SOFTWARE-DEFINED SECURITY FOR CLOUD

STEALTH™

Cloud Security Challenges

Even before the COVID-19 pandemic disrupted how organizations around the world operate, cloud computing likely was an integral part of your enterprise network. The IDG Cloud Computing Survey 2020 shows that a huge majority of organizations (92%) have at least one cloud deployment, while more than half of organizations (55%) use multiple clouds.[i]

IDG says cloud spending is on the rise and that "32% of IT budget is expected to be allocated to cloud computing within the next 12 months." This is not surprising, given that the COVID-19 pandemic has made cloud deployments essential for organizations to support a highly decentralized workforce and remain connected with partners, suppliers, and customers.

But cloud no longer is a single line-item in the budget. Cloud has grown and evolved as a technology to encompass an array of core and associated products and services. Public, private, and hybrid are just the bare infrastructure essentials, as apps, DevOps tools, containers, microservices, and third-party SaaS platforms continue to proliferate.

Though this trend has given rise to powerful and innovative computing options for organizations, it also has introduced complexity—and uncertainty—for IT professionals charged with securing expanding cloud footprints in their organizations. And with remote work becoming the rule rather than the exception, scalability has become yet another immediate cloud management challenge for your organization.

Moreover, as every IT security professional knows, the major burden of cloud security falls squarely on you: Cloud vendor service agreements provide only for security guarantees within the vendor's cloud infrastructure, and configuration and modification of security to protect customer data is left solely to the customer.

> **"Through 2025, 99% of cloud security failures will be the customer's fault. CIOs can combat this by implementing and enforcing policies on cloud ownership, responsibility and risk acceptance. They should also be sure to follow a life cycle approach to cloud governance and put in place central management and monitoring plans to cover the inherent complexity of multi-cloud use."**
>
> **– Gartner.**[ii]

To reduce security vulnerabilities, technology research and consulting firm Gartner recommends a centralized, policy-based approach. Central management and monitoring plans for cloud security are difficult to implement, however, given the diverse nature of cloud technology as well as legacy on-premises security systems and intrusion detection and protection devices. Add to that cloud vendor security measures, and complexity and risk multiply. Indeed, most security professionals can clearly identify cloud security "hot spots" that require attention and remediation to reduce risks in their environments. The following are among the top cloud security challenges IT security professionals face today. Most undoubtedly will seem familiar to you:

- Scaling security to meet the needs of a growing remote work force
- Consolidating and centrally managing security
- Eliminating cloud security blind spots
- Protecting hybrid cloud
- Coordinating multi-cloud security
- Containing shadow IT and "rogue" device risks
- Extending security to future cloud: DevOps, containers, and tools

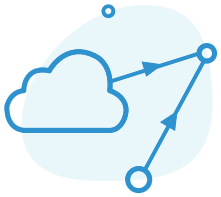
Centrally Managing Cloud Security

For you to get a better handle on cloud security, it is imperative that your organization move toward centrally assessing, implementing, and monitoring security—extending from existing legacy premises systems to multi-cloud. Without central policies and enforcement, vulnerabilities and risk are inevitable, not to mention duplicative efforts in piecing together and reconciling separate security technologies and policies across differing architectures, workloads, and devices.

There's a good chance you're "flying blind" when attempting to secure your enterprise's expanding cloud. A recent SANS Institute survey shows that "48% of respondents said they lack visibility into data that is processed within their organizations," as "nearly 55% struggle with a lack of integration between current security analytics tools and cloud infrastructure." Furthermore, "43% faced a lack of threat insights targeting cloud environments."[iii]

Protecting Hybrid Cloud

When you move data and workloads to the cloud, it is easy to underestimate the complexities of securing the hybrid on-prem/cloud ecosystem you have created. While the cloud portion of the systems may be sufficiently secured, the remaining on-premise security may not follow the same policies and procedures due to out-of-date tools. Such a disconnect can occur when legacy, on-premises security methodologies and technologies are too inflexible or not designed to support the dynamic, elastic nature of today's (and tomorrow's) cloud environment. This potential gap in policy enforcement and technology flexibility shows: Cloud security breach reports significantly increased in 2019, with many high-profile security failures making headlines, like the Container Worm and public cloud provider DDoS attacks. The bottom line is that if on-premises and cloud security are not coordinated and monitored, the chances of vulnerabilities increase.



"Of the cloud technology decision makers at large companies surveyed, 86% said they now have a multi-cloud strategy. And 60% of enterprises are now moving, or have already moved, mission-critical applications to the public cloud, the report found." –

– TechRepublic.[iv]

Coordinating and Governing Multi-Cloud Security

Many of the same platform incompatibilities found in a hybrid cloud can follow you to multi-cloud environments where multiple clouds—and multiple cloud vendors—are utilized for greater efficiency, performance, or to leverage innovative business opportunities. Multiple vendor solutions can be especially difficult to secure given the different security configurations for each. For example, Azure, AWS, and Google each have specific and platform-dependent security configuration parameters. Nonetheless, proper governance of security policies across multiple clouds is essential and up to you, the customer, to provide.

Containing Shadow IT and Rogue Device Risks

Shadow IT in the form of SaaS applications and document and app sharing services is an ongoing, perennial cybersecurity challenge. Meanwhile, rogue devices on your network pose additional, unnecessary dangers. The common risks shared by shadow IT and rogue devices are unenforced security policies on an enterprise level. If you establish and enforce system-wide best practices, both risk factors can be mitigated to dramatically reduce security vulnerabilities. In most environments, however, these risks are addressed separately – and with mixed results.

"82% of the respondents [surveyed] are concerned that employees don't follow cloud security policies and 38% have issues detecting and responding to cloud security incidents."

– Survey report, CSO Online.[v]

Cloud Security Future

If IT pros have learned one thing over the past decade, it is that cloud technologies are constantly evolving. New tools, architectures, and processes are driven as much by customer demand as by developers. And all that innovation comes with potential risk. Container technology, for example, adds flexibility and speed to market for customers—but can also introduce vulnerabilities and complexity. Security flaws in dozens off-the-shelf containerized apps have been widely documented. To help curb these risks, you need consolidated, centrally administered mechanisms for both implementing their best practices and monitoring results.

Unisys Stealth Cloud Security Solution

Unisys Stealth® is software-defined security. It simplifies yet improves network and cloud security and serves as the backbone of your whole-network Zero Trust strategy. Stealth™ blankets every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy—from mobile phones and desktops, to servers, to cloud, and even IoT. In fact, Stealth orchestration and deployment are highly automated and centrally managed. As your security policies evolve, changes can be made and instantly propagated across the enterprise. Meanwhile, Stealth monitors and enforces all your Zero Trust policies, automatically isolating violations and alerting administrators. With Stealth Zero Trust, security is seamlessly woven into the fabric of your entire network. It's the engine that drives your speed to security.

Stealth achieves this through micro-segmentation and compartmentalization, deploying hyper-secure encrypted IPsec tunnels to and from the cloud to create communities of interest (CoIs). CoIs limit user and application access to just the other users, applications, and data also assigned to that CoI.

Outsiders cannot gain access to the CoI, and data cannot be shared with or exfiltrated to users or applications outside of the CoI. All data in motion is strongly encrypted—even if malicious attacks intercept data, it is useless to them. Applications, legacy servers, or clouds outside of the CoI will not respond to pings or other means of network sniffing or discovery. This cloaking eliminates visibility for hackers, whether they're using a rogue device from within a network or attacking from the outside via a public cloud. In the unlikely event of a cloud breach, even if a user's account is compromised or malware is detected, Stealth can automatically isolate the threat in real time. If malware goes undetected, it cannot "phone home" to a command and control server if that server is outside of the CoI. This renders the malware useless. Similarly, phishing attacks are immediately blunted and blocked, with no chance of data exfiltration or deletion.

Best of all, in the new, remote-heavy enterprise working environment, Stealth scales easily and works on any existing IP network—on-prem, in the cloud, or integrated into a partner's network. Even non-IP based IoT devices can be locked down using secure Stealth Virtual Gateway.

Stealth also provides a valuable tool that is essential for security and operational awareness. Stealth Security Dasboard is a comprehensive, real-time security dashboard that provides you with a clean, simplified look at the status of your network in a single view. This enables you to safely address your business outcomes with immediate insights about the environment, your users and their devices that were isolated, your isolations trends and statistics. This will in turn help you make informed decisions, meet compliance requirements, and improve the overall security of your enterprise.

Public and hybrid cloud—Stealth ensures all connections, traffic to, from, and within the cloud and on-premises are encrypted in hyper-secure tunnels and locked into clearly defined, trusted enclaves.

Multi-cloud—Stealth ensures connections to and from multi-cloud and multi-vendor clouds are encrypted and secured at both ends, with no gap or void for attackers to exploit. Stealth improves inter-cloud security and is not dependent on any one set of vendor security controls.

As with agile development strategies, the allocation of security resources to inspect traffic or respond to a threat needs to be instantaneous. Unfortunately, many of the security tools available in cloud environments have not been fully optimized to take advantage of the functionality of the cloud, which can cause threat detection and response to be delayed or incomplete. In many respects, this is the same mistake that organizations made when they tried to extend their on-premise applications to the cloud."

CSO Online, April 2019.

Cloud containerized microservices—Cloud containerized microservices—Stealth extends protection for provisioned microservices to provide container, pod, cluster, and microservice-level segmentation of Docker and Kubernetes environments that you deploy and manage within a public cloud. Core security policies in place are propagated throughout the system, regardless of location within the enterprise. In short, Stealth works across your entire IT estate.

Software Defined Security and Fabric

Stealth gives you a ubiquitous, best practice-driven software fabric that requires no separate configurations or hardware dependencies among different platforms—one policy engine drives protection across legacy, cloud, partner, and multi-cloud devices and platforms, regardless of vendor or location. Shadow IT is eliminated, and rogue devices are blocked. The Stealth security fabric delivers persistent, real-time monitoring and proactive protection. Policies are applied and automatically distributed from a central console. In the process, many security point solutions and legacy firewalls and devices can be dramatically reduced or eliminated.

Stealth Cloud Security Benefits

By deploying Stealth, you get speed to security—all with your existing cloud infrastructure and applications. There is no need to rip and replace anything. By relying on hyper-secure, encrypted IPsec tunnels to establish CoI-based least-privilege access to networks, applications, and data, you can deploy one of the most advanced cybersecurity platforms in the industry from a provider you know and trust. Among the specific benefits of Stealth:

Ensures easy-to-assign policy and role-based protections for every user across private, public, hybrid, and multi-cloud.

- Ensures easy-to-assign policy and role-based protections for every user across private, public, hybrid, and multi-cloud.
- Designed with cloud cybersecurity professionals and admins in mind.
- Guarantees least privilege – seen by most as a critical component to true cloud security.
- Enables you to defeat the adversary (both automated and manual) prior to Phase 1 of the Cyber Kill Chain® – during the critical reconnaissance phase. Stealth starts working at Phase 0 – effectively removing your network and cloud from adversary detection.
- Offers agentless options and protections.
- Provides purpose-built integration, serving as the backbone for any global network security architecture, whether it's AWS, Azure, Palo Alto Networks, SOCs, SIEMs, or Fusion Centers.
- Reduce and eliminate security point solutions and devices.
- Amplify and empower the human element of security, giving back control of the network and enabling true network and cloud resilience.

No longer just "monitor and detect" – Stealth provides your enterprise with the key to a comprehensive, holistic monitoring, detection, and response posture.

In Summary

Unisys Stealth provides flexible, extensible security for public, private, hybrid, and multi-cloud all within one software-defined security fabric. Policies and role-based protections are propagated from one central console, eliminating complex management and the need for multiple security point solutions. Real-time proactive isolation of malicious devices and operations ensures protection from both internal and external threats. In short, Stealth improves security, reduces costs, and streamlines management of your entire cloud environment.

Unprecedented times call for unprecedented infrastructure security. Stealth can protect your operations better, faster and more cost-efficiently than outdated security methodologies, while scaling to meet the challenges of a post-pandemic, highly decentralized network computing environment.

i. IDG Cloud Computing Survey 2020.
www.idg.com/tools-for-marketers/2020-cloud-computing-study/

ii. Gartner. “Is Cloud Secure?” Smarter with Gartner. October 10, 2019.
www.gartner.com/smarterwithgartner/is-the-cloud-secure/

iii. SANS Institute Identifies Security Blind Spots as Organizations Tackle Advanced Threats. August 26, 2019.
www.continuitycentral.com/index.php/news/technology/4364-survey-identifies-security-blind-spots-as-organizations-tackle-advanced-threats

iv. Rayome. “Why 86% of enterprises employ a multi-cloud strategy and how it impacts business.” Tech Republic. July 12, 2018.
www.techrepublic.com/article/why-86-of-enterprises-employ-a-multi-cloud-strategy-and-how-it-impacts-business/

v. Pratt. “3 top multi-cloud security challenges, and how to build a strategy.” CSO Online. October 22, 2018.
www.csoonline.com/article/3313110/3-top-multi-cloud-security-challenges-and-how-to-build-a-strategy.html

For more information or to request a demo, contact us
www.stealthsecurity.unisys.com/contact-us/

For more information visit www.unisys.com