KEY PRINCIPLES AND STRATEGIES FOR SECURING THE ENTERPRISE CLOUD

A Cloud Security Blueprint

EXECUTIVE SUMMARY

Organizations are increasingly deploying a variety of workloads across multiple clouds. In turn, business-critical data and services are increasingly scattered across this distributed infrastructure. Using the shared responsibility model as a guiding principle, enterprises rely on cloud providers to protect the network, storage, and computing layers, while enterprises (end-users) own the security for everything that is built, deployed, or stored in the cloud. Due to multi-cloud adoption, most enterprises maintain heterogenous environments, with tools from each cloud platform differing significantly.

For organizations, this results in a complex, nonuniform network security infrastructure. The only viable answer is a unified security solution that runs across multiple cloud platforms. Organizations seeking to deploy applications in the cloud must deploy security solutions that embody three key attributes: 1) native integration with all major cloud providers, 2) a broad suite of security tools to cover the entire attack surface, and 3) the ability to centrally manage the security infrastructure as well as automate security operations. These must offer unified visibility and control and policy management that supports risk management and compliance requirements. The corresponding security architecture must support a wide variety of security use cases for various cloud deployments.

Enterprises use an average of **61** different cloud apps, which are 1/3 of their total applications.[1]

WHITE PAPER

Digital transformation (DX) is fueling unprecedented growth in cloud adoption, and many organizations have an increasing amount of business processing in the cloud. The heterogeneity of the resulting cloud environments expands the overall attack surface. This, in turn, makes it more and more difficult to protect cloud deployments. And even though public trust in the cloud has increased dramatically over the past decade, security remains one of the top concerns of business and technology leaders when it comes to cloud adoption. Thus, it is critical that security is an integral part of the design process for any cloud solution and for an organization's overall cloud infrastructure.

THE CLOUD SHARED RESPONSIBILITY MODEL

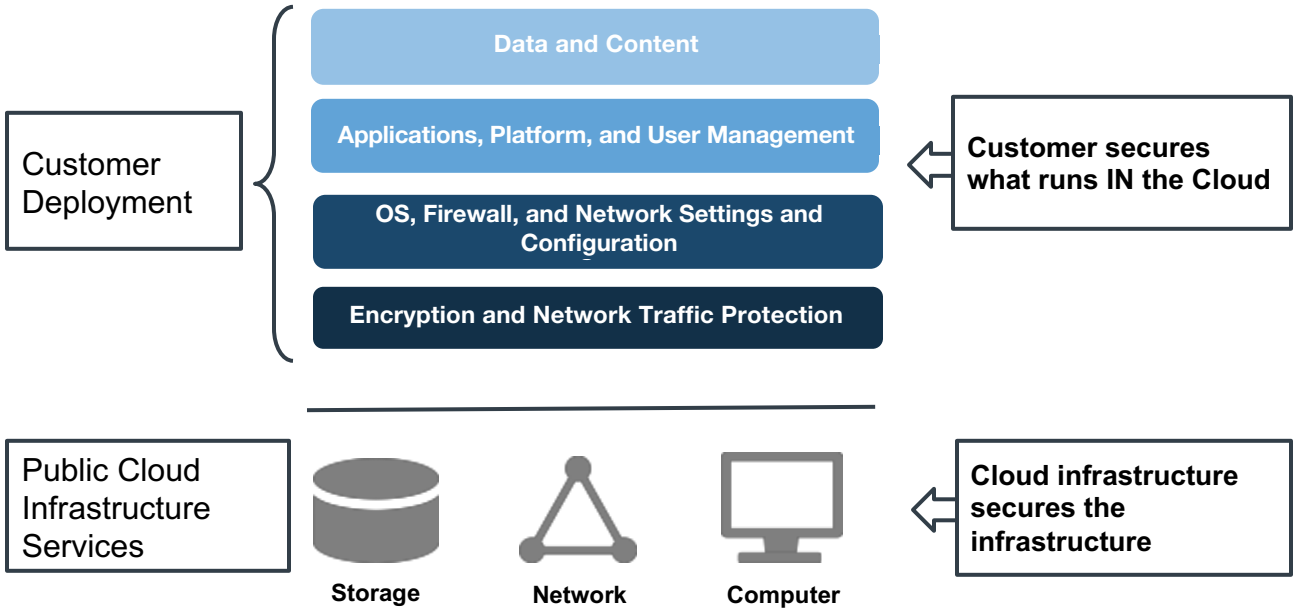
Cloud providers go to extensive lengths to protect their infrastructure. Protection of data and applications hosted or deployed in the cloud, however, is the responsibility of the customer (end-user). Yet, customers are falling short in upholding their responsibility, with projections that they will be responsible for 99% of cloud failures by 2023. This is the result of human error in many cases, which can be attributed to a misunderstanding of the shared responsibility model between cloud providers and their customers.[2]

The shared responsibility model is described frequently with an analogy of the OSI layers model. Here, cloud providers protect the lower physical layers, while customers must protect the layers above those. Nonetheless, the OSI layers model is not always sufficient to describe the complex relationship and responsibilities of cloud security. For example, customers may create overlay networks on top of a cloud provider network or build other abstraction layers that assemble services on top of the cloud's infrastructure. Despite these nuances, customers are responsible for securing anything it adds to a cloud infrastructure, and anything they manage within that cloud environment. Furthermore, customers are now required to secure the API/cloud management layer, as much of the cloud-related operation is performed via this interface.

A COMPLEX ARRAY OF SECURITY APPROACHES

While there are small differences in how the shared responsibility model is represented between different cloud providers, the biggest distinction is in how native cloud security capabilities are implemented and managed. Often different cloud providers accomplish the same security services using very different tooling and approaches. For example, Amazon Web Services (AWS) extends security policies based on security groups that are associated with cloud resources, whereas the Google Cloud Platform (GCP) uses firewall rules that offer equivalent functionality but are managed through different interfaces. Many of these differences stem from the unique way that each cloud's underlying architecture is structured and differing philosophies involving cloud operations.

For customers operating in multiple clouds, the default state of security is a heterogenous architecture with no central visibility or control and thus no consistency in how security is enforced and managed. In this context, each public and private cloud—as well as the on-premises data center—becomes an independent silo in a fragmented network security infrastructure.



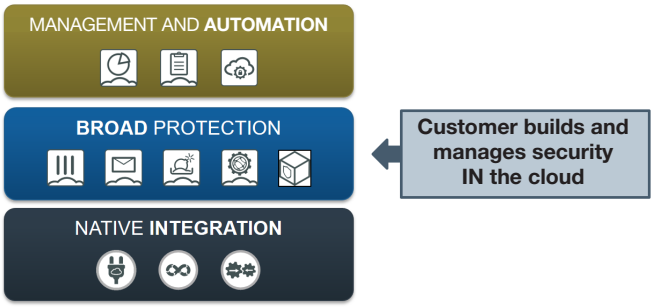
THE CUSTOMER AND THE CLOUD PROVIDER ARE RESPONSIBLE FOR SECURING DIFFERENT RESOURCES.

ESSENTIAL ELEMENTS IN A COMPREHENSIVE SOLUTION

Regardless of the types of cloud services an organization utilizes and how they are structured, keeping network security management heterogenous and disjointed increases risk. It requires more skills and, in turn, staff time to manage the different platforms. It also complicates compliance reporting and companywide communications of threat intelligence.

Instead, today's threat landscape requires a consistent and unified approach to cloud security. There are three critical elements for an effective multi-cloud security solution:

- Native integration
- Broad protection
- Management and automation



THERE ARE THREE CRITICAL ELEMENTS FOR AN EFFECTIVE SECURITY SOLUTION.

1. NATIVE INTEGRATION

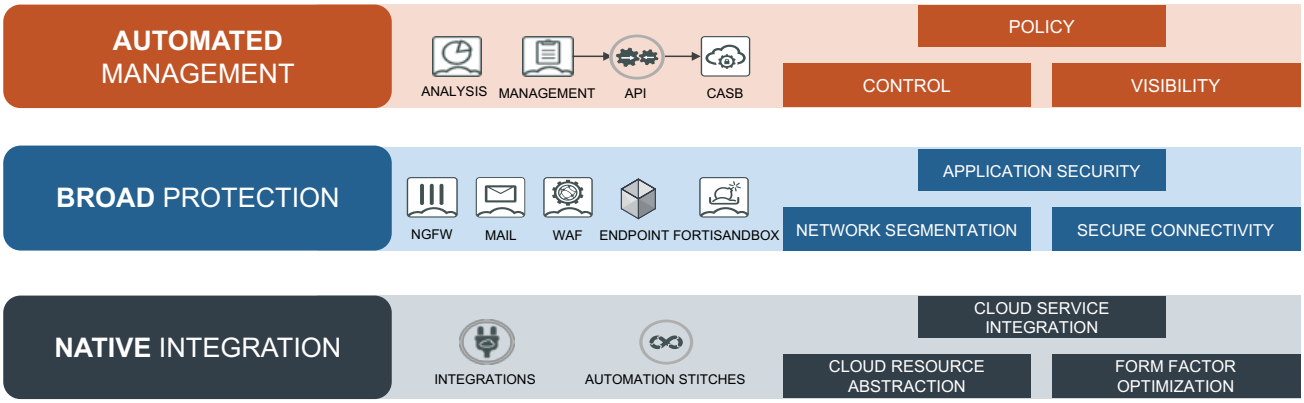
Native integration pertains to a security solution's ability to understand cloud-based information classification as part of overall security policy management and enforcement capabilities as well as leverage native cloud services as part of the security solution. Following are some of the key capabilities of a natively integrated cloud security solution:

- **Cloud connectors.** Security solutions must be able to connect to the cloud and represent all resources in the cloud in a way that security administrators can intuitively define policies and analyze security events. They must also enable security devices to dynamically enforce security policies in accordance with the continuous changes that take place in the cloud infrastructure.

  With cloud resources typically using metadata and labels to indicate their logical function or classify their information, connectors can be used to normalize the different types of resource metadata across multiple clouds. This enables them to build and enforce consistent security policies. More advanced implementations of cloud connectors learn and list the overall set of cloud resources and represent them in a more comprehensive manner, such as in the form of a network topology. This makes it easier for security teams to investigate their cloud security posture and to implement effective security policies.

- **Optimization.** To keep up with the cloud-based resources and infrastructure performance, security solutions must be integrated with the different cloud services and provide optimized software solutions that utilize the highest possible performance in the cloud. Thus, security solutions will never become a bottleneck when protecting a cloud-based workload. The most suitable solution should be provided for each form factor such as container or VM on a particular type of hardware.
- **Automation scripts.** Preparation for unplanned events in the cloud require automation scripts. These enable quick reaction to system failures, infrastructure changes, or major security events. These scripts need to access the native automation capabilities of each cloud system, utilizing those capabilities to automate processes consistently across all clouds.
- **Threat feeds.** A comprehensive, multi-cloud security solution integrates dynamic threat feeds as dynamic objects, which are continuously blocked. These threat feeds consist of extensive intelligence based on events across the security provider's infrastructure. This includes threat intelligence collected from all of their customers' deployments. The ability to integrate these threat feeds from the different clouds, combined with other sources of threat intelligence, is essential to protect an organization's entire infrastructure.
- **High availability.** Each cloud supports high availability leveraging different capabilities. The underlying security must support each cloud environment in a way that offers consistent and predictable security enforcement. In this case, it must support different active/active or active/passive schemes, natively integrating with each cloud to support the availability of business-critical systems.
- **Auto-scaling.** One of the primary benefits of a cloud infrastructure is its elasticity and on-demand capabilities. This includes the ability to scale usage in and out of the cloud based on varying business needs—paying only for what is used. Native integration with the auto-scaling capabilities of the cloud enables the security infrastructure to keep up with cloud infrastructure scaling based on volume and demand. This ensures that applications are continuously protected.
- **Configuration templates.** An essential part of integrating with the cloud operational model is the ability to templatize deployments using configuration templates. These help security administrators provision security solutions quickly and accurately across various cloud platforms and in accordance with varied cloud workload deployments. The use of configuration templates reduces the potential for human error—notably, in the way security solutions are configured. They also accelerate the ability to attach security to new workloads and, in turn, confidently deploy new workloads.

- **Service integration.** Cloud platforms offer software and platform services that simplify the consumption of various capabilities by eliminating users needed to master each of these technologies. The ability of a security solution to integrate with each cloud platform and to offer security functionality as part of the native service consumption model is critical. Here, integration extends security protection to more use cases and services as a fundamental capability, offering basic protection for experimentation environments as well as those that are not yet part of a broader security management life-cycle routine.



THERE ARE THREE PILLARS OF MULTI-CLOUD SECURITY: NATIVE INTEGRATION, BROAD PROTECTION, AND MANAGEMENT AND AUTOMATION.

2. BROAD PROTECTION

The rapid adoption of cloud infrastructure for business-critical applications requires a new form of coordinated and broad multilayer security solutions. This is especially true given the continued evolution in the advanced threat landscape and the complexity of distributed, multi-cloud infrastructures. Organizations using multiple clouds should ensure that every part of the attack surface is protected against every kind of threat. The following are some of the key elements of network security that are a part of a comprehensive solution:

- **Zero-day threat protection.** According to FortiGuard Labs, up to 40% of malware observed on a given day in 2018 is unknown or zero-day. This is partly because auto-generated, single-use malware is increasingly popular with cyber criminals. Sandbox analysis, in which potential malware is observed in a simulated environment before being allowed into the network, is an essential part of a cloud security strategy.

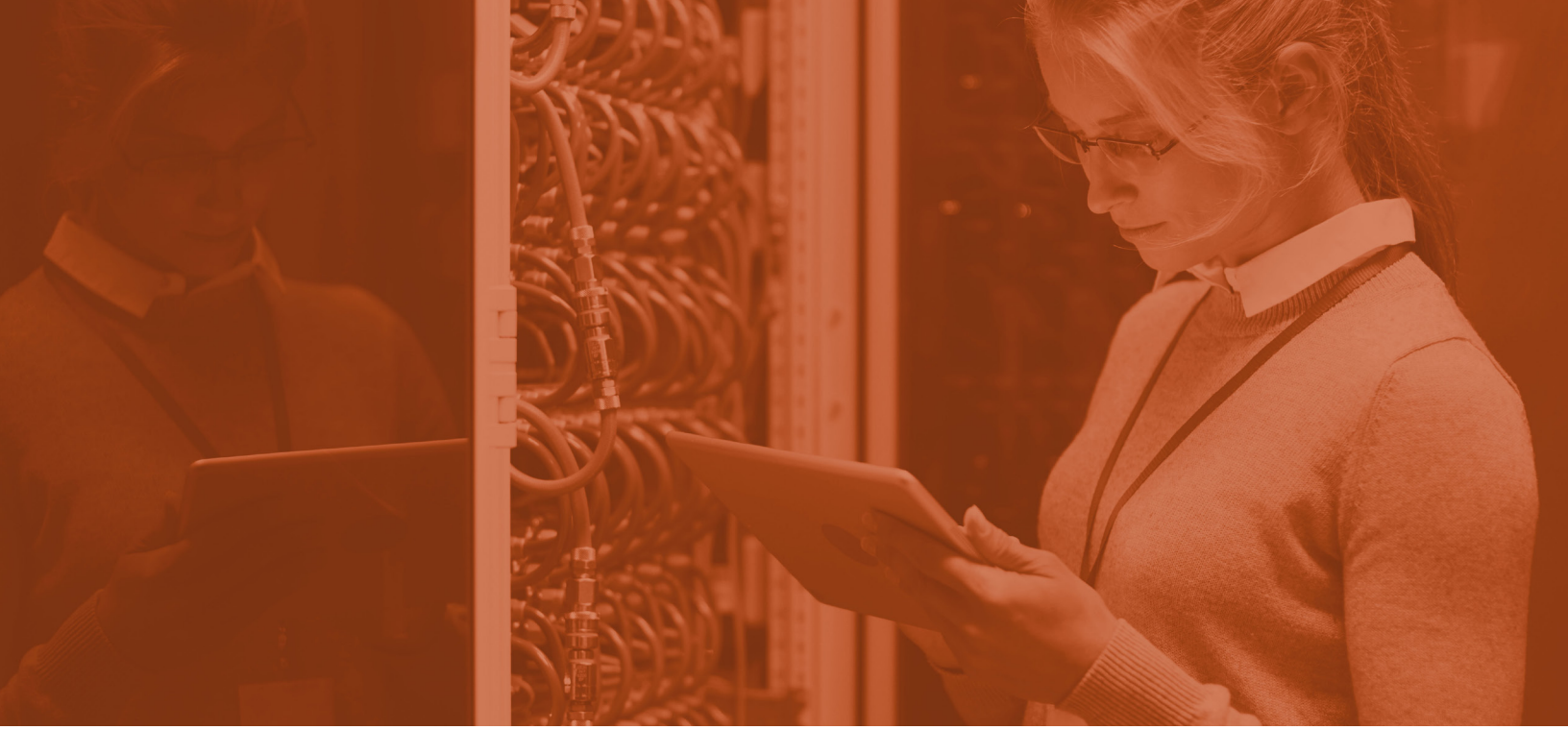
  But sandbox analysis is time- and processor-intensive and can slow performance to a crawl if most traffic is not prefiltered. Robust use of artificial intelligence (AI) and machine learning (ML) for threat detection through analysis of characteristics catches many threats before they need to be subjected to sandboxing. The ability to deploy sandboxing technologies, either in Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS) environments, is an essential capability that should be part of any multi-cloud security strategy.

- **IPsec VPN.** The ability to extend connectivity into the cloud and across clouds from different sites is essential. As traffic across cloud environments occurs frequently, the ability to isolate traffic and build consistent networking security policies across the infrastructure are key enablers to unifying the disparate cloud environments. The support of both site-to-site IPsec VPNs and VPNs across cloud virtual networks is essential to consistently isolate networks. VPN implementations should be interoperable with different cloud VPN solutions, offering flexibility for different organizations and organizational units.

- **SSL VPN.** SSL VPN is very important for providing access to select business-critical services, whether hosted in the cloud or on-premises. The ability to extend an organization's remote-access infrastructure to the cloud enables seamless connectivity regardless of where a service is hosted.

- **Application control.** As organizations place an increasing variety of applications on the cloud infrastructure, the need to gain visibility and manage security at the application level becomes more important. Security is more adequate when it is performed based on the actual application being used and not only the resource or service that is being accessed. The ability to implement application-aware security in the cloud, across clouds, and across the hybrid cloud infrastructure is essential in building a fluent multi-cloud infrastructure without compromising security.

- **SD-WAN.** Organizations are now investigating—and many are deploying—software-defined wide-area network (SD-WAN) solutions to leverage reduced cost of internet connectivity while gaining increased access to cloud-based applications. The ability to backhaul traffic to the internet through a centralized security infrastructure in the cloud offers substantial benefits to organizations as they strive to reduce their physical data-center footprint. The existence of SD-WAN functionality in cloud-based security products is gaining in importance as organizations work toward a multi-cloud strategy and build an underlying infrastructure to support this transition.



- **Stateful firewall.** As much as stateful firewalling is considered basic functionality, the ability to statefully segment networks and application traffic remains the cornerstone network isolation capability. Specifically, the ability to enforce consistent policies across multiple cloud networks and cloud infrastructures statefully gives organizations the ability to port applications across infrastructures with more confidence.
- **Next-generation firewall (NGFW).** With organizations building more business-critical applications in the cloud, the need for advanced security capabilities increases. It is imperative to offer the same breadth of security functionality for the cloud as for on-premises services. This includes benchmark protections such as intrusion prevention, web filtering, and anti-malware.
- **Web application firewall (WAF).** Specifically addressing the threats associated with the largest category of applications, web application firewalls help organizations address the requirements of risk-management policies and regulatory requirements related to protecting end-user information and ensuring business continuity. Some of the key features offered by a WAF service are data leak prevention, contextual understanding of web application flow, and the dependency between different elements of an application.
- **Mail security.** As email remains the most common vector for the delivery of malware, and as organizations move their email systems to the cloud, the cloud is often the logical placement for a mail gateway. Further, the cloud remains the preferred infrastructure to deploy backup systems, with a mail security gateway the ideal product to place in the cloud for backup purposes.

3. MANAGEMENT AND AUTOMATION

Unifying the management of an organization's network security infrastructure makes the visibility and control throughout the entire infrastructure practical and usable—from the data center to multiple clouds. Further, centralized management enables the automation of security life-cycle management processes as well as the application of consistent security policies across multiple clouds. The goal is to be able to manage the cloud and on-premises infrastructures similarly by leveraging the same level of visibility and control. This enables organizations to fulfill desired enterprise risk management and regulatory compliance objectives.

Effective security management and automation consists of four primary elements: visibility, control, policy, and compliance.

- **Visibility.** Visibility into the diverse set of applications, networks, and infrastructures in a multi-cloud environment is a cornerstone of a security posture assessment. Such assessments are both a starting point and an ongoing process in security management. Organizations should be able to identify resources spread throughout the infrastructure, associate traffic flows with those resources, understand which applications are being used by each resource, and identify what data traverses the network.

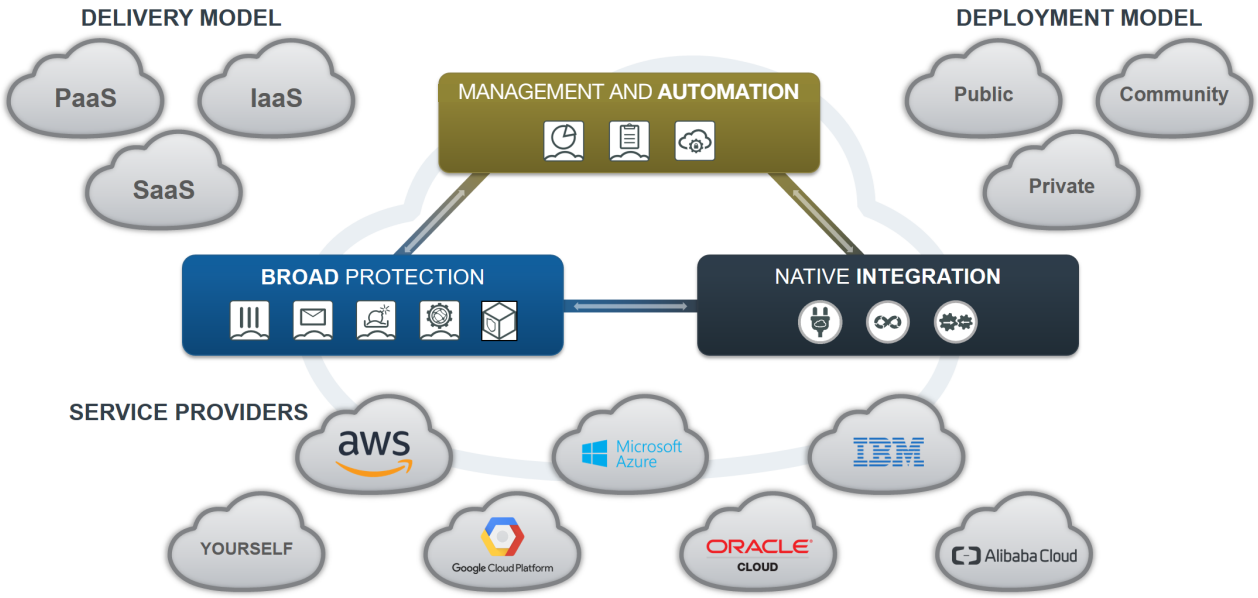
  This information allows an organization to validate whether security policies are effective and if additional security policies are needed to provide adequate levels of security for the infrastructure. In a multi-cloud environment where applications communicate across the various infrastructures, the ability to centrally trace traffic flows and understand the sequence of events across each cloud environment often offers more insight than what standard security tools reveal. In addition, the ability to tie security infrastructure insights with cloud infrastructure visibility into a single pane of glass simplifies operations even further.
- **Control.** Once an organization has full security visibility, the next step is to apply controls to relevant functions. This involves applying configuration changes and populating the security

infrastructure with the relevant resource-related information pertaining to the multi-cloud security posture. Security management tools should extend a consistent control framework across the broad set of security functions. Additionally, the control framework should extend to the native security functionality provided by each cloud platform. This should allow administrators and operators to apply security changes throughout the infrastructure, regardless of the underlying technology.

- **Policy.** By leveraging the visibility and control capabilities enabled by the desired multi-cloud infrastructure, an organization gains significant security management capabilities and can realize the premise of consistent security management and enforcement throughout the infrastructure. For example, centralized visibility and control enables security staff to implement application-driven policies regardless of where different application components reside. Since the overall application life cycle is what drives changes to the infrastructure, the burden and time to interpret how changes to applications affect the infrastructure are significantly reduced. Instead, security staff can modify security settings in accordance with application life-cycle events to achieve more consistent security policies.

  And at a strategic level, instead of spending cycles on how a security policy should be implemented for each unique cloud platform to comply with organizational requirements, security staff can rapidly implement policies in a unified security management tier that abstracts the underlying technologies and allows for much faster updates.

- **Compliance.** Ultimately, network application and information security tools and practices allow organizations to manage the risk associated with operating digital assets and compliance with industry regulations. Specifically, maintaining a consistent security posture and automating security operations significantly increases an organization's ability to maintain regulatory compliance. In addition, centralizing security management and automating workflows and threat-intelligence sharing gives organizations the ability to quickly react to emerging threats. They also can more effectively mitigate risk across their entire attack surface without requiring overly challenging security operations.



A COMPREHENSIVE SOLUTION BUILT ON NATIVE INTEGRATION, BROAD PROTECTION, AND SECURITY MANAGEMENT AND AUTOMATION CAPABILITIES MUST WORK ACROSS DIFFERENT DELIVERY MODELS, DEPLOYMENT MODELS, AND SERVICE PROVIDERS.

SPECIFIC CLOUD USE CASES

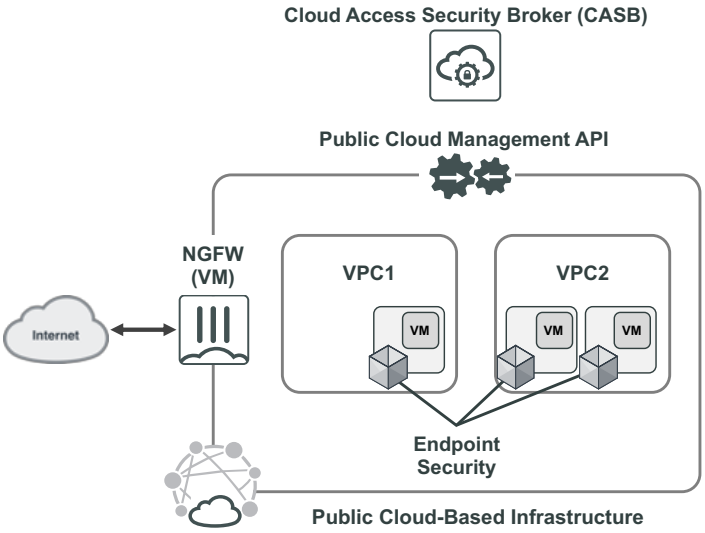
Security for cloud workloads and applications must be implemented in a way that proves value and is intuitive to build and operate. The result should be a solution that is truly comprehensive in risk mitigation for a specific given use case. The following are some of the most prominent examples:

INSIDE-OUT IAAS SECURITY

Cloud providers protect their individual infrastructures. However, end-user organizations need to protect their cloud assets and applications. When deploying specific applications in the cloud, securing the supporting infrastructure of these applications presents unique challenges and should be addressed inside out from three different dimensions:

- At the workload level, with an agent controlling the consistency of both the application and east-west traffic.
- At the network level, securing north-south communications with an in-line NGFW that also offers VPN functionality.
- At the API level, there is a need for a third party to manage an organization's security posture via the cloud's API. A cloud access security broker (CASB) supports that function.

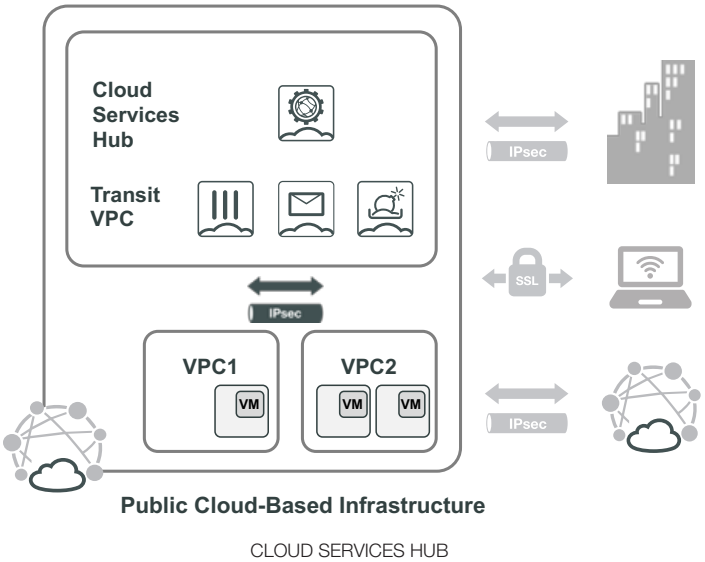
The different products securing these different dimensions should work together and be managed centrally through a consistent security policy.



INSIDE-OUT IAAS SECURITY

CLOUD SERVICES HUB

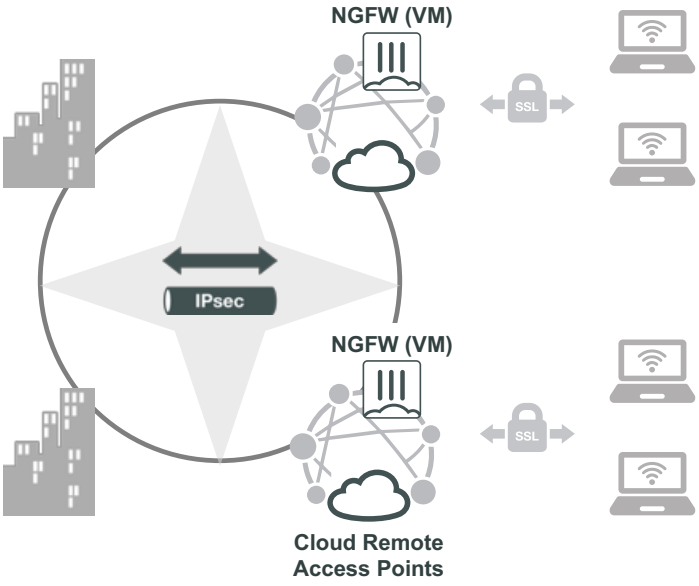
Organizations can leverage a cloud-based VPN to provide shared services to cloud and on-premises networks. Networks and applications that are independently developed and operated by different organizational units (viz., lines of business) can be connected to the cloud services hub over a VPN connection. They then utilize shared services such as application-based firewalling, application communication protection, context- and application-aware WAFs, email security, and sandbox-based advanced threat protection services. All of these can be managed from the cloud.



CLOUD SERVICES HUB

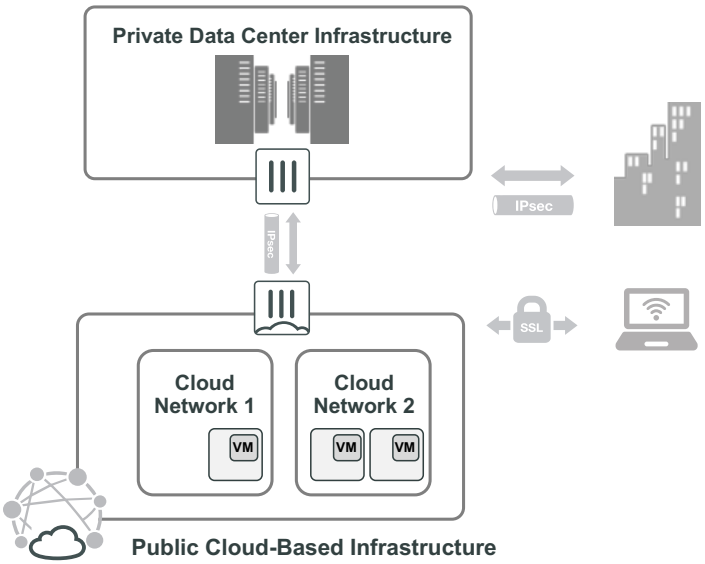
REMOTE ACCESS VPN

Leveraging the global presence of cloud regions and data centers, organizations can build remote-access VPN termination points globally and deploy gateways dynamically based on end-user requirements. Consistent management of the different VPN termination points provides flexibility to deploy them worldwide without introducing unnecessary management overhead. Additionally, the dynamic nature of the cloud means that deployment is not permanent, but rather it can be set up or turned off as needed. This scenario applies to both when applications reside in the cloud and when they are on-premises. In the case of on-premises applications, they can connect to the cloud using site-to-site IPsec VPN tunnels.



HYBRID CLOUD

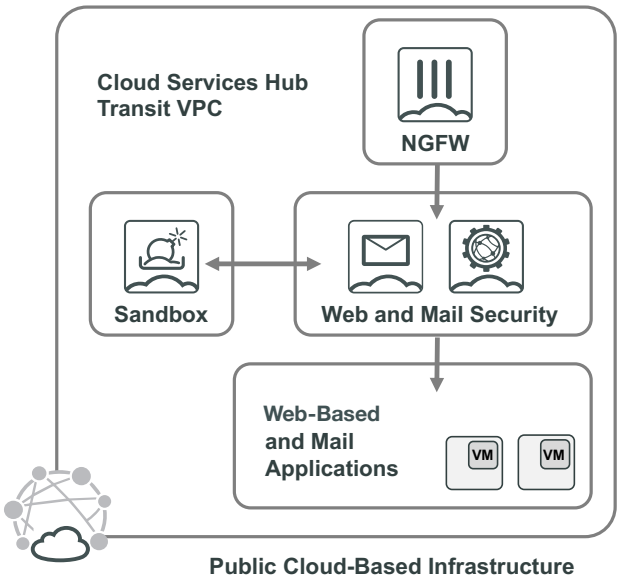
Many organizations leverage the public cloud to provide infrastructure for IT solutions alongside on-premises data centers. In many cases, new applications are uniformly deployed to the public cloud, while in other instances they are deployed across public and private clouds in parallel. It is important for a solution to offer support for both private cloud and public cloud technologies. It must also deliver fast and powerful security in order to cope with high-volume data transfers. Consistent management of security policies is critical, too. This ensures migration of applications from one infrastructure to the another does not incur unwanted security operational overhead that could potentially result in human error that compromises security. Additionally, security must protect the entire attack surface and scale to accommodate constant change.



ADVANCED APPLICATION PROTECTION

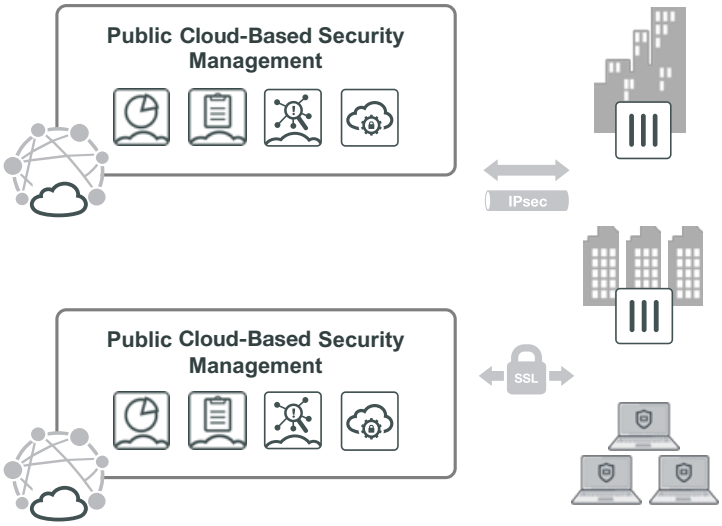
As organizations deploy business-critical applications containing sensitive data in public clouds, providing security at the application level becomes critical. This helps support organizational risk-management objectives while ensuring compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the European Union's General Data Protection Requirement (GDPR).

Security solutions must offer broad, multilayer, application-specific security. This allows organizations to move applications to the cloud based on business requirements rather than security availability. Further, organizations have the flexibility to choose the cloud platform that makes business sense rather than technical constraints.



SECURITY MANAGEMENT FROM THE CLOUD

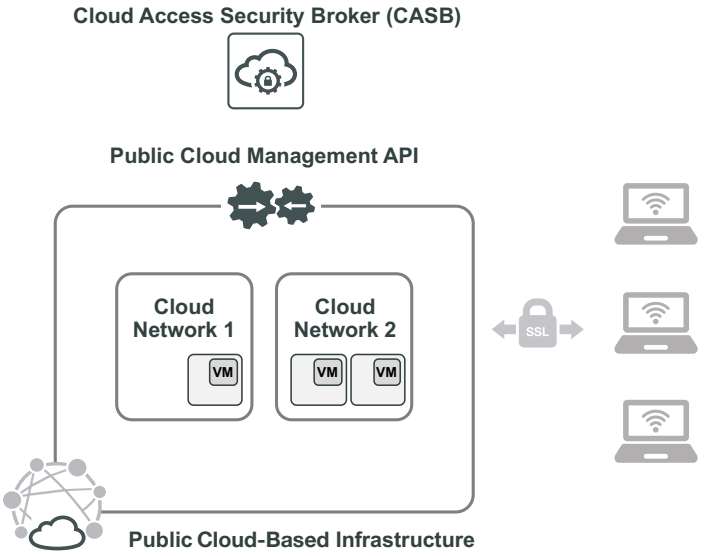
As organizational networks become global and distributed, connectivity is required across multiple branches, data centers, and cloud environments. Thus, organizations must be able to manage security in a scalable, fault-tolerant manner that simplifies operations and streamlines security life-cycle management. Security management solutions should leverage the global presence of top cloud infrastructure providers and the elasticity of storage and computer resources for centralized, global security management and operations systems.



PUBLIC CLOUD USAGE MONITORING AND CONTROL

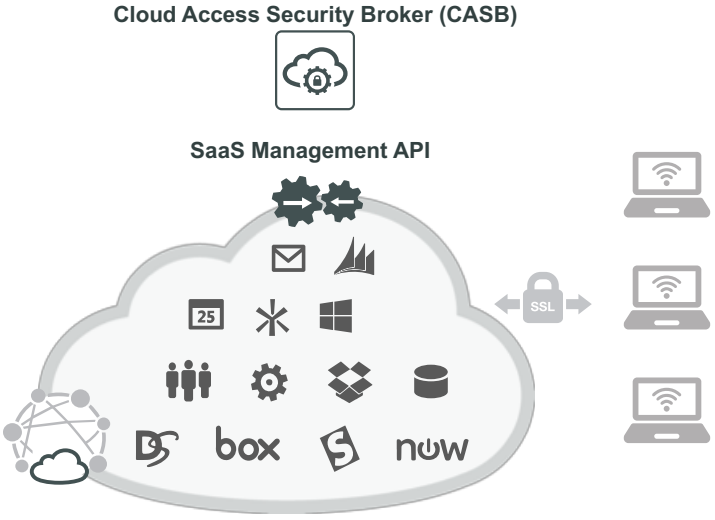
Public cloud usage is often not monitored. Further, users can perform almost any function they want to—limited only by the permissions of their associated user role. This unsupervised pattern leads to unsecure, cost-ineffective usage of cloud resources.

However, with CASB performing security posture management in concert with the in-line capabilities of the security infrastructure in the cloud, organizations gain full visibility over configuration changes across a variety of public cloud infrastructures. They can also make better decisions and policy modifications addressing their business requirements while enforcing acceptable use policies and compliance with regulations and security standards.



SAAS USAGE MONITORING AND CONTROL

As the use of SaaS applications grows from both enterprise and remote locations, so does the need to enforce a consistent security policy at the user level. Cloud security must integrate security controls from perimeter firewalls used to inspect all outbound traffic, including that generated by SaaS applications. Here, malicious content and insecure access may often be traced only by correlating different vectors of communications. For instance, collaboration on a specific file in a SaaS application and sending that file via email can only be traced by a comprehensive CASB and in-line protection such as an on-premises firewall.



SAAS USAGE MONITORING AND CONTROL

CONCLUSION

The cloud offers organizations immense business opportunities. But without the right security infrastructure and operational framework in place, the cloud presents serious security challenges that can have far-reaching repercussions. Business-critical applications and data are scattered across multiple clouds. The rapid, decentralized adoption of cloud services often results with a heterogenous set of security tools and policies that are managed in individual silos.

The shared responsibility model for cloud security dictates that cloud providers only protect the infrastructure. This does not include applications that are deployed and running on the cloud as well as data that is stored in the cloud. Rather, end-users are responsible for securing the application layer. With each cloud provider using different tools and approaching security differently, this creates additional complexity for enterprises that must connect those into the security tools they employ to protect their applications.

To secure multi-cloud environments, enterprises must follow three principles:

- Native integration with all major cloud providers
- A broad suite of security tools that cover the entire attack surface
- Centralized management of security, including automation of workflows and threat-intelligence sharing

Due to the heterogeneity of cloud deployments, there are multiple security use cases that organizations must consider. Each of these comes with security requirements such as integration of all security elements across the entire attack surface, security automation that extends across multiple clouds, cloud-specific security frameworks with centralized policy management for regulatory compliance, security that stretches across the full application life cycle, and a cloud services hub for delivering security services, and more.

[1] "Fortinet Threat Landscape Report Q3 2017," Fortinet, November 17, 2017.

[2] "Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond," Gartner, October 6, 2015.

December 3, 2018 11:45 AM

270835-0-0-EN

WP-Key-principles-securing-the-enterprise-cloud