CloudPassage

Agile Security at the Speed of Modern Business.

EXECUTIVE SUMMARY

Modern elastic computing is the single most disruptive force for IT organizations in the last decade. And while it has been an amazing catalyst for business growth and innovation, it has also placed Chief Information Security Officers (CISOs) in the uncomfortable position of slamming on the brakes for the sake of security. The highly distributive, elastic and on-demand nature of Infrastructure-as-a-Service (IaaS) has also resulted in unprotected workloads, shaky compliance postures and limited visibility into virtual infrastructure. It has also fragmented the tools needed to secure all corporate infrastructure, leaving security teams inundated with too many overlapping solutions that don't always play nice together.

The good news is that new, agile security platforms can help CISOs overcome these challenges and allow businesses to take full advantage of modern computing models. A truly agile security solution implements orchestration and automation to keep up with diverse, fluid and fast-moving infrastructures. It delivers comprehensive security and compliance capabilities that can be instantly provisioned to both traditional and virtualized datacenters, as well as private, public and hybrid cloud environments. It is built on an open, holistic platform that integrates with existing security and orchestration tools. And it scales to support a high growth infrastructure without penalizing processing power and driving up cost.

Agile security can empower CISOs and their teams to move at the speed of modern business and become enablers of innovation and growth. It puts security and compliance teams in a position to embrace elastic infrastructures and align security objectives with the strategies and objectives of the business.

DISRUPTIVE TECHNOLOGY CAN DISRUPT SECURITY

One of the biggest problems facing security and compliance teams is the agile nature of virtual computing. That's because traditional security and compliance tools are not designed to provide visibility, detection and protection in highly elastic environments. In the past, rolling out new assets or building out an infrastructure took months, which gave security teams the necessary time to configure and deploy security controls in lock step with the rest of IT.

Today, modern infrastructure enables organizations to launch thousands of server instances or containers in minutes. These workloads may have a lifespan of weeks, hours or even just minutes. That rapid rate of infrastructure change creates significant problems for security teams that rely on traditional approaches and tools that don't scale and require days, weeks or even months to configure and deploy.

Even if time wasn't an issue, effectively securing the distributive nature of elastic infrastructure is an elusive effort. With cloud computing, rather than having all of an organization's assets secured and segmented behind four walls and a firewall, its servers, workloads, data, applications and other assets can end up being scattered across multiple—and sometimes disparate—environments from traditional datacenters to private, public or hybrid clouds. Perimeter-based or datacenter-centric security and compliance solutions are not designed to address that degree of distribution.

Similarly, traditional solutions are ineffective at handling the lack of natural segmentation within cloud environments, whether private or public. When the infrastructure becomes virtualized, it takes the form of a large, flat network, which causes perimeter-based network level security approaches to break down. Organizations who route their traffic over Virtual Private Networks (VPNs) to security appliances in front of their own network still have no visibility into or way to understand and analyze the East-West traffic between the workloads, leaving them open to attack for lateral movement.

ACCELERATING M&A WITH INSTANT VISIBILITY

The world's number one CRM company grew up in the cloud and empowers companies to connect with their customers in a whole new way. As the company grew, it expanded its portfolio of product offerings many times through strategic acquisition of other firms. But ensuring visibility, protection and compliance across disparate IT environments can take months to pull off.

When acquiring another company that often had invested in diverse cloud infrastructure, the security team at the CRM company had to quickly assess policies, procedures and compliance prior to the merger being finalized. Typically this has to be done in the 90-day "quiet" period between when the merger is announced and the day the merger is finalized. But here's the catch: the security and IT teams cannot do anything to alter the acquired company's infrastructure during this time.

Using traditional tools and manual processes, this would take months; far too long to be ready on day one of the newly merged company. Here's how the CRM company solved the problem. During the 90 day "quiet period" prior to the merger being finalized, the security team took a few minutes to install CloudPassage Halo in read-only or audit mode on every virtual workload in order to gain complete visibility into the acquired company's infrastructure. Now the security team knew what they were dealing with and could plan their strategy for the combined companies. On the day the merger was finalized, Halo was switched into full enforcement mode and new security policies were uploaded, ensuring that the entire cloud infrastructure for the whole (merged) company was now being protected in a consistent, compliant way.

Left without a viable way to secure cloud infrastructures, security teams have little choice but to push back against business initiatives that seek to gain from the agility offered by modern infrastructure. That resistance runs counter to the business mandates for growth and innovation, creating rifts between CISOs and their business counterparts. As a result, many business units may simply go into shadow IT mode and contract computing services without the IT group's knowledge or involvement.

Rather than resisting change, security organizations need a way to embrace cloud computing and business agility. They need an agile security platform designed specifically to deliver protection and compliance for systems everywhere—from bare metal to public cloud.

THE ESSENCE OF AGILE SECURITY

Agile security needs to move at the speed of business—while also delivering orchestrated security and compliance that enables automated, hands-free provisioning for virtual infrastructures. A truly agile security model provides:

- Fast, on-demand deployment
- Instant visibility across mixed infrastructure
- Layered protection at the workload
- Automated, orchestrated security that complements DevOps methods and tools
- Seamless scalability without performance impact
- Full integration with existing tools

Fast, On-Demand Deployment

The highly flexible and elastic nature of virtual infrastructure helps drive agile businesses. But traditional security solutions weren't built for this kind of flexibility. Often they take weeks or even months to configure and deploy, slowing down the benefits of agile infrastructure. Agile security solutions must be offered as a service, take just minutes to deploy and are fast to update.

CloudPassage® Halo® is just such a solution. Halo is delivered as a service, so it's on-demand and fast to configure and deploy, allowing customers to get started in minutes. Halo agents are lightweight and non-intrusive, allowing them to be deployed on all systems, so security teams no longer need to compromise on server coverage. Agents can deploy through DevOps automation and orchestration tools for new IaaS instances or workloads, or through scripts or even manually on traditional servers. The agents can even deploy on live systems without reboot, making CloudPassage Halo completely non-disruptive to production environments. As new systems or workloads get spun up, the Halo security orchestration engine scales up automatically, giving enterprises great flexibility as their compute infrastructure expands and contracts.

Instant Visibility Across Mixed Infrastructure

As organizations take advantage of new compute models, they typically invest in different types of infrastructure environments. To handle baseline load of normal day-to-day operations, they might have traditional data centers, their own virtualized infrastructure or they may have built a private cloud on a platform such as OpenStack. To deliver a specific enterprise service or high-demand periodic or seasonal loads, they might use public IaaS from Amazon Web Services, Microsoft Azure, IBM SoftLayer or Google Compute Engine.

Organizations will often link their different public and private infrastructures together into a hybrid environment. This linkage might be designed to allow for greater integration or to augment the overall capability and capacity of their infrastructure. For instance, hybrid computing comes into play when organizations temporarily ramp up their capacity by leveraging a public cloud service when demand spikes beyond the capability of their private cloud infrastructure.

Increasingly, sophisticated threats and attacks put enormous pressure on enterprises that need to maintain visibility into their (now mixed) compute infrastructure. Traditional security tools simply don't work well in this dynamic environment. They often have a

heavy footprint on each workload so they don't scale well. And they don't automatically deploy on systems that are spun up, so organizations end up picking and choosing which servers receive a full set of security tools. This leaves many of their servers vulnerable to attack with no way to see it coming. To gain complete visibility would require hours of manual effort, put a burden on virtual server performance and create a logistical nightmare of multiple tools.

CloudPassage Halo solves these challenges by delivering a comprehensive set of layered security controls that allows companies to maintain complete, continuous visibility into all of their systems with a single user interface, no matter where those servers are deployed. This is accomplished with Halo agents that sit at each server/workload/container. The agents can be deployed in minutes, giving near instant visibility across complex infrastructure models. By making Halo agents ultra-lightweight and non-intrusive, they can be deployed everywhere on every server instance. With Halo, companies receive key security events, see any systems left exposed to newly discovered vulnerabilities across the entire enterprise, discover misconfigurations and get alerted if any workloads are being tampered with.

The "works anywhere" foundation of CloudPassage Halo gives assurance that once security and compliance capabilities are defined, they will work together seamlessly, no matter where the agents are deployed within a mixed enterprise environment. An added benefit of the "works anywhere" aspect of agile security is that it enables the flexibility to switch or expand to other IaaS providers as needed. As a result, companies are not locked into a single service provider that might work fine today, but quickly get surpassed by other providers in terms of features, performance or reliability.

Layered Protection at the Workload

Modern elastic cloud infrastructure is fundamentally breaking traditional security approaches. Public clouds have no natural perimeter and network segmentation, leaving individual cloud servers exposed. In private clouds, malicious East-West traffic inside the network is a serious threat. As new workloads are added and retired dynamically, change control is difficult and updating granular firewall rules and security policies becomes a risky, manual process. Traditional approaches break down as virtualized security appliances lack the dedicated hardware acceleration they've depended on, which limits scalability. Endpoint security tools have a large footprint, imposing a heavy burden on each workload. As a result, many workloads are left unprotected.

The CloudPassage Halo platform solves these issues by delivering hardened protection to every server, no matter where it lives. Each workload is instantly protected with multiple layers of security, not only against inbound attacks but also against lateral movement inside a cluster of workloads. Security policies are defined by logical application groupings instead of static network parameters, which means new workloads pick up appropriate settings automatically.

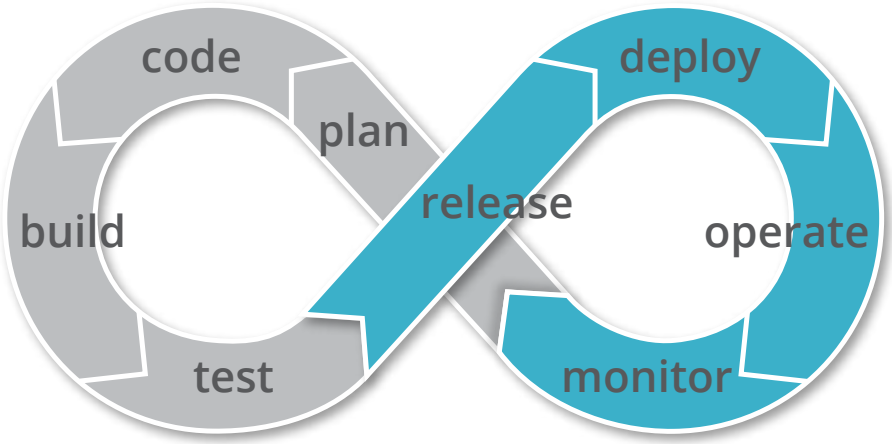
Unlike traditional security platforms that need to be configured or customized for each new deployment, context, change or environment, layered Halo security allows teams to define how they want certain types of systems to behave and then appropriately replicates those controls, coordinating their automatic deployment across multiple environments and contexts.

Host-based workload firewall management is at the center of the protection scheme. Layers of protection, including intrusion detection, configuration security monitoring, software vulnerability monitoring, file integrity monitoring and much more, augment these features. When used together, these capabilities form a more complete protection scheme and a complete picture of an organization's security posture, giving security teams the ability to rapidly detect and respond to vulnerabilities.

Automated, Orchestrated Security That Complements DevOps Methods & Tools

The rise of agile software development and DevOps methods have brought speed and quality benefits, but they have inadvertently put a huge strain on security organizations. Applying security policies based on static parameters and making manual rule changes just before production leaves little time for provisioning the policies. This impacts release quality, increases risk of errors and slows down the DevOps cycle. Trying to use DevOps orchestration tools to provision security can leave companies exposed since these tools lack critical controls and don't integrate with the rest of the security infrastructure.

Many organizations are now solving these challenges with CloudPassage Halo, which delivers security automation and integrates with orchestration tools like Chef, Puppet or Ansible. Security can now be an integral part of the DevOps cycle from development to test to production, maintaining speed and agility throughout the continuous process. DevOps teams provision new server images automatically with the assurance that security policies appropriate for that server are included. Security policies are defined by logical application groupings instead of static network parameters, making new workloads automatically protected. This way, layered security is built in during the development phase, not added on at the last minute.



For example, when security configuration monitoring is initially configured for a particular type of system, it can be defined once and Halo automatically implements monitoring in that same manner for any protected workloads that fall into that logical group. This orchestrated deployment can apply to any security and compliance function, speeding up the provisioning process.

Seamless Scalability Without Performance Impact

Scalability is one of the biggest technological hurdles to securing elastic infrastructure. The security platform itself has to be able to cope with rapid changes on demand and scale for large enterprise deployments. This can be a challenge with traditional security systems that aren't built from the ground up to deal with elastic environments. Additionally, the degree to which a security solution requires more virtual machines or compute power to run, the less it allows an organization to take advantage of the elastic nature of cloud computing and scalability.

Some vendors have tried to transform the capabilities of a physical security appliance into a virtual appliance in an attempt to secure cloud infrastructures. The problem with this approach is that physical security appliances rely on specialized hardware acceleration to perform the high-speed operations required by security and monitoring operations. This limits the scalability of each virtualized appliance, and requires the deployment of a greater number of virtual appliances to perform normal operations. Consequently, as an organization builds up its cloud environment, virtual security appliances quickly reach a point where they cannot keep up with scalability demands.

Other vendors take an agent-only based approach with virtualized end-point security tools. The compute demands at the endpoint of this approach can consume more than 25 percent of the instance's CPU cycles, significantly decreasing the performance of the actual workload on the server and dramatically inhibiting the ability to scale, while at the same time increasing overall cost of infrastructure. If agents have a footprint larger than 3MB, there will be scalability issues. The larger the footprint of the agent and the more the security processing is done at the endpoint, the more hardware memory and processing power is required to secure the cloud environment. Those processing requirements can multiply exponentially as infrastructure scales up with more containers and VMs. Realistically, it's extremely difficult to keep the footprint of a security agent small enough in an agent-only approach, which is why some security solutions have large agents with footprints larger than 100MB or even 200MB, even though it drastically compromises scalability.

THAT'S ENTERTAINMENT!

The world's leading online entertainment company has more than 60 million subscribers enjoying more than two billion hours of TV shows and movies per month, on nearly any Internet-connected screen. Heavily invested in cloud computing, the company dramatically expands or contracts its IT infrastructure hourly to accommodate customer demand and improve efficiency. Manually provisioning security policies in this highly fluid environment would be impossible. But leaving consumers unprotected isn't a viable option either. So the company leverages CloudPassage Halo to provide comprehensive visibility, security and PCI compliance for credit card and other critical customer information. Halo seamlessly integrates with existing operational models and IT orchestration tools so policy provisioning is fully automated and on-demand.

Notwithstanding the scalability issues, both the virtual appliance and some endpoint agent approaches have technological issues that also prevent them from being effective. With the highly distributed nature of cloud infrastructure, IT teams don't really know where their services are running, leaving them with a challenge on where to create a checkpoint or gateway to run a virtual appliance.

Meeting the scalability needs of agile security requires an approach that leverages cloud computing itself in conjunction with the use of lightweight agents. That's why the CloudPassage Halo agile security model employs a fast, lightweight security agent that collects status telemetry and enforces policy in real-time at the workload level, but offloads compute-heavy processing and analysis to a security analytics engine running in its own scalable, elastic cloud environment. This model allows CloudPassage Halo to collectively secure all the individual containers or workloads in large-scale private, public or hybrid cloud infrastructures without negatively impacting processing power—all while enabling high elasticity and scalability.

Full Integration with Existing Tools

The dynamic nature of modern infrastructure produces new capabilities and technologies at a rapid pace. To keep up with that change, agile security must be architected to take advantage of anticipated technologies so organizations can adapt and expand into new disruptive infrastructure models without breaking their security platform. That requires a holistic approach, as well as the use of open application programming interfaces (APIs) that can enable full integration with an organization's existing and future virtual infrastructure tools.

PROTECTING DIGITAL MARKETING FOR MILLIONS OF CONSUMERS

With more than $4 billion in annual revenue, this globally recognized software company recently completed a successful business transformation from physical product delivery to total online customer experiences by investing heavily in cloud computing infrastructure. They are also a digital marketing powerhouse, capturing online clickstreams for dozens of Fortune 1000 companies from millions of consumers every day. Employing traditional security tools in this highly dynamic environment simply wouldn't work. Manual policy provisioning, manual audit trails for compliance and multiple user interfaces would take many extra hours of manpower, slowing down the business.

The company solved the problem by using CloudPassage Halo to gain visibility on and protect tens of thousands of virtual servers used to store invaluable clickstream data from millions of consumers every day. The consumer data is analyzed in real time and used to push compelling marketing offers back out to the customer, dramatically improving marketing efficiency. Halo is fully integrated into the provisioning of the virtual infrastructure, making it fast and easy to scale visibility, policy provisioning, enforcement and compliance along with IT capacity.

These open APIs should provide full access to the agile security solution's monitoring and enforcement control functions. They should enable access at the individual control level (e.g., changing firewall management rules) and at the orchestration platform level (e.g., scaling security services for an application that is auto-scaling).

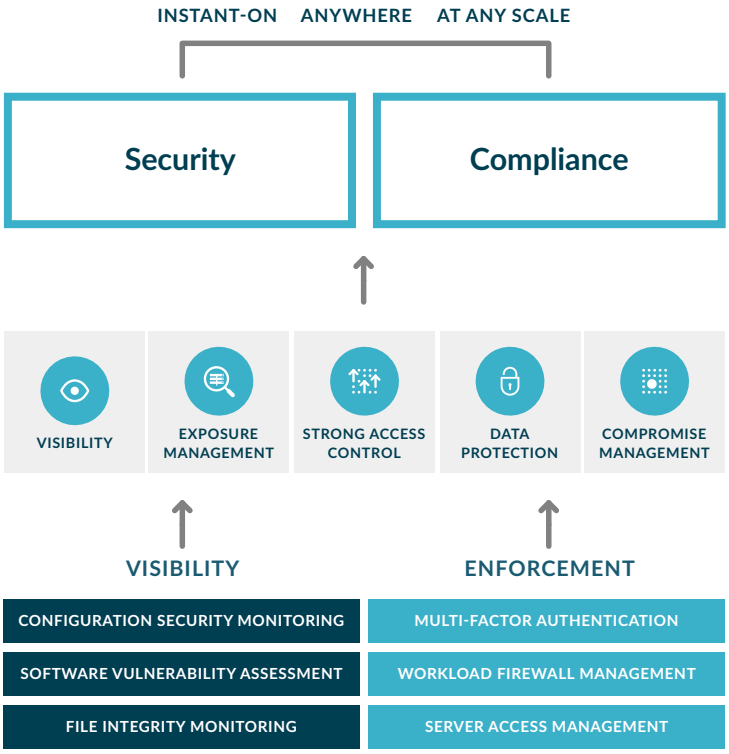
That is why CloudPassage Halo employs open RESTful APIs that enable clean extensions of security functionality within the Halo platform itself, and across third-party products and solutions. The ability for Halo to programmatically interact with other solutions enables it to leverage even more automation, orchestration and data-sharing capabilities from within the overall security environment. These same open APIs give Halo the characteristic of timeless persistence, enabling it to easily extend and integrate with emerging technologies and address future security demands.

This allows for quick, seamless integrations to any variety of systems already used by Security, Operations and Compliance teams. Customers often integrate with systems such as Security Information and Event Monitoring (SIEM) tools like Splunk or ArcSight as well as Governance, Risk and Compliance platforms like Archer. The use of open APIs also enables a high-speed DevOps workflow, weaving security into the very fabric of the DevOps cycle from development through testing and deployment with tools such as Chef, Puppet or Ansible.

AGILE SECURITY FROM CLOUDPASSAGE

CloudPassage Halo is an agile security platform that delivers continuous server visibility and protection no matter where the servers live. Halo enables organizations to take full advantage of IaaS speed and flexibility while keeping critical assets safe. Halo works seamlessly across any infrastructure, anywhere, including private, public or hybrid clouds—or traditional data centers. Halo frees limited security resources to focus on higher-value efforts. The automation of orchestrated security services inherent to Halo ensures consistency and accuracy, enables rapid provisioning and minimizes administrative effort.

CloudPassage Halo delivers continuous visibility into all servers and workloads, including risks and exposures they present. It enables teams to mitigate severe risks immediately and implement additional controls over time as needed. Halo protects against East-West traffic and lateral movement of attacks within the infrastructure and supports a "trust-but-verify" model for development and testing purposes. It gives the flexibility to deploy applications in multiple IaaS environments, whether they're private, public or hybrid. The deployment of Halo requires minimal support from operations and no ongoing effort from development or operations teams. Additionally, its on-demand licensing allows for a "start small, grow-as-needed" approach.



CloudPassage Halo levers deliver a full spectrum of enforcement and compliance capabilities that modern infrastructure demands:

- **Configuration Security Monitoring:** Evaluates new and reactivated servers against the latest configuration policies in seconds with almost no CPU utilization. Halo automatically monitors operating system and application configurations, processes, network services, privileges and more.
- **Multi-Factor Network Authentication:** Keeps server ports hidden and secure while allowing temporary on-demand access for authorized users. Halo supports secure remote network access using two-factor authentication (via SMS to a mobile phone, or using a YubiKey) with no additional software or infrastructure.
- **Software Vulnerability Assessment:** Scans thousands of server configuration points in minutes to maintain continuous exposure awareness in the cloud. Halo automatically and rapidly scans for vulnerabilities in packaged software—across all cloud environments.
- **Workload Firewall Management:** Easily deploys and manages dynamic firewall policies across all cloud environments. Build firewall policies from a simple web-based interface, and assign them to groups of servers. Policies update automatically across all protected systems within seconds of server additions, deletions and IP address changes.
- **File Integrity Monitoring:** Protects the integrity of cloud servers by constantly monitoring for unauthorized or malicious changes to important system binaries and configuration files. File integrity monitoring first saves a baseline record of the "clean" state of server systems and then periodically re-scans each server instance and compares the results to that baseline, with support for multiple baselines in simultaneous production use. Any differences detected are logged and reported to the appropriate administrators.

- **Server Access Management:** Easily identifies invalid or expired accounts. Halo evaluates who has accounts on which cloud servers, what privileges they operate under and how accounts are being used. Monitors all servers in public, private and hybrid cloud environments through a single online management console.
- **Event Logging & Alerting:** Easily manages and detects a broad range of events and system states. Halo enables the definition of which events generate logs or alerts, whether they are critical and who will receive them.

A SECURE INVESTMENT

This leading financial services firm helps more than 23 million consumers invest their life savings. With more than $5 trillion in assets under management, the bank has invested heavily in a click-to-compute private cloud infrastructure as a strategy to lower operating cost and become more agile in delivering new IT capabilities to the business. The problem? Its existing security and compliance solutions wouldn't scale at the same rate, taking months to provision and deploy. A new approach was needed.

The bank chose CloudPassage Halo as their agile security platform. Halo scales seamlessly, takes just minutes to deploy and gives the bank instant visibility into their private cloud infrastructure. Halo moves at the speed of the new IT organization, while providing continuous visibility, protection and compliance within a very dynamic cloud environment at the same time. CloudPassage Halo is now fully integrated into a click-to-compute model that offers seamless, automated scaling of IT resources within the bank.

ENABLING BUSINESS INNOVATION WITH CONFIDENCE

Modern compute models have become the clear catalyst for business growth and innovation. Instead of being left behind, CISOs and security teams need to find a way to say "YES" to elastic infrastructure in order to enable business success. CloudPassage Halo delivers agile security and empowers organizations to align with the goals and strategies of the business.

To learn more about how agile security from CloudPassage can help embrace elastic computing with confidence, visit www.cloudpassage.com or call 800-215-7404.

ABOUT CLOUDPASSAGE

CloudPassage® Halo® is the world's leading agile security platform that empowers enterprises to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Halo delivers a comprehensive set of continuous security and compliance functions right where it counts—at the workload. Halo orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center—even bare metal servers). Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility. Headquartered in San Francisco, CA, CloudPassage is backed by Benchmark Capital, Meritech Capital Partners, Tenaya Capital, Shasta Ventures, Musea Ventures and other leading investors.