PROTECTING YOUR CLOUDS.

TABLE OF CONTENTS

About this report: This document has been prepared by CBS Interactive on behalf of Palo Alto Networks. Palo Alto Networks has specified topic, title and key themes of this report and may have contributed to and exercised editorial control over the content. This report may only be quoted and reproduced by Palo Alto Networks in its entirety.

MEET THE PARTICIPANTS

In February 2017, CBS Interactive's Tech Pro Research reached out via email to registered users of ZDNet and TechRepublic in the United States to engage them in a survey about their current cloud security operations and priorities.

ZDNet's breaking news, analysis, and research keeps business technology professionals in touch with the latest IT trends, while TechRepublic provides IT professionals with a unique blend of original content and peer-to-peer advice from the largest community of IT leaders on the Web.

After ensuring respondents' primary job function was in IT, the complete survey sample resulted in a data set of 515 responses.

As the following chart shows, nearly 80 percent of all respondents fell (almost evenly) into the following four categories: C-Level and executive management, endpoint (or desktop) support, network operations (as distinguished from security operations), and DevOps engineering.

Of those who identified themselves as C-Level or executive management, 29 percent self-identified as having the CIO title. Another 25 percent identified as CTO. The rest have a smattering of executive-related titles, including CISO, CSO, and COO.

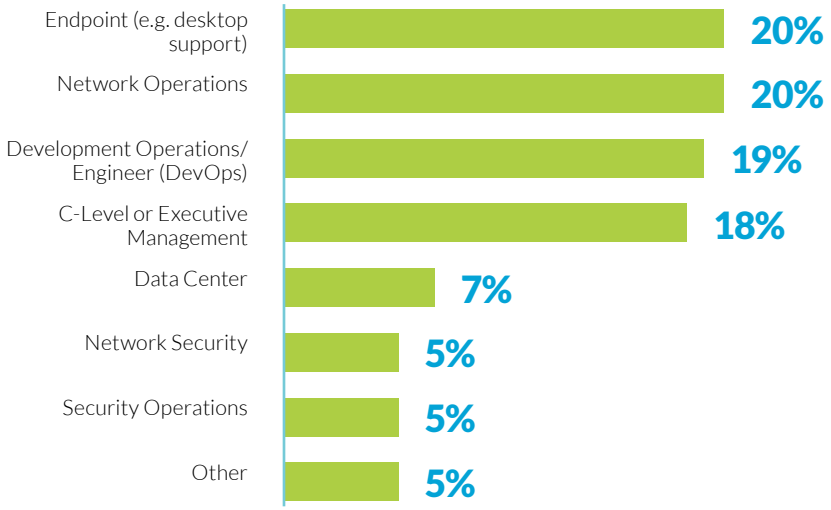
Of those IT professionals who reported having endpoint responsibilities, 44 percent listed themselves as desktop support analysts. Another 27 percent responded that they are managers of desktop support.

Network operations respondents are mostly hands-on IT professionals, with 25 percent listing themselves as system admins, and another 30 percent evenly split between network engineering and systems engineering.

In DevOps, 30 percent of the respondents are applications developers. Twenty-four percent identified themselves as applications engineers. Another 15 percent identified themselves as managers or directors of IT applications.

FIGURE 1: *RESPONDENTS BY JOB FUNCTION.*

In which of the following categories does your primary job function/role best fit?
Base: IT Primary Job Function



In network security, a third of the respondents identified themselves as either managers or directors of network security. Close to two-thirds identified as hands-on network security engineers, administrators, or specialists.

The demographics of our security operations respondents were similar, with about a third of the respondents being managers or directors of information security. The rest comprised an assortment of hands-on IT security-related titles.

Only ten percent responded that their primary responsibility was in either network security or security operations.

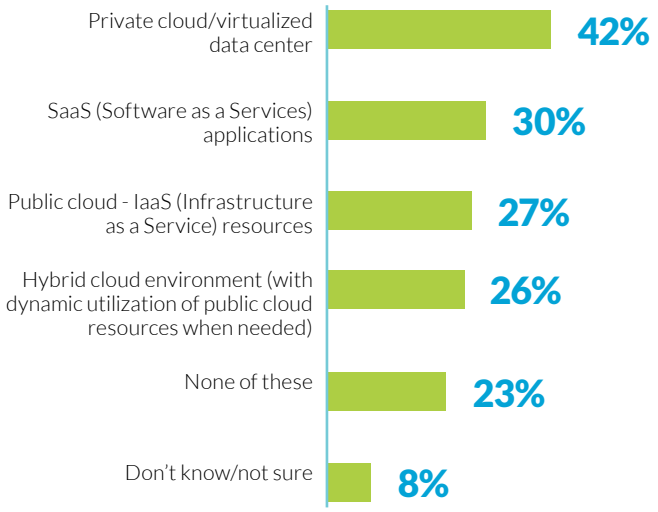
As the following chart shows, most of the respondents are already using cloud capabilities. Of note, however, is that while most respondents are using cloud capabilities, only 30 percent are using SaaS (software as a service) applications.

In terms of infrastructure, nearly half have implemented some form of private cloud/virtualized data center operation, while about half the respondents have implemented either public cloud infrastructure as a service (IaaS) or a hybrid cloud environment that utilizes public cloud resources dynamically and on-demand.

Given such a strong level of usage of cloud-related services, the following sections of this report will take a deep dive into private/hybrid cloud considerations, IaaS usage and preferences, and adoption and concerns of SaaS in IT operations.

FIGURE 2: *TYPE OF CLOUD TECHNOLOGIES IN USE.*

Does your organization use the following cloud capabilities? Select all that apply.
Base: IT Primary Job Function



PRIVATE/HYBRID CLOUD

Our first area of discussion with respondents was regarding their implementation of private and hybrid cloud infrastructure. The detailed findings are very interesting, but if you want some quick highlights, here are three key takeaways:

1. Insider threats are of the greatest concern to private/hybrid cloud users.

2. Multiple teams are involved in security control decisions, including network operations (74 percent), security operations (70 percent), and server operations (51 percent).

3. Virtual security appliances need to solve for concerns of manageability and complexity of integration for IT professionals to feel more comfortable implementing these solutions.

THREAT ELEMENTS OF HIGHEST CONCERN

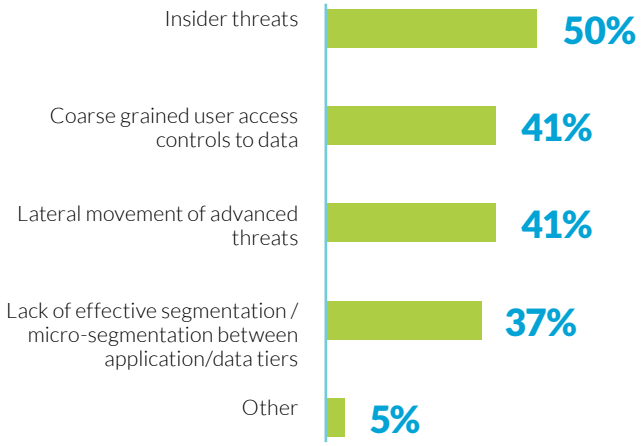
For any given corporate network, there are zones of concern: everything inside the network and everything outside. Movement of data between the internal network and the public Internet is often described as North-South. Movement of data laterally, within a supposedly secured corporate network, is often described as East-West.

Historically, the focus of IT security attention was on the gateway between the two zones, typically protected by a firewall. Anything inside the protective walls is considered to be trusted, and therefore considered friendly.

In this context, it's particularly interesting that nearly half of our IT pros indicated a concern over insider threats. In fact, the concern of insider threats was the highest-ranked. Insider threats, by definition, are threats that originate from inside the organization, threats that lay dormant on compromised hosts and become active once the hosts are within the enterprise network, and therefore not subject to security checks at the enterprise perimeter.

FIGURE 3: *TOP SECURITY CONCERNS FOR PRIVATE/ HYBRID ENVIRONMENTS.*

What are your top threat concerns within your data center/ private cloud? Select all that apply.
Base: Utilize Private or Hybrid Cloud



More than 40 percent indicated a concern about the lateral, or East-West, movement of malware. An identical percentage expressed a concern about data access controls not having enough granularity to ensure safety.

Since one of the most effective ways of protecting an internal network from compromised enterprise assets, is through the use of network and application segmentation, it comes as no surprise that more than a third of respondents indicated that they were worried about a lack of effective segmentation inside their networks.

HOW RESPONDENTS DECIDED TO EMPLOY PHYSICAL AND VIRTUAL FIREWALLS

Our respondents' concerns about lateral, East-West security is confirmed by their security practice. More than 75 percent of all respondents use a combination of both physical and virtual firewalls.

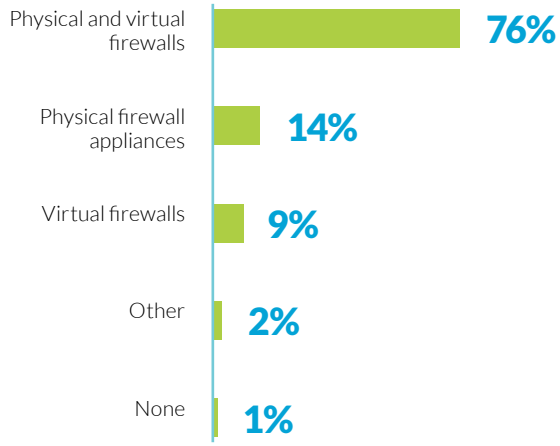
Physical firewalls, as previously mentioned, are most often used at the gateway between internal and external networks. Because of this, most physical firewalls provide very little visibility or protection over traffic that's traveling East-West within the local network or virtualized infrastructure.

While it's also possible to set up physical firewalls inside the network, management can be quite painful, because applications and business needs often change rapidly, and physical firewalls can take some time to set up and configure.

This is where virtual firewalls can really help out. Virtual firewalls, running on top of a software-defined network (SDN), offer excellent protection against both lateral malware propagation and rogue insiders. Additionally, virtual firewalls can be automated, spun up, taken down, and moved along with application workloads. As such, they offer a great way for the IT organization to be agile and flexible, while also being secure.

FIGURE 4: *PHYSICAL AND VIRTUAL FIREWALLS.*

What do you use to enforce security controls in your data center/private cloud? Select all that apply.
Base: Utilize Private or Hybrid Cloud



Of those respondents who use only one or the other, 14 percent use physical firewall appliances. Just under 10 percent indicated they only use virtual firewalls.

CHALLENGES FACING ADOPTION OF VIRTUAL SECURITY APPLIANCES

Survey participants acknowledged there are challenges when it comes to setting up and operating virtual security appliances.

Without a doubt, the most resounding response was the challenge of managing and integrating virtual security appliances. More than half of our respondents indicated manageability (58 percent) and complexity of integration (57 percent) are key challenges.

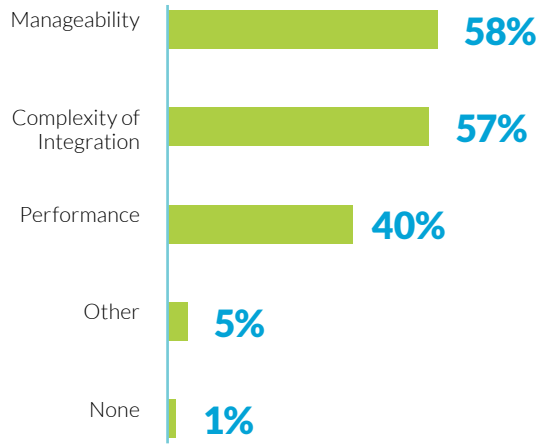
This is where single-pane user management tools, like Panorama from Palo Alto Networks, come in handy. Panorama provides for easier management of next-generation firewalls, including physical firewalls at the network edge and virtual firewalls inside the virtual infrastructure.

Panorama uses rules and policy updates to reduce the overall workload of IT administrators and provides increased visibility and control into network security infrastructure. Panorama allows firewall policies to be pushed from the physical to the virtual world without having to recode or recreate all the details of a policy implementation for each VM. This can save enormous time.

A smaller group (40 percent) was concerned about the performance impact of security appliances on the overall network operation. Of the remaining five percent, "cost," "financing," and "money" were often cited, along with the challenge of training IT pros on the newer security paradigms that are available as a result of software-defined networking.

FIGURE 5: *CHALLENGES TO DEPLOYING VIRTUAL SECURITY APPLIANCES.*

What is your biggest challenge in deploying virtual security appliances within your data center/private cloud? (pick up to 2)
Base: Utilize Private or Hybrid Cloud



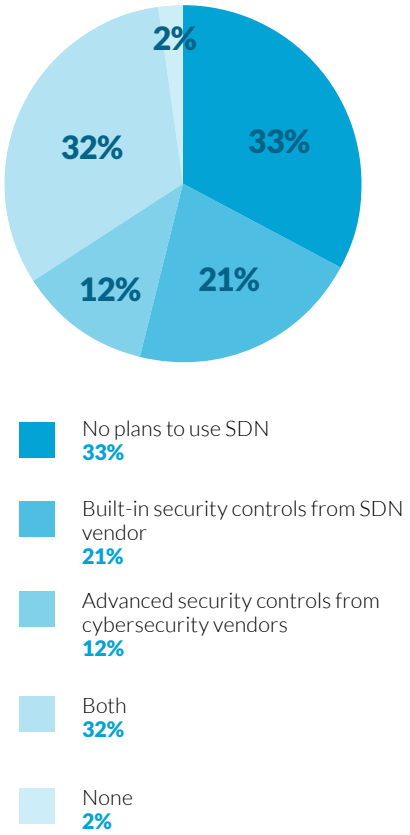
SECURITY MANAGEMENT

We were curious about what security controls were used when a SDN has been deployed. Of our respondents who indicated they're currently operating a SDN, 20 percent indicated that they simply use the controls provided by the SDN vendor.

More of our respondents indicated a desire to increase their security controls; almost a third indicated that they use both the controls that come built-in from the SDN vendor paired with advanced security controls provided by third-party cybersecurity vendors. Another 12 percent indicated they solely use third-party cybersecurity vendors.

FIGURE 6: *SECURITY IN SDN ENVIRONMENTS.*

What security controls do you use / plan to use within your private cloud? Select all that apply.
Base: Utilize Private or Hybrid Cloud with no Plans to Use SDN



A third of our respondents indicated they had no plans to implement a SDN in their private cloud environment. Of those respondents, 70 percent instead indicated the use of virtual firewalls, and another 70 percent indicated the use of physical firewalls. The overlap indicates that many are using both physical and virtual firewalls in their operation.

Splitting security management across different vendor solutions can be challenging. For those who have chosen to implement a hybrid cloud strategy, the message is resounding: A uniform security posture is mandatory. Almost two-thirds of our respondents indicated that they want to enforce a uniform security posture across cloud solutions.

Only 12 percent indicated that they plan to use different security vendors across their data center and public cloud. Of those, several respondents explained that for their unique implementations, a single-vendor solution wasn't available for situations where they manage infrastructure across different industries with different requirements, or for integrations that just don't support uniform solutions.

Palo Alto Networks has built a natively integrated platform for security in the network (on-prem or in the cloud), within the SaaS and at the endpoint. All deployment scenarios are supported by the platform, and with a single user management tool, a uniform security posture can be achieved.

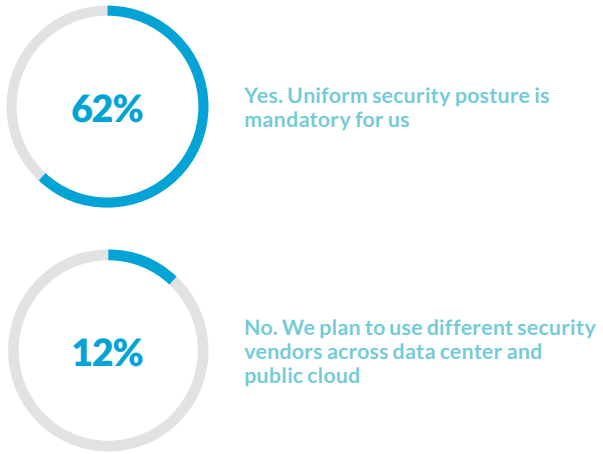
The careful reader will notice that we've only accounted for about three-quarters of our respondents in this discussion. That's because nearly a quarter indicated they don't know whether a uniform security posture is a must for their organization. Clearly, for these IT pros, an overall cloud security strategy is still a work in progress.

When it comes to implementing security controls within their data centers or private clouds, survey respondents indicated that visibility (40 percent) and regulatory compliance (34 percent) were key motivators. The issue of lateral movement of attacks showed up in this answer, as well. A quarter of the respondents were concerned about the risk of a breach inside the perimeter due to the lateral movement of attacks.

Two of our respondents summed up adoption drivers quite succinctly. One said "Simply protecting our data" was of paramount importance while another gave a one-word answer: "Paranoia."

FIGURE 7: *UNIFORM SECURITY ACROSS ON-PREM AND OFF.*

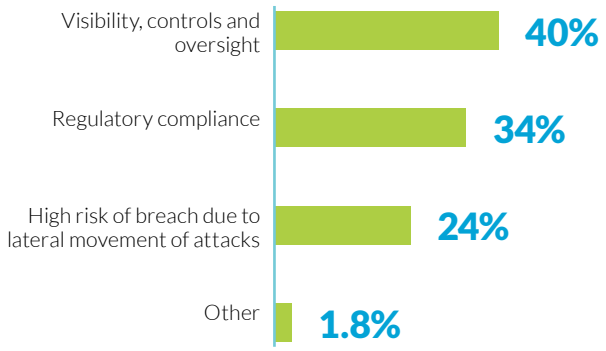
You mentioned utilizing a hybrid cloud strategy (on premises data center and public cloud), are you looking to enforce a uniform security posture across the clouds?
Base: Utilize Hybrid Cloud



Other responses: Other 5%, Don't know 22%

FIGURE 8: *DRIVERS OF SECURITY FOR PRIVATE/HYBRID USERS.*

What is the top driver for implementing network security controls within your data center/private cloud?
Base: Utilize Private or Hybrid Cloud



INFRASTRUCTURE AS A SERVICE (IAAS)

Our next area of exploration involved moving physical infrastructure to the cloud. Here are two takeaways from our study:

1. IaaS is poised for growth in the next 12 months.

2. IT managers are still running behind when it comes to cloud security implementations.

INFRASTRUCTURE MIGRATION TO THE CLOUD

From an accounting and cost-management point of view, there's a considerable benefit in moving expenses from the capital expense (CAPEX) category, which must be amortized over years, to the operational expense (OPEX) category, which can be expensed on a year-by-year basis.

The CAPEX to OPEX tax benefits mirror the real operational benefits of infrastructure as a service (IaaS): agility and flexibility. Growth in infrastructure can mirror demand dynamically, instead of either being overbuilt in anticipation of growth, or lagging behind growth due to the natural delays in the procurement, shipping, and installation of hardware.

Expenses are also gradual and predictable, rather than chunky. Instead of suddenly running out of capacity, requiring a substantial purchase for a large addition in capacity, IaaS allows metered capacity that tracks with the rate of growth.

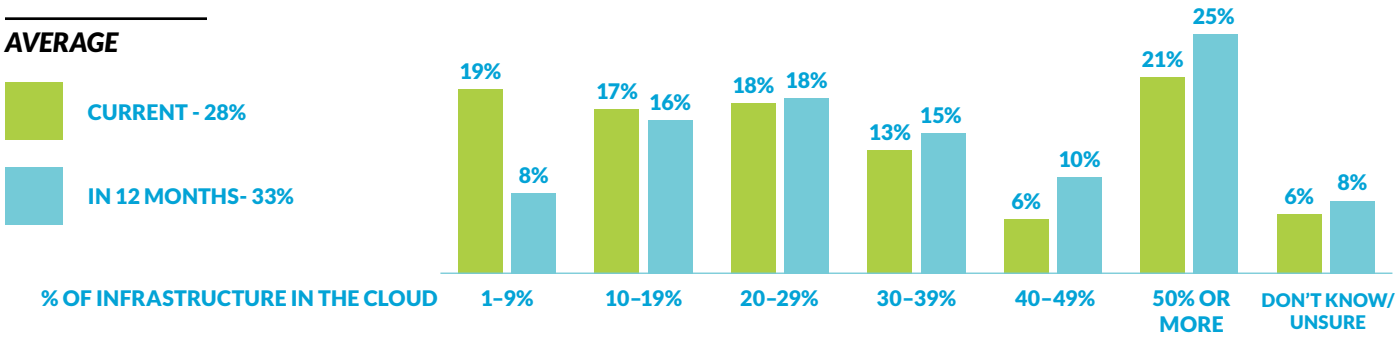
It is for these reasons we see considerable movement of infrastructure to the cloud. If we look at infrastructure cloud migration among respondents today, we see an interesting pattern: Organizations have either moved a lot to the cloud or relatively little. This is reinforced by the fact that of our respondents, nearly two thirds have migrated less than 30 percent of their infrastructure to the cloud.

By contrast, less than 20 percent have migrated 30-50 percent of their infrastructure to the cloud. At the

FIGURE 9: *IAAS GROWTH EXPECTATIONS.*

What percentage of your infrastructure have you moved the cloud?
Base: Utilize IaaS

What will that percentage be in the next 12 months?
Base: Utilize IaaS and know current percentage of infrastructure in the cloud.



high end of the spectrum, more than 20 percent of our respondents have already migrated more than 50 percent of their infrastructure to the cloud.

That accounts for current status. A quarter of our respondents expect to have more than half of their infrastructure in the cloud within the next year. We also see a jump in growth for those who expect migration to progress, the 30-50 percent migrated group, where another 25 percent of respondents expect to see reach the 30-50 percent mark within 12 months.

Across the full spectrum of respondents, an average 28 percent of infrastructure usage is happening in the cloud. That's expected to grow to 33 percent within a year.

CLOUD INFRASTRUCTURE VENDORS

When it comes to choosing a public cloud IaaS provider, our respondents reflected similar percentages to the market penetration numbers that have been reported in ZDNet and TechRepublic.

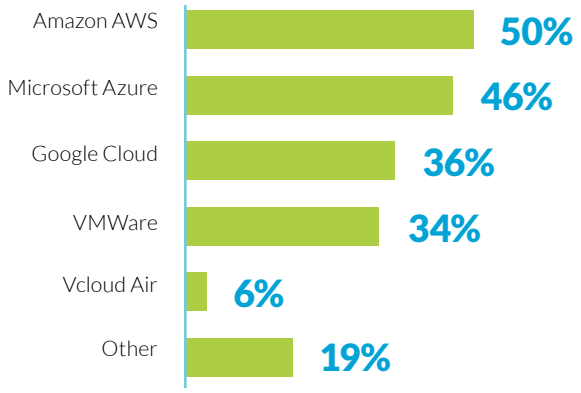
Amazon leads among our respondents, with 50 percent stating they're using AWS. Microsoft Azure follows closely, with 46 percent. Another 36 percent say they're using Google's cloud offerings. In addition, VMware and Vcloud Air together are used by 40 percent of our respondents.

The results indicate that a good percentage of our respondents are using more than one public cloud IaaS provider. From a disaster recovery and business continuity perspective, using multiple cloud providers is a wise choice. Multi-cloud does increase management complexity, though. This may shed light on our previous observation that nearly two-thirds of our respondents want a uniform security posture across all cloud implementations. Managing a variety of services via disparate interfaces can get old, fast.

This is where security vendors that offer both on-premise and cloud infrastructure solutions can provide substantial value. If you choose vendors that provide *natively integrated security* and the management thereof, to implement across your entire hybrid stack, you can reduce your overhead, costs, and complexity considerably.

FIGURE 10: *CLOUD VENDORS IN USE.*

Which environments are in use? Select all that apply.
Base: Utilize IaaS



SECURITY STRATEGIES FOR IAAS DEPLOYMENTS

When it comes to security in public cloud deployments, our respondents clearly leaned one of two ways: relying on the cloud provider to provide security or extending in-house security measures to the cloud.

Less than a fifth of our respondents indicated they were going to use a third-party security provider. This indicates an important need for IT managers to come up to speed on the options available to them in added security services. Third party security managers are able to do something that neither in-house, on-premises security, or cloud-based security services can do: span the entire hybrid network and allow for comprehensive, big-picture, single-pane management.

It's important to keep in mind that services like AWS and Azure may offer limited protections, but they provide resources, not policing. This is a very important distinction. Cloud-based infrastructure providers provide infrastructure. They give you the storage, computing, and communications capabilities you need on a metered basis. They will also offer rudimentary security, but ultimately the responsibility

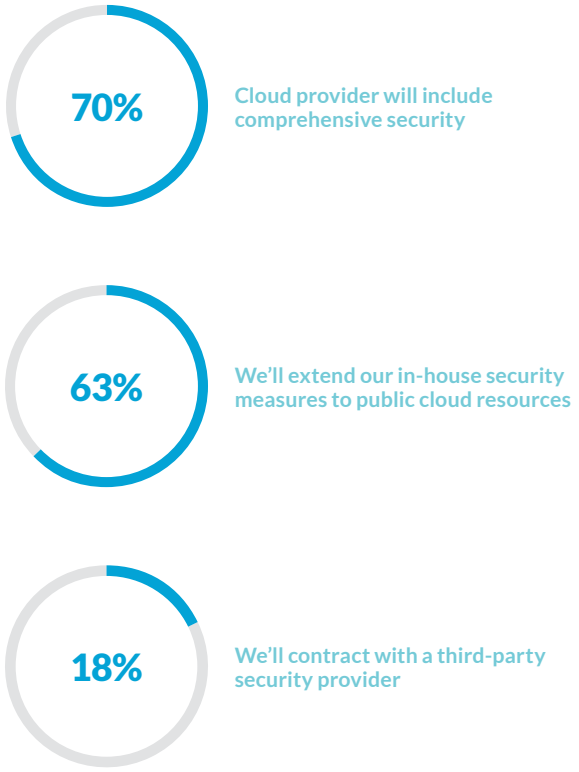
to secure your apps and data falls to you.

Amazon and other cloud providers will not make your security their number-one priority. In fact, if you misconfigure something, that responsibility falls on you. If you want your AWS and other cloud infrastructure secured, it is essential that you bring in dedicated security professionals and dedicated physical and virtual security infrastructure.

It's only by combining services like AWS with *next-generation security technologies*, that will enable your organization to prevent cyber breaches.
Given that 70 percent of our respondents indicated they expected to use security services provided by the cloud providers, while nearly 70 percent also indicated they were using in-house security measures, it's clear that many of our IT pros were employing a belt-and-suspenders approach utilizing a combination of the two strategies.

FIGURE 11: *PUBLIC CLOUD SECURITY EXPECTATIONS.*

What are your expectations around public cloud security? Select all that apply.
Base: Utilize IaaS



SOFTWARE AS A SERVICE (SAAS)

Our final deep dive was in cloud-based SaaS applications. There are four main takeaways from our research in this area:

1. IT professionals estimate an average of 14 percent of SaaS apps in their organizations are unsanctioned - meaning, do not have IT security oversight.

2. Data leakage is the top security concern with SaaS.

3. Next-generation firewalls are the leading measure IT is using to control unsanctioned apps.

4. About a third of our IT professionals consider a CASB (Cloud Access Security Broker) as a potential solution to their SaaS data security concerns.

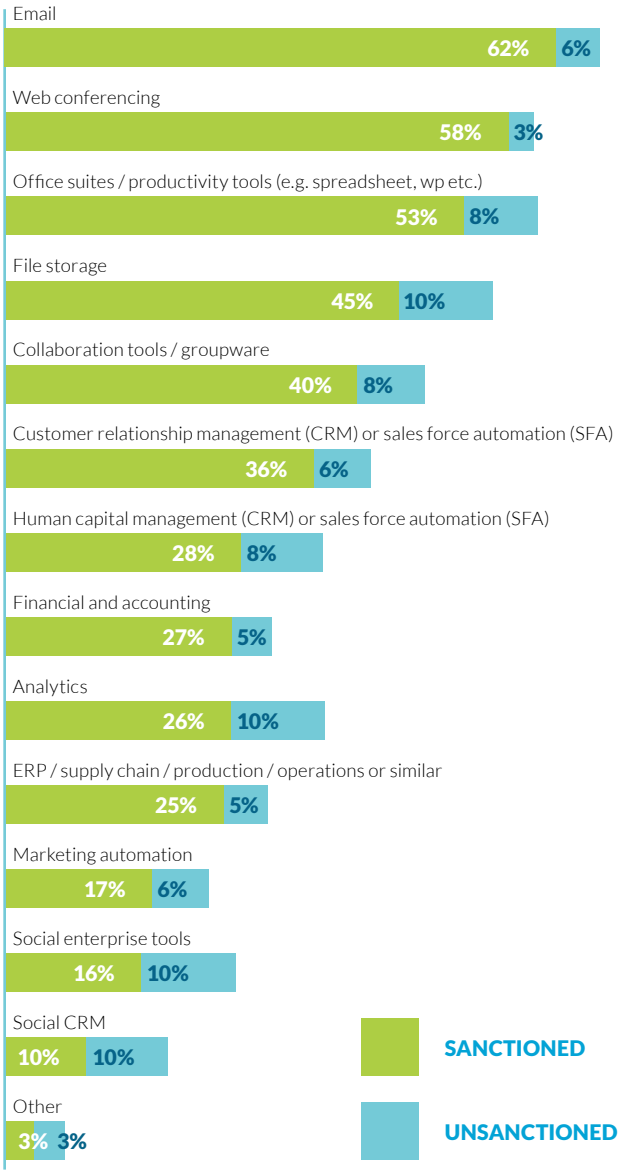
UNDERSTANDING SAAS APPLICATION USAGE

The following chart provides a wealth of information about application usage within our respondent organizations. Clearly, cloud-based email is the winner, with two thirds of our respondents reporting adoption. Following close behind are web conferencing, cloud-based office apps, file storage, and groupware or collaboration tools.

FIGURE 12: *SAAS APPLICATIONS IN USE.*

Which of the following SaaS capabilities does your organization use? Please select all that apply.

Which of the SaaS applications are allowed (Sanctioned) by IT?
Base: Utilize SaaS



UNDERSTANDING IT VS. EMPLOYEE-DRIVEN APPLICATION ADOPTION

One thing to notice is the distinction between "sanctioned" and "unsanctioned" applications. We'll discuss this in depth throughout this section.

Put simply, sanctioned apps are applications that are implemented and managed by the IT professionals of the organization. Security controls are often integrated into the organization's security posture, as are the establishment and management of user accounts and federated sign-on.

Unsanctioned apps are used by employees without IT's direct management, support, or approval. In some companies, there isn't even a defined policy where SaaS fits into the IT operation or how employees can make use of the public SaaS services available.

The motivation for using unsanctioned apps is obvious: They get the job done. Many employees are very mission-focused. If the IT department implementations are too slow compared to the speed of innovation required by line of business employees, those employees often route around the more formal infrastructure to find their own solutions, essentially creating their own "shadow IT" operations outside of standard channels.

This is where cloud is both a challenge and a benefit to IT organizations. Because cloud services are so easy to adopt (all it usually takes is an email address and a valid credit card), employees can set up their own services without needing to involve IT. Sometimes, public SaaS applications need access to private corporate information contained in email or other SaaS applications. What happens is that public SaaS applications are often granted some form of access to what should be gated information, often through an API or other form of access key. Clearly, public SaaS access to confidential data can provide a security failure point if not managed correctly.

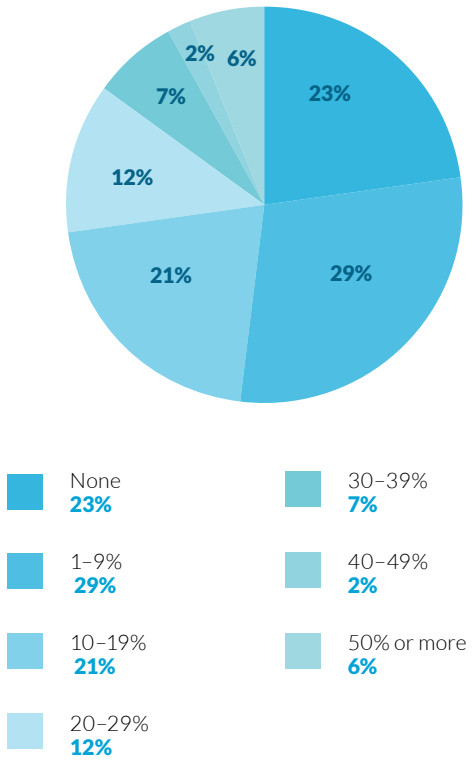
This, of course, makes managing and securing what may be confidential or regulated organizational data difficult for the IT professionals tasked with keeping the organization and employees safe.

On the other hand, that same quick sign-up that makes cloud services so easy for employees to adopt on their own makes it easy for IT operations to embrace and extend SaaS services, bringing them in as part of the overall IT strategy. Cloud-based SaaS applications are often nearly turnkey at the enterprise level, as well as at the individual user level.

While shadow IT does exist within most organizations, our respondents have indicated they believe there to be a relatively small percentage of unsanctioned applications in their organizations. In fact, our respondents indicated that they thought that less than 15 percent of the SaaS applications in use are unsanctioned.

FIGURE 13: *AVERAGE PERCENTAGE OF SHADOW IT.*

What percentage of SaaS applications being used in your organization would you estimate are unsanctioned (e.g. Shadow IT)?
Base: Utilize SaaS



This relatively low figure is unlikely to be accurate. Instead it reflects what may be a systemic lack of awareness as to the extent in which shadow IT services have been installed in their organizations. For those companies without a central management structure that can track and secure shadow IT, any employee may have turned to an external service and the IT management organization has no way of finding out. This, obviously, is a serious security concern. Identification of shadow IT can be accomplished, however, with next-generation with tools, like *App-ID*. *App-ID* scans and identifies all traffic and apps traversing the network, weeding out unauthorized activity or suspicious traffic behavior, so the IT team enjoys end-to-end visibility.

Microsoft's Office 365 is the clear winner in terms of SaaS implementations both among our respondents and in the broader market. Google follows at a distant second. This makes a degree of intuitive sense. Given that nearly three-quarters of our respondents have already implemented either a hybrid cloud (26 percent) or a private cloud/virtual data center (42 percent), Microsoft's unique ability to provide its applications both on-premises and in the cloud (with a coherent security and authentication strategy between the two) has a great appeal to organizations spanning both on-premises and cloud solutions.

The only pure cloud play that beats adoption of other vendors' sanctioned apps is Salesforce, which takes a commanding (69 percent) lead over all other contenders.

PROTECTING AGAINST SECURITY THREATS

While the use of unsanctioned applications can often indicate the presence of a motivated and proactive workforce, there are many security implications for shadow IT.

This is particularly the case with file-sharing applications. ZDNet has run numerous articles describing how files placed on public file sharing services resulted in confidential, proprietary, and regulated information getting out onto the Internet at large.

FIGURE 14: *SAAS PROVIDERS.*

Please provide the names of the applications sanctioned for use by IT?
Base: Utilize SaaS Answering

Office Suites / Productivity tools:

MICROSOFT	84%
GOOGLE	28%
OTHER	2%

Collaboration:

MICROSOFT	43%
GOOGLE	17%
SLACK	9%
ATLASSIAN	9%
OTHER	49%

Web Conf:

WEBEX	39%
MICROSOFT/SKYPE	31%
GOOGLE	12%
WEBEX	39%
GOTO MEETING	10%
OTHER	30%

Email:

MICROSOFT	39%
GOOGLE	31%
OTHER	12%

File Storage:

ONE DRIVE MICROSOFT	51%
GOOGLE	26%
DROPBOX	12%
OTHER	28%

CRM/SFA:

SALESFORCE	69%
OTHER	38%

This concern is clearly confirmed by our respondents, with nearly 40 percent expressing data leakage as their top concern.

Reflecting answers discussed previously, insider threats and malware were also considered serious security concerns. Seventeen percent of our respondents said they were quite concerned with how identity management will be handled in this brave new world.

In addition to getting ahead of unsanctioned app usage by quickly adopting and integrating cloud services, IT operations also need to protect their organizations, customers, clients, and employees against the security risks that come with unsanctioned and unsupervised app usage.

According to our respondents, the clear leader in this area is the use of next-generation firewalls, which allow for a wide variety of protections including deep packet inspection and blocking of files to and from certain applications and sites.

Next-generation firewalls are often smarter and provide a much greater degree of configurability than legacy firewalls. This lets IT executives allow sites to be reached under certain sanctioned circumstances, while blocking transmissions from actions that indicate the possibility of unsafe behavior.

In fact, about a third of our respondents reported that they're currently decrypting and inspecting traffic to and from SaaS applications today.

About one in five of our respondents have indicated that they've specifically implemented a Cloud Access Security Broker (CASB). CASB software is a category of product that consolidates cloud security and access processes, essentially filling in the security gaps between on-premises networks and multiple cloud solutions. CASBs can be implemented in a variety of ways, some of which may impose additional friction in the user experience. But by combining CASB solutions with next-generation firewalls, organizations can increase security, better integrate disparate cloud applications, and still preserve a quality user experience.

While CASBs are not attached to most of our respondents' networks today, about a third of our IT professionals indicated they plan to add CASBs in the future.

FIGURE 15: *SAAS SECURITY CONCERNS.*

What is your main security concern with SaaS applications?
Base: Utilize SaaS

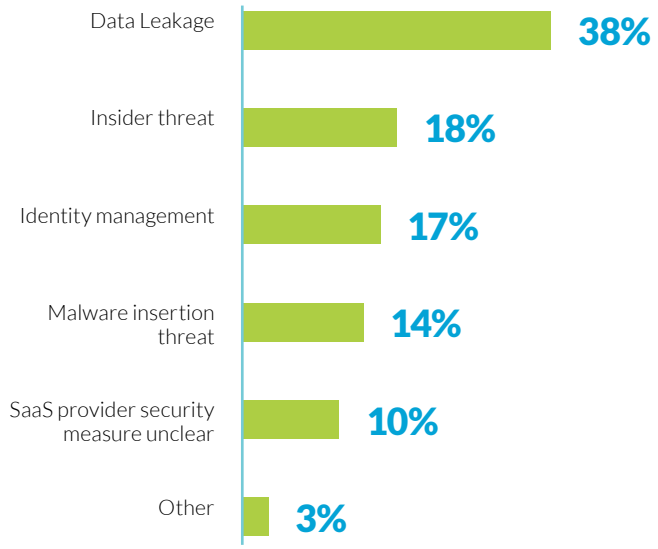


FIGURE 16: *MEASURES FOR CONTROLLING SHADOW IT.*

What steps do you take to control use of unsanctioned SaaS applications?
Base: Utilize SaaS

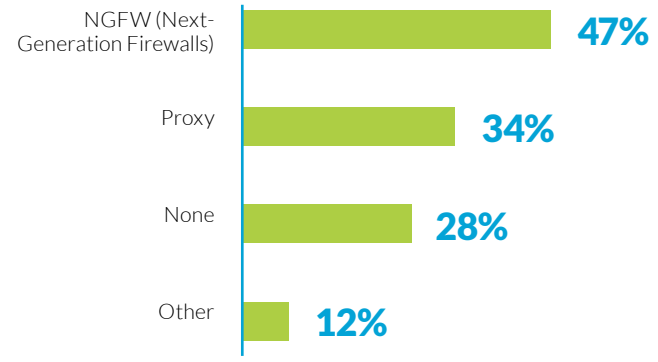
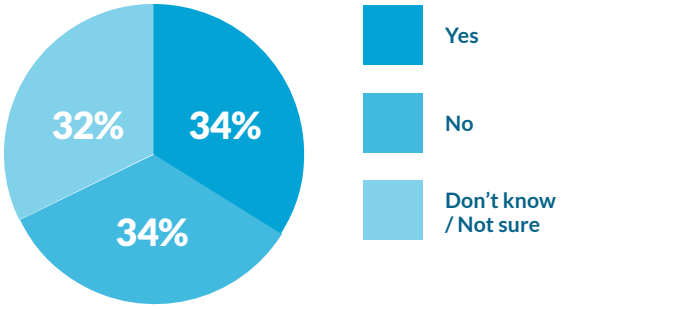


FIGURE 17: *PLANS FOR CASB ADOPTION.*

Do you decrypt connections to SaaS applications today?
Base: Utilize SaaS



Do you have a Cloud Access Security Broker (CASB) today to secure SaaS?
Base: Utilize SaaS

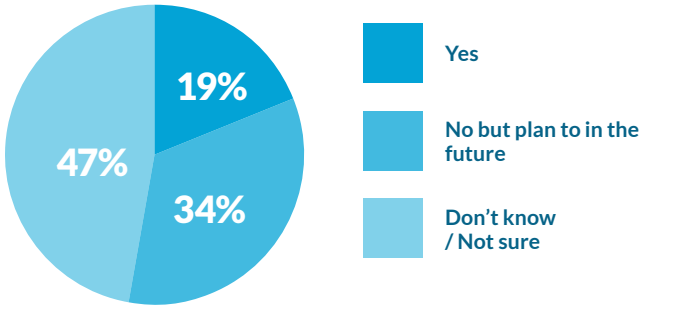
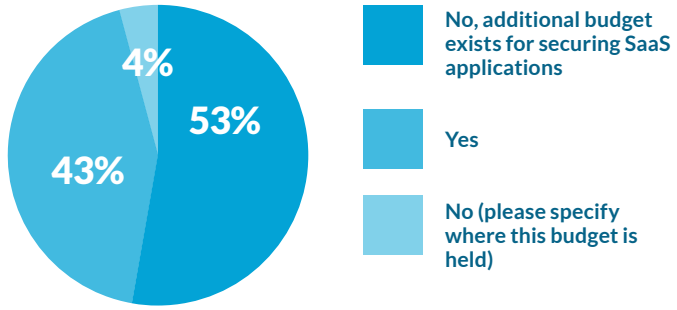


FIGURE 18: *BUDGET ALLOCATIONS FOR SAAS SECURITY.*

Is the budget for securing applications part of your organization's IT budget?
Base: Utilize SaaS



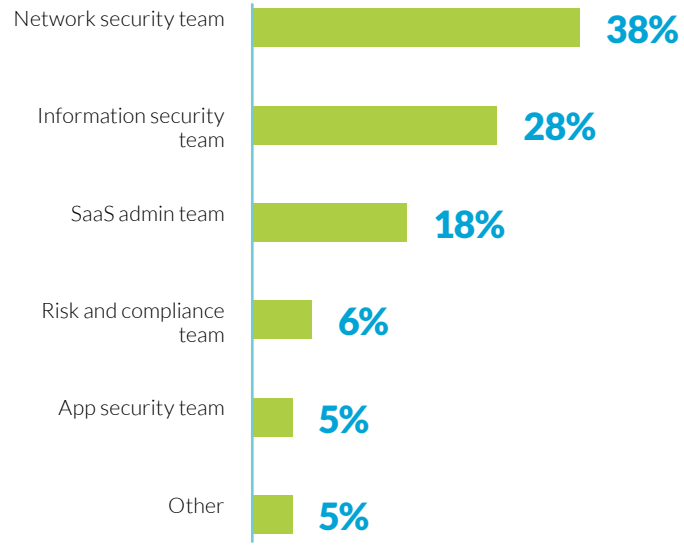
MANAGING THE SECURITY OF SAAS APPLICATIONS AND CORPORATE DATA

About half of our respondents are either relying on their existing security budgets, or the resources of their SaaS providers, to keep their SaaS users secure. On the other hand, 40 percent say they have budget dollars specifically allocated for securing SaaS applications.

Finally, we wanted to see if there was any change in responsible security roles when it comes to protecting SaaS applications. The lion's share of responsibility falls to network and IT security teams, although nearly 20 percent indicated that they have a specific SaaS administration team to administer security tools for SaaS applications. It's important to note that the best approach is for information security, networking security, and SaaS admins to work together to guarantee that sensitive corporate data remains protected regardless of its location.

FIGURE 19: *WHO'S IN CHARGE OF SAAS SECURITY?*

What team primarily administers security tools for the SaaS you utilize?
Base: Utilize SaaS



CONCLUSION

Our survey indicates that responsibility for security is often shared among groups, money for security is tight but available, and there is an increased concern over lateral threats originating inside the network. As infrastructure extends to include cloud services, companies must gain a better understanding of how to apply uniform security measures across all of their IT architecture.

While it's often difficult for senior management (particularly those outside the IT organization) to see how additional expenditures on security can benefit the bottom line, the reality is that the cost of insufficient security can be astronomical.

Expanding security across an entire hybrid infrastructure and building out systems to manage that security in a cohesive, centralized, and efficient manner will become key to protecting organizations both from outside penetration and internal threats.

But it's not enough to merely implement a robust security solution. Infrastructure security needs to be flexible enough to accommodate changing needs and threat vectors while also remaining strong. It also has to be easy enough to implement so that IT personnel keep it in force, rather than route around it to simply get the job done.

By using a combination of centralized management, monitoring, virtual next-generation firewalls and automation; modern security platforms can offer both protection and agility, and do so while freeing up IT professionals to focus on business-driving growth opportunities.

The Palo Alto Networks® Next-Generation Security Platform was built from the ground up for breach prevention, with threat information shared across security functions system-wide, and designed to operate in increasingly mobile, modern networks. By combining network, endpoint and cloud security with advanced threat intelligence in a natively integrated security platform, Palo Alto Networks safely enables all applications and delivers highly automated, preventive protection against cyber breaches at every stage of the attack lifecycle without compromising performance.

To learn more about Palo Alto Networks® Next-Generation Security Platform for cloud, visit *go.paloaltonetworks.com/secureclouds*.

