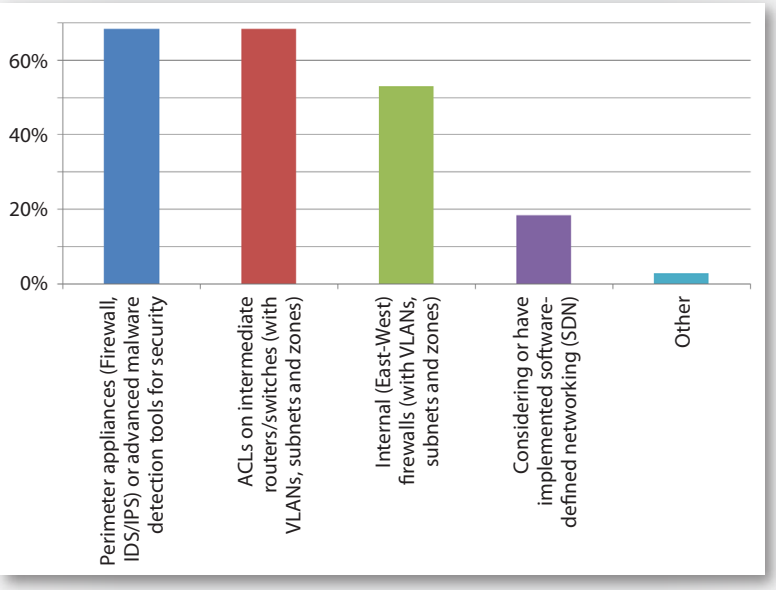


Figure 12. Strategies to Secure East-West Traffic

In addition to monitoring network traffic between internal environments and the cloud, as well as East-West traffic, encrypting traffic internally and between on-premises and cloud environments is key to actually protecting the data in transit. To accomplish this, 66% of respondents' organizations are currently using SSL technology, and 56% use IPSec, as shown in Figure 13.

What are you currently using to encrypt network connections between your data center (on-premises) resources or between your data center and cloud-based assets?

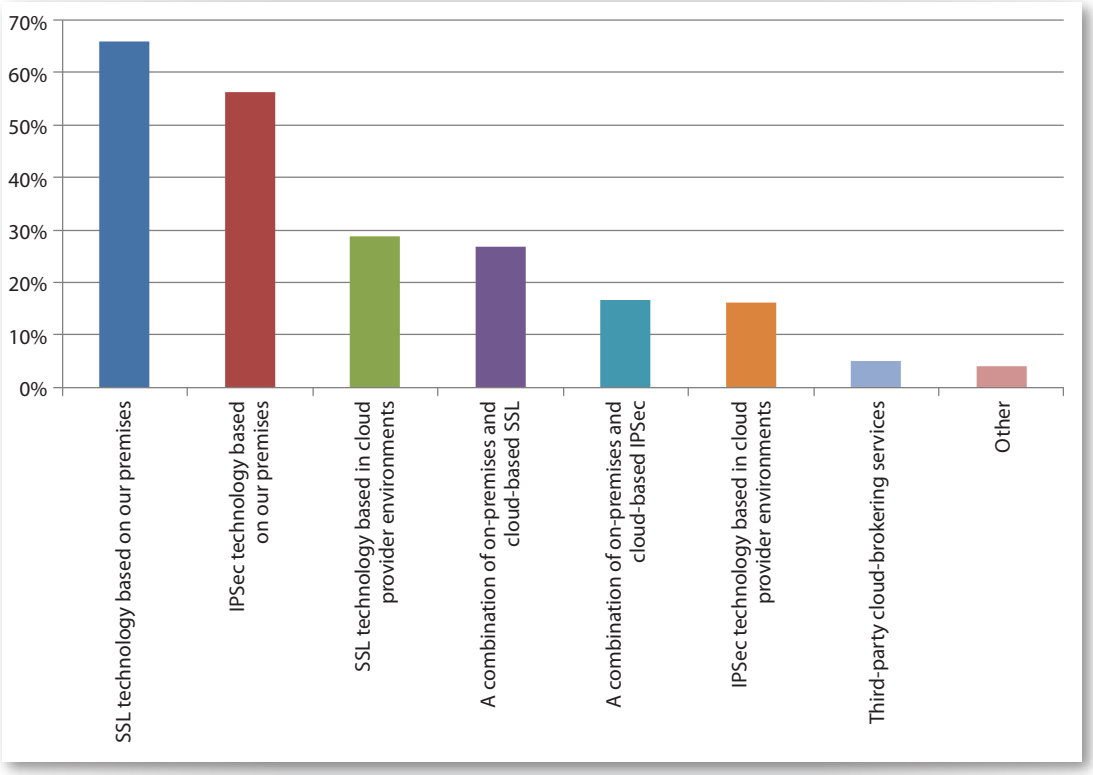


Figure 13. Network Encryption Technology in Use

Using on-premises encryption tools makes sense, because many organizations already have these in place and can continue to use them as they migrate to cloud service environments. SSL in the cloud provider environment is the third choice, selected by 29%, followed by hybrid SSL and IPSec strategies combining on-premises and cloud provider technology options, at 27% and 17%, respectively. Only 5% of respondents are using third-party brokering services.

Conclusion

Security teams need to do a lot of thinking to keep up with the rapid diversification of enterprise computing into a variety of private, public, cloud and traditional environments. They should re-evaluate their policies and priorities, and put significant effort into rethinking the types of policies, processes and tools they use to implement a sound security strategy. Teams that are ahead of the game have already developed strategies describing how traditional and cloud computing models fit together, typically outlining what data or other assets can go to which type of external provider and what conditions should be placed on providers of different types or security levels. They may even have researched and documented the types of controls and reviews needed to properly secure and monitor assets in each environment. Unfortunately, only 32% of respondents' organizations have thought that far ahead, and 20% don't know whether their organizations have such a strategy, which likely means they don't. That leaves almost 49% of respondents that acknowledge their organization does not have a strategy in place to define the mix of environments they are using and specify the security requirements for each.

Enterprise security has always revolved around—and stopped at—the perimeter of the network. But such controls don't cover the gap when users add SaaS services. It's obvious that we need a new way of approaching enterprise security, especially in light of the dynamic nature of workloads used across in-house data centers and cloud provider environments. Without the ability to implement security controls—such as network monitoring, application monitoring and control, data protection with encryption, and other technologies for both system-to-system and data center-to-cloud traffic flows—organizations leave themselves vulnerable to continued security incidents. IT operations and security teams should focus less on the network perimeter and more on the systems, applications and data in motion, with the goal of implementing security controls that can accommodate both in-house and cloud-based deployment scenarios whenever possible.

About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this survey's sponsor:

illumio