Fidelis® Cybersecurity

WHITE PAPER

Achieving Complete Security and Compliance Visibility in Public Cloud Environments

Table of Contents

Introduction

The evolution of IaaS (Infrastructure as a Service) has resulted in a rapid shift of enterprise workloads to the cloud—a move which has introduced a new spectrum of challenges and requirements for security visibility. Both industry analysis and news on the causes of breaches and data loss in recent years have underscored the importance of achieving complete security visibility and compliance.

The same properties that make a dynamic cloud environment attractive to businesses add complexity to matters of security and compliance—a daunting challenge for quickly evolving, agile businesses, as well as those with legacy systems resistant to change. As outlined in our Five Nastiest Security Mistakes whitepaper, root causes are often traced back to simple oversights and errors which inadvertently expose core business and customer data.

These easily-overlooked problems can, unfortunately, translate into serious exposure and risk—both financial, and operational. Without the ability to rely on a perimeter as the first line of defense and with the increased speed and distribution of deployments, the need for visibility into the security and compliance across all objects has become more critical than ever.

As IaaS grows in adoption, cybersecurity professionals are increasingly realizing the complications involved. The very nature of distributed systems can make it difficult to obtain accurate and up-to-date visibility and inventory of cloud assets. Also, rapid growth across multiple environments can make it nearly impossible to consistently apply best practices for security and compliance. This paper will examine the challenges of security visibility in these environments and the characteristics of a successful solution.

Fidelis has built the Fidelis CloudPassage Halo® platform to help security teams deal with the challenges of cloud infrastructure, as well as maximize its benefits and opportunities. By optimizing and automating security visibility, it helps your team boost security defenses, streamline operations, and ensure compliance across your public cloud infrastructure.

Security Visibility is Mission-Critical

In today's business environment, the core value of many organizations lies in their digital footprint. Unauthorized access or damage to that infrastructure represents a significant risk to the business, and in many cases, compliance with security practices is a critical need to operate in the marketplace.

The most prominent breaches typically involve the loss of data. Even where there is no direct harm to business operations, potential repercussions to customers, partners, and the public add legal, compliance, and marketing risk to the direct impacts of an attack. When the needs of a business expand to require diverse methods of data access and storage, the risk of potential exposure increases. To manage business risk and protect customers, it is critical to maintain visibility into this rapidly changing landscape and its security posture.

Computational infrastructure is also important to understand and monitor. It represents the processes and activity of the business and can be an attractive target for hackers looking to subvert, damage, hold for ransom, or simply exploit for their own ends. The increasing scale and rate of change of this infrastructure presents challenges in maintaining visibility and preventing threats.

Compliance with regulatory standards is an essential requirement for many businesses. While an ever-expanding range of managed services reduces the need for custom infrastructure and speeds up development and deployment of projects, it also adds a broad and expanding range of infrastructure components—all of which require assessment and inspection. This presents unprecedented challenges, which must be addressed by a new approach to cloud security and compliance.

IaaS Creates a Challenging Technical Environment for Security Visibility

For the past two years, digital security threats have occupied two of the top five slots in the World Economic Forum's yearly Global Risks Report 2019.[1] While these concerns are not new, trends in digital transformation demand an accompanying security transformation. There are a number of challenges to achieve security visibility in cloud environments.

IaaS Creates a Challenging Technical Environment for Security Visibility

- Fast, dynamic infrastructure outruns traditional security techniques
- Challenges are as distributed as your system
- An expanding array of infrastructure components present net new security challenges
- The traditional tools of network security are no longer effective

Fast, dynamic infrastructure outruns traditional security techniques

Software-defined infrastructure creates a dynamic environment that accelerates deployment, agility, and scalability. Simply put, it's fast—and it's rapidly changing the way the world does business.

The benefits offered by this increase in speed and flexibility are immense, but automated deployment and infrastructure expansion also means less time for audit and review. Application infrastructure is not just deployed and scaled quickly, it also changes with increasing frequency as DevOps practices enable continuous deployment—with some organizations topping dozens of releases per day.

Traditional security techniques are no longer effective in an IaaS environment. To achieve agile security and maintain compliance visibility, a shift in approach is required.

Challenges are as distributed as your system

Transitioning to a cloud model enables faster operational and management changes, yet also removes the centralization of both infrastructure and IT management. There is value and flexibility inherent in infrastructure which can be scripted and coded, but this dynamic nature also drives the management of infrastructure closer to the individual teams that build it.

This results in a distribution of not only location but also of responsibility and power to make changes. Distribution of operations to individual teams means more points of control. At the same time infrastructure is increasingly distributed across more locations—across multiple cloud service accounts, multiple cloud service providers, or in combinations of public and private clouds and traditional data centers.

Both trends eliminate single points of control for security. The traditional perimeter is gone, as is the ability to find assets on a limited set of networks or get consolidated security and compliance visibility into them. The security model must shift as well, aligning with the advantages of cloud infrastructure and DevOps practices rather than being frustrated by them.

An expanding array of infrastructure components present net new security challenges

The shared responsibility model for the security of public cloud environments relieves some traditional security concerns in the data center, and it simultaneously adds complexity and net-new vulnerabilities in the management and configuration of IaaS accounts and assets.

Visibility into the security and compliance posture of cloud service accounts require continuous assessment of the state and settings of both the accounts and the diverse assets they contain. The scale and speed of an IaaS environment are vast when compared to traditional IT environments—which makes this extremely challenging.

This assessment itself needs to evolve as new types of services and technologies are added and new issues and best practices are discovered and developed. A diverse and expanding range of infrastructure components requires continuous assessment and inspection. For example, the use of containers and Kubernetes resolves operational issues but require a strategic approach to maintain security visibility. And serverless functions add operational agility, but require different techniques to secure.

The traditional tools of network security are no longer effective

Legacy security tools and appliances are not designed for the dynamic distributed virtual environments of the cloud. In a recent survey from AWS, 85% of respondents confirmed that legacy security solutions either don't work at all in their cloud environments or have only very limited functionality.[2]

Security Solution Checklist

Your ideal security solution should be:

Fast – Aligns with dynamic IaaS, automatic deployment and assessment

Scalable – Expands or contracts to meet shifting needs

Portable – Works across multiple IaaS providers and components

Integrated – Visibility mechanisms are part of the infrastructure

Continuous – Supports rate of change demands with continuous issue visibility

Comprehensive – Covers all critical aspects of both security and compliance

Actionable – Presents actionable security and compliance intelligence

Critical Characteristics of a Cloud Security Solution

Achieving security visibility requires comprehensive and continuous discovery and assessment of all assets. This helps an organization achieve two crucial goals—understanding and managing security risk, and achieving compliance. Cloud brings net-new challenges to security organizations, and also offers new opportunities. A properly designed security solution can benefit from the characteristics of both the cloud and DevOps processes to maintain more comprehensive security visibility with less manual effort.

What are the requirements to achieve that? The following are the characteristics of a security solution that will work effectively in the cloud, helping security teams leverage this transformation instead of being challenged by it.

Fast deployment and assessment

A successful security solution will match the speed of change in cloud environments. Cloud adoption is driven by the ability to represent infrastructure as code, aligning the creation and deployment of infrastructure with agile processes that have accelerated development and release of new software.

This trend creates security blind spots unless the security solution can deploy and assess at the same speed. It needs to integrate with deployment processes and continuously discover new infrastructure to provide timely security insight as soon as assets are deployed.

Scalable to transparently grow with the business

One of the great advantages of cloud environments is the ability to size infrastructure for current needs. This means that projects can be deployed without large upfront costs or risky predictions. Instead, they are deployed at a limited scale and designed to rapidly add resources as demand grows. Security solutions for these types of environments need to scale seamlessly and automatically.

To achieve scalability demands a model that automatically adds sensors to new assets and resources and invisibly grows security analytic capacity. Traditional security solutions need forethought and planning to provide the resources necessary to assess an environment of a certain size. To be successful in the cloud, a modern security solution must have the same transparent scaling properties of the cloud environments it protects.

Portable across providers and components

A recent survey by 451 Research noted that nearly 70% of organizations are moving towards a multi-cloud environment.[3] Modern environments often include multiple cloud providers, as well as on-premises virtualization. And within public cloud environments, the number of services and infrastructure components is expanding at a breakneck pace. A security solution must work within an organization's current infrastructure, and must also be portable across the providers and components it may use in the future.

To attain complete visibility and compliance in modern environments, a security solution needs to be portable across all IaaS providers and infrastructure types. It should be able to support changing trends in development and deployment, such as the move to containerization. In addition, as new managed offerings from cloud providers are adopted, the solution must continue to provide insight across the entire infrastructure.

Integrated into the infrastructure environment

Increasing complexity and rate of change mean that achieving security visibility cannot be an afterthought in cloud environments. To provide complete visibility, a security solution must be able to integrate into environments and infrastructure components so the security knowledge of the environment grows and changes as it does.

Integrating security sensors into the componentry and processes of the environment allows it to scale transparently and automatically up and down. This allows the reliable understanding of security posture over time, achieving visibility and compliance for even highly ephemeral assets. It also drives the automation of deployment and assessment necessary to handle a growing array of challenges with limited security personnel.

Continuous visibility and assessment

Without ongoing insight into your infrastructure, it's impossible to manage the security posture of a cloud environment. Because continuous discovery, inventory, and assessment are critical, effective automation of these needs in a dynamic IaaS environment is a must.

Automation relieves the burden of manual monitoring inherent in legacy systems—and drastically streamlines the security management of IaaS. This allows your organization to quickly and effectively mitigate risk, remediate issues, and maintain compliance, all while reducing burden to your IT security team. That is why continuous risk assessment and issue visibility supporting daily, hourly, and on-demand needs is critical.

Comprehensive evaluation of infrastructure components

As the speed and complexity of environments increases, an effective solution should help security teams consolidate and automate functionality. An increasingly broad array of infrastructure components offered by cloud providers need to be covered, and assets like servers and containers require in-depth analysis.

A successful security solution should have the depth to cover multiple types of controls, and the breadth to provide insight into an increasing array of components. All critical aspects of both security and compliance should be addressed—for each and every component of your cloud infrastructure. No stone should be left unturned!

Actionable results to drive remediation

The results a security solution produces must be actionable—not just in terms of their content, but in terms of how they are delivered. The intelligence generated needs to be presented to infrastructure operators "on their terms," in a way that's actionable as part of their standing workflow and which carries enough context to allow automated action.

The processes that enable organizations to move towards continuous delivery represent an opportunity to drive towards continuous remediation. This is only possible if the security solution can integrate into these processes, becoming a service used to not only rapidly assess security posture in testing and production but also provide consumable intelligence on changes that can make systems more secure.

Critical Characteristics of a Cloud Security Solution

- Fast deployment and assessment
- Scalable to transparently grow with the business
- Portable across providers and components
- Integrated into the infrastructure environment
- Continuous visibility and assessment
- Comprehensive evaluation of infrastructure components
- Actionable results to drive remediation

Fidelis Halo Addresses Critical Cloud Security Requirements

Enabling organizations to gain complete security visibility across their entire cloud infrastructure is why we've developed Fidelis Halo, a comprehensive security solution designed to address the challenges specific to cloud infrastructure. Fidelis Halo is purpose-built to address the key security and compliance requirements of IaaS. We help organizations take advantage of the opportunities inherent in IaaS—creating secure, comprehensive, and functional cloud programs that automate cloud security.

Deploys quickly, delivers value instantly

Fidelis Halo deploys simply and rapidly, quickly returning value and enabling it to maintain security and compliance visibility into changing cloud infrastructure. Onboarding is simple and fast, returning data on thousands of assets within minutes. That means our customers gain value from the platform immediately and can leverage the platform to further automate and increase productivity over time.

Highly scalable

Fidelis Halo is blazing fast and its architecture is highly scalable. Because it was built in the cloud as well as for the cloud, it fully leverages the ability to componentize operations, scaling elastically to handle any load. Integrated into an environment, it increases coverage invisibly, providing security visibility no matter how fast it grows.

Portable across multiple clouds

Fidelis Halo provides visibility across diverse infrastructures and is portable across multiple clouds including on-premise environments and private clouds.

Easily integrated into high-speed DevOps process

The Fidelis Halo platform offers opportunities to improve security maturity and increase value. By leveraging Fidelis Halo's strengths to integrate visibility mechanisms into the infrastructure componentry and processes, your team partners with DevOps to deploy, evaluate, and remediate and pushes left into the CICD pipeline to rapidly evaluate builds on code check-in.

Continuous security and compliance coverage

Once deployed, Fidelis Halo offers ongoing continuous coverage. A scalable distributed architecture makes it easy to manage various schedules, and stay current with infrastructure security and compliance posture. Users can configure scans to repeat at intervals that make sense for their business and aligning with a highly dynamic, changing cloud environment.

Comprehensive security visibility coverage for cloud infrastructure

Fidelis Halo offers comprehensive coverage, tracking, and evaluation of all infrastructure components in the cloud service plane. And it offers deeper insights into server/VM workloads and containers.

Actionable insight

The value of quality security and compliance visibility is limited if not translated into action. Fidelis Halo provides thorough details and metadata, clear remediation guidance, and actionable intelligence communicated to infrastructure operators as part of their standing workflow.

Fidelis Halo Addresses Critical Cloud Security Requirements

- Deploys quickly, delivers value instantly
- Highly scalable
- Portable across multiple clouds
- Easily integrated into high-speed DevOps process
- Continuous security and compliance coverage
- Comprehensive security visibility coverage for cloud infrastructure
- Actionable insight

Expand your Visibility, Fast and Free

The move to the cloud introduces new challenges and security concerns, and also opportunities to automate and integrate security best practices. Fidelis Halo helps security teams succeed in the cloud, providing complete and comprehensive security and compliance visibility across public cloud infrastructure.

Fidelis offers a free trial of the Fidelis Halo, allowing you to effortlessly assess your AWS and Azure cloud infrastructure for security and compliance issues. Set-up is quick and easy, and most cloud infrastructure environments can be fully assessed within fifteen minutes.

Your trial account can also be used to take a deep-dive into your server and container environments. Policy templates for standards like CIS Benchmarks, PCI, HIPAA, and ISO 27001/2 are included, so you can easily pinpoint potential problems. And Fidelis Halo doesn't just show you problems, it also provides detailed technical remediation advice for identified issues.

To review more advanced capabilities, use the Fidelis Halo REST API to try some DevSecOps style automation. See what's in the Fidelis Halo Toolbox for inspiration and "starter" code, and plug into the Fidelis Halo API SDK to make integrations go faster.

Learn More About Fidelis Halo

Register for a Fidelis Halo free trial:
https://www.cloudpassage.com/cloudpassage-halo-free-trial/

Check out the Fidelis Halo REST API:
https://api-doc.cloudpassage.com/help

See what's in the Fidelis Halo Toolbox:
https://cloudpassage.github.io/halo-toolbox/

Browse the Python SDK for Fidelis Halo:
https://github.com/cloudpassage/cloudpassage-halo-python-sdk

End Notes

[1] World Economic Forum's yearly Global Risks Report 2019:
https://www.weforum.org/reports/the-global-risks-report-2019

[2] 2019 AWS Cloud Security Report:
https://blog.cloudpassage.com/2019/08/14/2019-aws-security-report/

[3] 451 Research 69% of enterprises will have multi-cloud/hybrid IT environments by 2019:
https://451research.com/images/Marketing/press_releases/Pre_Re-Invent_2018_press_release_final_11_22.pdf

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**