# Contents

Foreword ....................................................................................................................................................................5
Letter from the Co-Chairs...........................................................................................................................................6
Acknowledgments ......................................................................................................................................................7
1.0 Introduction..........................................................................................................................................................8
   1.1 Intended Audience .......................................................................................................................................8
   1.2 Scope ...........................................................................................................................................................8
      1.2.1 Functional Areas Covered..................................................................................................................9
      1.2.2 Cloud-Delivered Versus Traditional Intrusion Services .................................................................9
      1.2.3 Related SecaaS Categories and Guidance .........................................................................................9
2.0 Requirements Addressed .................................................................................................................................. 10
   2.1 Intrusion Detection and Response ................................................................................................................ 10
      2.1.1 Techniques and Strategies................................................................................................................ 10
      2.1.2 Correlation and Response ................................................................................................................ 12
   2.2 Intrusion Management.................................................................................................................................. 12
      2.2.1 Element Management and Incident Reporting ................................................................................. 13
      2.2.2 Infrastructure for IM SecaaS............................................................................................................. 13
      2.2.3 Service Standards and Functions...................................................................................................... 13
   2.3 Service Levels and Business Model Requirements........................................................................................ 13
3.0 Considerations and Concerns............................................................................................................................ 15
   3.1 Considerations............................................................................................................................................... 15
      3.1.1 Service Level Agreement Language.................................................................................................... 15
      3.1.2 Financial Considerations.................................................................................................................... 15
      3.1.3 Technical Considerations.................................................................................................................. 15
      3.1.4 Architecture Considerations............................................................................................................. 15
      3.1.5 Security Considerations.................................................................................................................... 16
   3.2 Concerns........................................................................................................................................................ 16
      3.2.1 Gaps with the Provider Solution........................................................................................................ 16
      3.2.2 Integration Concerns........................................................................................................................ 16
      3.2.3 Environmental and Security Concerns ............................................................................................. 17
3.2.4 Technical Performance Concerns

3.2.5 General Challenges

3.2.6 Specific to Cloud Consumers

3.2.7 Specific to Cloud Service Providers

4.0 Implementation

4.1 Architectural Overview

4.1.1 Intrusion Detection Framework

4.1.2 Intrusion Detection and Protection Architecture

4.1.3 Network-Based Detection

4.1.4 Virtualization Layer Detection

4.1.5 Client-Based Detection

4.1.6 Application Layer Detection

4.1.7 Hybrid Solutions

4.2 Cloud-Provided IM SecaaS Implementation

5.0 References and Useful Links

5.1 References

5.2 Useful Links
Foreword

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information.

Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change.

One mission of the Cloud Security Alliance is to provide education on the uses of Cloud Computing to help secure all other forms of computing. To aid both cloud customers and cloud providers, the CSA SecaaS Working Group is providing Implementation Guidance for each category of Security as a Service, as delineated in the CSA’s SecaaS Defined Categories of Service. Security as a Service was added, as Domain 14, to version 3 of the CSA Guidance.

Cloud Security Alliance SecaaS Implementation Guidance documents are available at https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/.

We encourage you to download and review all of our flagship research at http://www.cloudsecurityalliance.org.

Best regards,

Jerry Archer   Alan Boehme   Dave Cullinane
Nils Puhlmann   Paul Kurtz   Jim Reavis

The Cloud Security Alliance Board of Directors
Letter from the Co-Chairs

Security as a Service is a specialized area categorized two years ago as growing rapidly and in unbound patterns. Vendors were struggling. Consumers were struggling. Each offering had its own path. We felt it was urgent to address the needs and concerns common to the implementation of Security as a Service in its many forms.

The Defined Categories of Service helped clarify the functionalities expected from each Category. In this series, we hope to better define best practices in the design, development, assessment and implementation of today’s offerings.

We want to thank all of the many contributors worldwide who have worked so hard to produce these papers providing guidance for best practices in Cloud Computing Security. Many have been with the Security as a Service Working Group since the beginning; many others joined in this effort. Each has spent countless hours considering, clarifying, writing and/or editing these papers. We hope they help move forward toward those unimagined innovations.

Sincerely,

Kevin Fielder and Cameron Smith
SecaaS Working Group Co-Chairs
Acknowledgments

Chair

Tim Owen, Secure Mission Solutions

Contributors

Girish Bhat, Wave Systems
Phil Cox, Rightscale
Robert Gutcho, Symantec
Bernd Jäger, Colt

Peer Reviewers

Jim Brigham, EMC/RSA
Justin Forster, Trend Micro
John Linn, EMC/RSA
Jean Pawluk
Robert Polansky, EMC/RSA
Said Tabet, EMC/RSA

CSA Global Staff

Aaron Alva, Research Intern
Vicki Hahn, Technical Writer/Editor
Luciano JR Santos, Research Director
Kendall Scoboria, Graphic Designer
Evan Scoboria, Webmaster
John Yeoh, Research Analyst
1.0 Introduction

The methods of intrusion detection, prevention and response in physical environments have matured over the last decade. However, the growth of virtualization and massive multi-tenancy is creating new targets for intrusion due to the complexity of access and difficulty in monitoring all interconnecting points between systems, containers, applications, and data sets. This raises many questions about the appropriate infrastructure, processes, and strategy for enacting detection and response to intrusion in a cloud environment, or even in a traditional environment with intrusion management services delivered via the cloud.

As if the difficulty of employing intrusion capabilities in the traditional enterprise were not enough, limitations on visibility, complexity caused by architectural incongruity, and complications such as encryption, data access and format, and multiple administrative boundaries make for even more difficult choices and reduced ability to deliver the service in a highly virtualized environment, or from a cloud to protect a traditional environment.

Because of the limited market maturity and lack of widely accepted best practices, this document provides implementation guidelines for cloud-based intrusion management service of multiple flavors—in the cloud, through the cloud, or from the cloud—focusing on the basic tenets of service and architecture rather than solutions. Its intent is to describe the functional areas of any IM SecaaS service, critical elements for effective delivery, and options for deployment, along with the minimum standards necessary to integrate those services successfully within the larger SecaaS model and security architecture framework.

While further development of standards are ongoing, these instruction sets and guidelines are designed to ensure that the basis for a service are defined sufficiently so that service providers, third-party solutions providers, and consumers are clearly in synch when crafting contract and service level language or ordering and executing the service.

1.1 Intended Audience

The intended audience is the gamut of IT professionals considering cloud-based security services. However, the bulk of the material contained herein is written with a technical audience in mind—engineers, implementers, operators, technical assessors of planned and implemented offerings, and the technical representatives of consumers of the services and functions.

1.2 Scope

This guidance covers the requirements and capabilities, considerations and concerns, and implementation criteria of cloud-provided Intrusion Detection, Response, and Management services. The material is designed to ensure all three potential perspectives are considered and that the standards are translatable to the requirements of each participant in the service. The content is also presented from the context of providing the service from a cloud, through a cloud, or with cloud enhanced capabilities. This guidance does not specifically address complete architectures, although they must be modeled to some degree in order to provide sufficient backdrop to describe implementation strategies and functional standards.
1.2.1 Functional Areas Covered

Detailed in following sections, the main functional areas covered by this guide include the standard functions and practices required to manage:

- Intrusion Detection through:
  - Network Traffic Inspection, Behavioral Analysis, and Flow Analysis,
  - Operating System, Virtualization Layer, and Host Process Events,
  - Application Layer Events, and
  - Correlation Techniques, and other Distributed and Cloud-Based Capabilities.

- Intrusion Response using:
  - Automatic, Manual, or Hybrid Mechanisms, and/or

- Intrusion Management Service Infrastructure, including:
  - Detection and Response Architectures and Design Requirements,
  - Intrusion Management Service Components,
  - Application, process, and data requirements,
  - Skills and Training, and
  - Governance, Regulatory, and Compliance Issues (data privacy)

1.2.2 Cloud-Delivered Versus Traditional Intrusion Services

The content is focused on describing parallels and distinctions between cloud-delivered versus traditional enterprise intrusion capabilities, drawing attention to the requirements, standards, options, and considerations for how to deploy such services to various target environments (IaaS, PaaS, SaaS). Likewise, given the fundamental assumption that a provider environment must first be secured before effectively delivering Security as a Service to another environment, nuances in requirements for delivery across the various configurations (provider cloud, third-party, private and on-site cloud, or non-cloud) are also detailed. In the end, there are no unifying architectures or generalized standards to convey, but unifying principles and generalized qualifications and strategies are depicted.

1.2.3 Related SecaaS Categories and Guidance

In order to keep content focused on cloud-delivered Intrusion Management Services—the infrastructure required to identify and respond to potential intrusion, delivered in the cloud, through the cloud, or from the cloud—this guidance does not cover specific algorithms or techniques of intrusion detection, or specific methods of intrusion prevention. Some facets of Intrusion Management (IM), like Infrastructure Protection and Resiliency, are more detailed in SecaaS Category 10 Network Security. This guidance does not address the management of security events or correlation (covered more in depth in SecaaS Category 7 Security Incident and Event Management [SIEM]) other than the control and process for security architecture response and adaption and the need for SIEM integration and interfaces for input/output to other SecaaS services such as Category 3 Web Security.
2.0 Requirements Addressed

In order to offer guidance and minimum requirements to cover the gamut of potential offerings and capabilities, a clear depiction of the requirements to be met or problems to be solved must be presented first. This section addresses the purpose of intrusion detection, response, and management; the functional areas, components, and capabilities used to meet those requirements; the complexities of various target environments; as well as the nuances for delivering the services in the cloud, through the cloud, and from the cloud.

2.1 Intrusion Detection and Response

The purpose of intrusion detection and response is to monitor the enterprise environment at key vantage points to uncover malicious activity aimed at degradation, disruption, infection, or exfiltration of data, applications, and the systems that host or transmit them, and then respond in some way to avoid, block, contain, disrupt, or continue to operate in the face of attack. A comprehensive intrusion service combines detection and response, management infrastructure for control and reporting, and interfaces to the rest of the security architecture in order to have a more holistic view of events and better uncover anomalous activity. Regardless of comprehensiveness, Intrusion Services are offered at varying service levels and with certain criteria, administrative agreements, reaction aggressiveness, and automation.

Intrusion detection/response elements are employed at opportune cross-connects or shared points, where protected and foreign traffic cross paths: a network administrative boundary, end system network interfaces, within hosts at virtualized container boundaries, or directly inside a guest environment. To manage the protection of hosts, applications, and data, an Intrusion Service must have control of, or at least visibility into, these points of interest; interface with information and event correlation capabilities; and provide the infrastructure for communications in and among the components of the service within the target enterprise, as well as back to the intrusion service provider environment. Delivering this capability from the cloud often requires administrative relationships, elevated user rights, and end to end transactional access between hosted elements and central control and reporting.

2.1.1 Techniques and Strategies

There are two flavors of detection techniques: network- or traffic-based (looking for binary or behavioral patterns and anomalous activity in network traffic) detection, and system event-based (looking for activity or events on the host at the system, virtual, and application layers) detection. Network-based techniques employ strategies for signature detection, behavior heuristics, and traffic pattern correlation and can be deployed using existing network equipment, specialized appliances and interfaces, or software that runs on the host. Event-based techniques employ access to or reporting of events and configurations to determine potential activity leading to or resulting from malicious attack, compromise, or resultant degradation, corruption, or exfiltration.

2.1.1.1 Network-based Intrusion Detection/Prevention (IDP)
The most common tactics for network intrusion detection and prevention are signatures, Network Behavior Analysis (NBA) or traffic analysis, and protocol analysis or heuristics. Each of these relies on some form of deep packet inspection (DPI): the ability of the detection device or software to understand various headers and components of network datagrams. Scanning techniques that either match data patterns against known signatures, behavior patterns against known attack vectors, or just the opposite—behavior inconsistent with the protocol supposedly being used—can occur in software (using cache space or volatile memory) or hardware. More aggressive techniques of “fingerprinting,” reverse engineering, “black box” and “white box” algorithms continue to advance and take advantage of offline or parallelized processes, more efficient memory conventions, and hardware acceleration.

2.1.1.2 Host, Virtual Layer, and System-Based Detection

Detecting potentially anomalous behavior or the resultant data loss, infection, or degraded or denied service on a system at various levels is the second technique for IDP. In this solution, events are detected through analysis of centrally reported logs or by software running directly on the system, in the virtual layer, or in the guest OS monitor for particular behaviors that indicate potential intrusion: policy violations, changes in configuration, workload changes, foreign processes or system calls, changes to the integrity of the OS and file systems, etc. Protections are often in the form of manual patches, updates, and other remediation, but for resident software, the option to do some forms of automatic remediation is also possible.

2.1.1.3 Complexities by Target Environment

Differences in the target environment—whether it is traditional, cloud, or hybrid in architecture; if it is in someone else’s cloud; and what type of cloud it is—have tremendous impact on the available functions and features of the delivered service. Moreover, delivering the solution from the cloud or a third party provider adds additional administrative and tactical complexity.

In a virtualized environment, event-based detection requires more visibility at more layers in the system. When that environment moves more to a multi-tenant cloud (where guest applications and data are also in different administrative or security boundaries or data remnants are an issue), additional complexities such as cloud APIs, guest process interactions, and the management plane are introduced. In these cases, some specific events or checks might include:

- Virtualization Layer (VMM/Hypervisor) events,
- VM Image Repository Monitoring,
- Integrity Monitoring VMM/Hypervisor (Hardware, Firmware, Software),
- Changes to the Management Plane,
- Interaction between Guest containers or interdependent workloads, and/or
- Cloud and other API activity.

Network-based detection in a cloud environment, on the other hand, can be much more arduous to deploy depending on the available resources in that cloud and the level of management or control of the devices,
services or configurations required. The table below depicts some of the potential network-based detection elements available by cloud type.

<table>
<thead>
<tr>
<th>Intrusion Detection Options</th>
<th>Cloud Service Provider</th>
<th>Cloud Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS</td>
<td>PaaS</td>
</tr>
<tr>
<td>Physical</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMM/Hypervisor vSwitch Introspection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMM/Hypervisor Monitoring/Integrity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Appliance (Routing)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Host-Based (Network or System)</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>3rd Party Service (Route Traffic Through)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 1: Intrusion Detection Options in Target Cloud Environments

1. Depends on the PaaS framework and the type of instance
2. Depends on the PaaS instance type

2.1.2 Correlation and Response

Response to suspected intrusion can range from manual configuration changes or system and software patches to automated blocking, redirecting, and even network-level reconfiguration and resiliency. What levels and specific capabilities are available in the target environment or delivered in, through, or from the cloud is dependent on the architecture as well as the administrative agreements between provider, third-party, and consumer. The authority to respond may reside in part with each of the parties in the service offering, much like the responsibility and capability for correlation.

Correlation, however automated, also depends on the administrative and security requirements of the participants in that appropriate data feeds and protocols are configured to allow communications between the central system and the devices and software that have the individual visibility into the environment. Crossing network and system boundaries such as firewalls and IDPs to get to the appropriate data is also necessary in implementing the service. In most cases, requirements are identified in the Service Level Agreement (SLA) to establish the connections, or to indicate the quality and comprehensiveness of the resultant service.

2.2 Intrusion Management

The second functional area of Intrusion SecaaS is Intrusion Management. This is the implementation of a managed capability to control and dynamically adapt intrusion detection configurations and policies, or enact response within the context. It should not be confused with a security information and event monitor (SIEM), though any level of intrusion SecaaS will interface and interact with SIEM. The primary facets of IM are element management (administering the individual detection and response components), processes for determining and
executing detection or response tactics (signatures, configurations, policies, etc.), the infrastructure for deploying intrusion architecture and protection services (including reporting and alerting), and the interfaces to other services.

### 2.2.1 Element Management and Incident Reporting

System administration of the individual devices and software is the responsibility of the owner of the device or as otherwise agreed to in the SA/SLA. At a minimum, enable central reporting or export of logs of events and alerts (either to the provider or the SIEM service), which may include protocol, data format, and administrative management of the device.

### 2.2.2 Infrastructure for IM SecaaS

Intrusion Management infrastructure would include the appropriate network, system, and software configurations to support the transmission, access, and organization of data elements in order to support the following:

- Central Reporting of events and alerts (either to the provider or the SIEM service),
- SIEM Integration,
- Administrator Notification for issues with service elements,
- Customization of Policy (automatic or manual) and other configurations,
- Mapping to Cloud-layer Tenancy (both in deployment as well as management and reporting),
- Cloud Sourcing Information to reduce false positives and improve coverage, and
- Remote Storage or Transmission of integrity information, to prevent local evasion.

The infrastructure (the data systems communicating over the network with the elements), should plan for the implications if network connectivity is hampered, and how it impacts alerting and reporting as well as access to protection systems. The inability to control devices remotely during an attack or in the event of outage may be significant.

### 2.2.3 Service Standards and Functions

As part of the service functionality, additional measures may be required to account for structural and policy division between virtualized containers, multi-tenant and guest access, as well as processes and data management standards for ensuring proper format and flow of information in and among service constituents. These policies and functions should be meshed appropriately to interface with SIEM systems, web security solutions, network security architectures, and security assessment tools and techniques. For the purpose of framing the overall IM solution, care should be taken in developing or procuring a service to ensure these features and functions have been addressed.

### 2.3 Service Levels and Business Model Requirements

In addition to the technical and functional requirements outlined above, this guidance addresses the business requirements for effectively planning, implementing, and procuring an Intrusion Management service. Necessary to implement, maintain, and mature a cost-effective cloud-delivered IM solution, the guidance
includes treatment of the skills and capabilities required to complement the technology and processes that make up the functional areas of the Intrusion Management Service (IMS).

Understanding the relevant IMS requirements and choosing the right deployment model (and provider) is also a challenging and potentially costly task. Therefore, this guide also provides the customer perspective of what is required to procure, implement, and integrate a cloud-delivered IM solution, including:

- **Basic understanding regarding the specific problems to solve with key considerations for implementation strategy, namely:**
  - Technical, architectural,
  - Functional, procedural, and
  - Logistical, financial, legal context.

- **Best practices, common pitfalls regarding:**
  - Intrusion Detection and Prevention strategies,
  - Implementation and Sustainment, and
  - Integration with Security Architecture, tools, and management systems.

- **Business case evaluation criteria to help:**
  - Evaluate and compare cost models and strategies,
  - Choose an appropriate service provider, offering, and features, and
  - Define Performance and Security Service Level Agreements (SLAs/SSLAs).
3.0 Considerations and Concerns

3.1 Considerations

As a consumer of IM SecaaS, identify that interfaces or mechanisms are available to get events into and out of
the service, as well as how reporting will be done. Providers will need to identify and document all the different
ways that they support getting data into their service.

If the IM SecaaS already has the consumer’s cloud providers as an integration point, this could significantly
increase the speed of deployment and likelihood of success.

3.1.1 Service Level Agreement Language

For the Service Level Agreement (SLA), the consumer needs to ensure that the terms in the SLA are consistent
with, and meet the requirements of, its information security policy (and likely its Incident Response Policy), as
well as any operational requirements that have been defined. Currently, the language in most SLA contracts is
very favorable to the provider, and consumers should require that IM providers have ways to meet their
business requirements; they should not change their business requirements to meet what the IM provider can
deliver. The consumer should ensure the following items are covered in the SLA, at a minimum:

- Performance requirements
- Bandwidth requirements
- Detection and protection requirements
- Packet management responsibilities

IM SecaaS providers should have the ability to enter into custom SLAs that are achievable for them. They should
not expect all clients to fit a cookie cutter approach.

3.1.2 Financial Considerations

Cost of “bandwidth” for getting events into the IM SecaaS should not be overlooked and could be considerable,
depending on the sources of information that are included.

3.1.3 Technical Considerations

- Are the events/alerts that are sent from IM SecaaS to consumer sent in a standard format? Is the
  format proprietary? Consider if vendor lock-in could be a concern.
- What about short lived instances? Host Intrusion Detections System (HIDS) and Host Intrusion
  Prevention System (HIPS) logs can be lost.

3.1.4 Architecture Considerations
• What happens to events if communication links are unavailable or faulty? Is there buffering of events to/from IM SecaaS?
• Lack of virtual SPAN ports in public cloud providers for typical deployment of a Network Intrusion Detections System (NIDS) or Network Behavior Analysis (NBA).
• Lack of network-edge TAP interfaces for public cloud and virtual private cloud for typical deployment of NIPS.
• Inability to utilize hypervisor (vSwitch/vNIC) introspection.
• Latency, resiliency and bandwidth concerns with proxying network traffic through virtual appliances or third-party services.
• If the environment is IPv6-enabled, this may cause an increase in log file size due to large addresses and may require third-party tools or applications to be IPv6 compliant in order to properly exchange information with end systems.

3.1.5 Security Considerations

• How is the information communicated in a secure manner? Consider getting info from IM SecaaS as well as getting data into the IM service.
• Proliferation of SSL required by deployment in public clouds adds complexity or may block visibility to network-based IDS/IPS, and thus the data available to the IM SecaaS.
• Who manages the correlation rules?

3.2 Concerns

An IM SecaaS provider should be able to answer each of the concerns listed below and provide reasonable attestation that the answers are true.

3.2.1 Gaps with the Provider Solution

While a consumer can export everything it needs to the IM SecaaS, its provider (IaaS/PaaS/SaaS) may not. The consumer will need to identify what gaps exist in the information that will be needed for a fully functional Intrusion Management system and work with its cloud providers to get them outside of the IM SecaaS.

This problem could occur if the cloud provider will not share the information, or the Cloud Provider does not have the technical capability to share the needed information. In either case, a gap plan must be developed and implemented.

3.2.2 Integration Concerns

Consumers should ensure that they are able to consume the information provided by the IM SecaaS in a manner that will meet the business needs defined. Consumers should perform due diligence on the IM SecaaS provider to identify if the provider appears to be using industry standard/accepted practices.
A major concern for IM and Cloud Services is the inability of the IM SecaaS to get data from IaaS/PaaS/SaaS cloud service providers. This information will be critical to a successful Incident Management program at the consumer. Partnerships likely will be an important vehicle for this in the short term.

3.2.3 Environmental and Security Concerns

Anything of a sensitive nature that should be filtered out before sending to IM SecaaS should be identified.

Some of the major concerns surrounding IM SecaaS deal with the security of the actual IM SecaaS provider’s service, as well as the data going into and out of it. Consumers should understand the technical specifics of when and where the data they give to the IM SecaaS is unencrypted. Consumers should know what type of access the IM SecaaS has to the data that is provided to them as well as who within the IM SecaaS provider has access, or potential access, to the unencrypted data.

There is a concern surrounding the separation of logs when in multi-tenancy environments at the IM SecaaS. How does the provider ensure proper segmentation?

3.2.4 Technical Performance Concerns

How does the IM SecaaS identify “dropped” or “missed” packets? Will the IM SecaaS be watching for sources that drop off line or become unresponsive, or will it be the consumer? This should be addressed in the SLA.

3.2.5 General Challenges

- Proliferation of SSL required by deployment in public clouds adds complexity or blocks visibility to network-based IDS/IPS
- Complexity and immaturity of Intrusion Management for APIs
- Lack of tools to manage instance-to-instance relationships

3.2.6 Specific to Cloud Consumers

- Lack of virtual SPAN ports in public cloud providers for typical deployment of NIDS or NBA
- Lack of network-edge TAP interfaces for public cloud and virtual private cloud for typical deployment of NIPS
- Inability to utilize hypervisor (vSwitch/vNIC) introspection
- Latency, resiliency and bandwidth concerns with proxying network traffic through virtual appliances or 3rd party services
- Privacy concerns of service-based security
- Short lived instances (HIDS/HIPS logs can be lost)
- Performance limitations with network traffic in a shared environment

3.2.7 Specific to Cloud Service Providers
• Policy management in a multi-tenant environment
• Policy management for application-layer multi-tenancy (SaaS, some PaaS services)
• Complexity of deployment and configuration in large cloud environments
4.0 Implementation

This implementation guidance covers the process, conventions, constraints, and architectural options for intrusion detection, response, and management as a cloud-delivered service. The elements and advantages and disadvantages to various approaches are also discussed to help develop (or procure) standardized service offerings in the areas of network-based or traffic-inspection detection and response, host-based or event-driven detection and response, and intrusion management service delivery.

Because this is an area of rapid technological development, the implementation guidance in this section focuses on current best practice using capabilities that exist at the time of writing. While future versions may further explore nascent capabilities, it is not in the scope of this document to discuss speculative or forward-looking approaches.

Additionally, guidance on developing and deploying service components such as reporting and data structure, SIEM integration or interfaces, multi-tenancy mapping, and incorporation of nascent algorithms and capabilities that enhance the service offering as well as the Governance, Regulatory, and Compliance and other issues (data privacy) that constrain it.

4.1 Architectural Overview

Intrusion detection is a combination of network traffic inspection using heuristics, signature detection, and other anomalous algorithms, and a conglomeration of investigation and correlation of information about the state of systems, applications, and user activity. Intrusion response to perceived threat ranges from manual interventions to autonomic and self-healing actions at the network, system, virtual, and application layers. Intrusion Management also requires an infrastructure whereby the elements of the solution can be managed, algorithms and signature portfolios can be centrally or distributively controlled, algorithms and computing capabilities can be orchestrated, data and reporting can flow to appropriate collectors, and interfaces to/from other facets of the security architecture (Web Security, SIEM, Network Security, etc.) are supported.

4.1.1 Intrusion Detection Framework

Because there are so many advances being made in physical, logical, and topological data and application architectures, it is impossible to define a single architecture for deploying an intrusion management system, and therefore, for the purpose of guidance, the following sections introduce various options for elements of the intrusion detection architecture.

4.1.1.1 Network-Based Intrusion Detection/Prevention (IDP)

The most common tactics for network intrusion detection or prevention are signatures, Network Behavior Analysis (NBA) or traffic analysis, and protocol analysis or heuristics. Each of these relies on some form of deep packet inspection (DPI): the ability of the detection device or software to understand various headers and components of network datagrams. Scanning techniques that either match data patterns against known
signatures, behavior patterns against known attack vectors, or just the opposite—behavior inconsistent with the protocol supposedly being used—can occur in software (using cache space or volatile memory) or hardware. More aggressive techniques of “fingerprinting,” reverse engineering, “black box” and “white box” algorithms continue to advance and take advantage of offline or parallelized processes, more efficient memory conventions, and hardware acceleration.

Strategically, network-based detection (and prevention) can be deployed on many types of network-aware equipment through hardware, software, even information reporting techniques. Network-based IDP relies on visibility into the raw packets and seeks to identify (and respond to) anomalous or malicious behavior or content found within network traffic—activity flowing to/from systems—as opposed to behavior or processes within an end system. IDP can be incorporated into or use information from existing network components (firewalls, routers, switches, sometimes even if the elements are virtual) or be deployed as an appliance (NIDS/NIPS). IDS can be passive, capturing traffic through a network TAP or spanned port off a network element for analysis only, or it can be placed in line to provide response.

Many firewalls and routers (with firewall software) offer pre-configured detection (usually referred to as “algorithms,” “ALGs,” or “screens”) that monitor activity on specific attack vectors (such as DDOS) or behaviors of particular applications/protocols (e.g. web, email, and session protocols like Voice over IP [VoIP]) with optional automatic protections to block. Most vendors of IDP-enabled devices, gateways, or NIPS/NIDS also offer subscription-based services of traditional black/white list variety as well as central or cloud-based signature updates, heuristics, and advanced algorithms.

NBA can also be an information-only solution whereby the network-aware devices in the enterprise report statistical information about traffic flows, which can then be correlated to identify attacks, suspicious activities, or other anomalous behavior. The central analysis can then optionally be used to manually update configurations or even modify the network routing and protection architecture through distribution of “rules” through a protocol known as BGP-FLOWSPEC. This enables hybrids of automatic and human-intervened changes to the environment to block, sink, or redirect suspicious traffic to devices or “scrub centers” in order to further analyze, intervene, or even inject countermeasures.

**4.1.1.2 Host, Virtual Layer, and System-Based Detection**

Host-based Intrusion Prevention/Detection (HIPS/HIDS) software installed on a host (or in a guest virtual container) operating system that monitors traffic for suspicious activity. HIPS is also generally bundled with firewall, policy enforcement, system event detection, software and system configuration control or reporting, and other host process capabilities. Detecting potentially anomalous behavior or the resultant data loss, infection, or degraded or denied service on a system at various levels is a technique used for IDP. In this solution, events are detected through analysis of centrally reported logs or by software running directly on the system, in the virtual layer, or in the guest OS monitor. Events are examined for particular behaviors that indicate potential intrusion: policy violations, changes in configuration, workload changes, foreign processes or system calls, changes to the integrity of the OS and file systems, etc. Protections are often in the form of manual patches, updates, and other remediation, but for resident software, the option to do some forms of automatic remediation is also possible.
4.1.1.3 Complexities by Target Environment

Differences in the target environment, whether it is traditional, cloud, or hybrid if it is in someone else’s cloud, and what type of cloud it is have tremendous impact on the available functions and features of the delivered service, much of which is described or implied above. Moreover, delivering the solution from the cloud or a third-party provider adds additional administrative and tactical complexity.

In a virtualized environment, event-based detection requires more visibility at more layers in the system. When that environment moves more to a multi-tenant cloud (where guest applications and data are also in different administrative or security boundaries or data remnants are an issue), additional complexities such as cloud APIs, guest process interactions, and the management plane are introduced. In these cases, some specific events or checks might include:

- Virtualization Layer (VMM/Hypervisor) events
- VM Image Repository Monitoring
- Integrity Monitoring VMM/Hypervisor (Hardware, Firmware, Software)
- Changes to the Management Plane
- Interaction between Guest containers or interdependent workloads
- Cloud and other API activity

Network-based detection to a cloud environment, on the other hand, can be much more arduous to deploy depending on the available resources in that cloud and the level of management or control of the devices, services or configurations required. The table below depicts some of the potential network-based detection elements available by cloud type.

<table>
<thead>
<tr>
<th>intrusion detection options</th>
<th>Cloud Service Provider</th>
<th>Cloud Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS</td>
<td>PaaS</td>
</tr>
<tr>
<td>Physical</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMM/Hypervisor vSwitch Introspection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMM/Hypervisor Monitoring/Integrity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Appliance (Routing)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Host-Based (Network or System)</td>
<td>No</td>
<td>Maybe²</td>
</tr>
<tr>
<td>3rd Party Service (Route Traffic Through)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 2: Intrusion Detection Options in Target Cloud Environments

¹ Depends on the PaaS framework and the type of instance
² Depends on the PaaS instance type

4.1.2 Intrusion Detection and Protection Architecture
Traditionally, the most prominent vehicles employed today for Intrusion Detection are various flavors of network traffic inspection (deep packet inspection, behavior analysis, and flow analysis). Architecturally, effective traffic- or network-based detection approaches seek visibility in crucial points where traffic shares a link or crosses borders between trusted and foreign zones, administratively controlled or data classification and security perimeters, or system or container boundaries. Proper placement and the ability to protect applications and data depend heavily on the physical and logical architecture within which inspection is deployed, or on access to the reported information from those systems. In some cases this can be done using a network-based appliance (whether in-line or port-mirrored off a physical or virtual switch) or as a client on a system that inspects traffic crossing the physical network interface. In other cases intrusion is detected by virtual layer solutions, separate software clients running on the host or in each guest OS, or solutions that monitor the application behavior.

4.1.3 Network-Based Detection

Recently, virtualization vendors added mirror port capabilities to their virtual switch products. If you have to support network traffic capture within a virtualized network, the most feasible way today is probably using a “sniffer” port on your virtual switch or “trunking out” the relevant traffic. If you want to implement this, you should ensure your virtual switch and your solution design supports it.

Intrusion detection and prevention systems can either inspect traffic by listening on a mirror port or as an inline device, “bridging” traffic and actively responding by blocking identified attacks. This leads into a variety of different deployment scenarios described below.

![Figure 1: Virtual Appliance Deployment](image)
Figure 1 shows a typical in-line IPS deployment, utilizing a virtual appliance.

Advantages:
- Easy deployment
- Interception of encrypted traffic via “Man-in-the-middle” theoretically possible

Disadvantages:
- As a software instance, the virtual appliance cannot use hardware support (ASICs) like today’s dedicated appliances
- High load on the IPS appliance will impact virtual machines or the host
- If the hypervisor is compromised, the IPS cannot be trusted
- If you “lose” the virtual appliance, your VMs will be cut off from the network as automatic “fail-open” hardware is not available

Figure 2: External, Physical IDS deployment

The deployment in Figure 2 uses a mirror port on a virtual switch, but traffic inspection is done by an external, physical IDS appliance.

Advantages:
- IDS is independent from hypervisor
High loads on the sniffer may have less impact on virtual machines or the host when compared to the above virtual appliance approach.

Disadvantages:

- Not all vSwitches support mirror ports
- Dedicated sniffer hardware and precious physical NIC required
- Potential scalability issues

Figure 3: Physical In-line IPS Deployment

Traditional IPS appliances can handle multiple physical network segments and VLANs. The deployment in Figure 3 trunks out all VM traffic to a physical switch. An external IPS appliance inspects and bridges all network segments.

Advantages:

- IDS independent from hypervisor
- High loads on the sniffer may have less impact on virtual machines or the host when compared to the virtual appliance approach
- Automatic “Fail-Close” mechanism available
- Supported by all virtual switches
- Interception of encrypted traffic via “man-in-the-middle” theoretically possible (for IPS)

Disadvantages:

- Most hardware intensive solution. Dedicated IPS hardware and precious physical NICs required
- Potential scalability issues (depending on the size of the cloud deployment, traffic, latency requirements as well as your own risk- and business requirement assessment)

To tap into “all” communication channels within a virtualized environment, pay attention to specific interfaces that might allow direct communication between entities like VMs, bypassing all network interfaces (virtual and physical). An example would be the “Virtual Machine Communication Interface” VMCI for the VMware hypervisor. As these interfaces typically increase the attack surface, you might want to disable them if not required.

Think about what you capture and record in a virtual environment: If you sniff on a vMotion network you might see (and store somewhere temporarily for investigation) sensitive information like clear text passwords or keys, or credit card numbers, etc., as they are included within the VMs’ RAM being transferred in clear text.

4.1.4 Virtualization Layer Detection

Virtualization Layer defense needs to address two areas:

1) Using the virtualization layer for detection/protection (i.e., utilizing APIs), and
2) Detecting and protecting against events specifically targeting the virtualization layer.

4.1.4.1 Using the Virtualization Layer for Detection and Protection

Forwarding all traffic to external interfaces for inspection (sometimes called “slowpath”) might not be feasible or scalable. To inspect traffic within the virtualization layer (i.e., direct VM-to-VM communication via RAM not using a switch) APIs provided by this layer must be used.

It is helpful to for detection and protection to have additional information on the current VM status or configuration data, including guest information like OS or patch level that could be obtained via introspection.

A high-level example architecture is shown below:
This type of integration allows inspection/blocking of guest events, offline VMs and “on-demand” and “on-access” scanning of virtual disks

Advantages:

- Easy deployment
- Interception of VM-to-VM communication
- Interception of guest operations
- Allows inspection of offline VMs
- Usage of additional configuration and status information

Disadvantages:

- A software instance cannot use hardware support (ASICs) like today’s dedicated IPS appliances
- High load on the IPS modules will impact virtual machines or the host performance
- If the hypervisor is compromised, the IPS cannot be trusted

4.1.4.2 Protecting the Virtualization Layer

The next level of protection is maintaining integrity of the hypervisor itself which is actually the foundation of all trust in the previously described technologies.
One approach is to work on the physical memory of your cloud environment and extract data from the hypervisor memory, define data sets, generate hash values (for data sets that should stay static), compile hashes into an inspection engine and scan your container (for any unknown code running).

Hypervisors should be monitored and protected as follows:

- Monitor hypervisor login failures and successes
- Perform real-time monitoring of hypervisor files and configuration settings
- Identify and alert when administrators connect to the virtualization system
- Protect against insider abuse and external attacks using granular policy-based controls. For example:
  - Perform intrusion detection and log inspection across management components
  - Restrict inbound and outbound port access to trusted programs
  - Deescalate user privileges to prevent tampering of virtual hosts or virtual machines

### 4.1.5 Client-Based Detection

If detection and filtering are done within the guest OS (either kernel modules of the OS vendor, or third-party modules using an OS API), try to identify and prevent an intrusion by inspecting and filtering certain events, (function calls, packets, write/read to memory, etc.).

![Figure 5: IM within the Guest OS](image)

**Advantages:**

- Easy deployment
- Interception of VM-VM communication
- Interception of guest operations
- View of calls to guest OS, write to memory, etc.
- Use of additional configuration and status information (e.g., patch level)

Disadvantages:

- A software instance cannot use hardware support (ASICs) like today's dedicated IPS appliances
- High load on the IPS modules will impact virtual machines or the host performance
- If the guest is compromised, the IPS can't be trusted anymore

**4.1.5.1 Host - Guest IPS/IDS Implementation in Virtualized Environments**

- Provides maximum security for virtual data centers across the guest, hypervisor, and management server reducing the risk of a data breach
- Within the guest, virtual machines are subject to similar attacks found on physical servers such as malicious software downloads and vulnerability exploits. At the hypervisor, system files and configurations must be monitored to detect unauthorized access and demonstrate regulatory compliance
- The Virtual solutions management server must be protected against external attacks as well as insider abuse, as a single unauthorized change could compromise all related hosts and virtual machines disrupting critical business operations
- Issues with encrypted traffic may limit what can be seen here, but IP level traffic statistics are available in most deployments

**4.1.6 Application Layer Detection**

Sometimes, especially in the case of encrypted content inspection, the application itself the best (and only) place where this is possible. Applications may have internal code detection and/or intrusion prevention. Web applications, for instance, typically have input parser filtering SQL injection attempts and also logging of these events.
Advantages:

- Can understand the application logic and spot specific and logical intrusion attempts
- Typically “built-in.” No deployment required (probably activation via configuration file or option)

Disadvantages:

- Only usable if the application supports it or it was built in
- A software instance cannot use hardware support (ASICs) like today’s dedicated IPS appliances
- High load on the IPS modules will impact virtual machines or the host performance

4.1.7 Hybrid Solutions

The approach below is an attempt to combine the advantages of external appliance-based traffic inspection (i.e., performance and load reduction) with virtualization aware, central policy driven enforcement controls within the hypervisor:
Central policies for certain types of VM groups are defined (DMZ, Web, PCI DSS, etc.). A controller module within the VMM kernel can intercept traffic and either send it out to an external IPS appliance or “route” it through a virtual appliance.

**Advantage:**
- Interception of VM-VM communication
- Can offload traffic to a powerful external IPS infrastructure
- Policy driven inspection that can follow moving VMs

**Disadvantage:**
- Most critical enforcement component (interception controller) lies within the hypervisor, thus integrity is critical

**Caution:**
- Scalability
4.2 Cloud-Provided IM SecaaS Implementation

As most of the guidance in the architecture section includes both potential architecture options at each layer within the target environment as well as necessary protections provided, this section need only provide guidance for implementation of those capabilities as a cloud-provided service. As indicated in the Introduction to this guide, since the market is immature and there is a lack of significant best practices or common architectures for implementing IM, let alone as a SecaaS, this version of the implementation guide provides only structural considerations for IM SecaaS and leaves room for additional guidance in future versions.

4.2.1 Intrusion Management Infrastructure

IM Infrastructure would include the distributed and/or cloud-based capabilities for management of policies, devices, and resultant data as well as the mechanisms for central collection and reporting and interfaces to event correlation served by all sources for context aware management and dynamic response. This may be an overlap or merely an interface to the SIEM service solution.

Infrastructure also may include features such as configuration and signature management and should incorporate appropriate policy and process for the management of the detection of and response to intrusions as fed by SIEM or manual intervention. It is critical to rectify integration concerns related to data management, policy or signature deployment, and roles and responsibilities for authorizing or approving changes to the system. Access to, format of, and data flow from log files and other system-based information are critical to success of centralized management and cloud delivery.

4.2.2 Policy Implementation

IM SecaaS solutions need to provide proactive, policy-based monitoring and protection to help organizations secure their physical and virtual server environments, as well as the business critical applications, databases, directories and file stores whether they reside within cloud-based servers or on systems outside the cloud infrastructure.

Cloud-based solutions should provide a protection policy library containing prevention and detection policies that can be used and customized to protect critical hosts.

- **A prevention policy** is a collection of rules that governs how processes and users access resources. For example, prevention policies can contain a list of files and registry keys that no program or user can access. Prevention policies can contain a list of UDP and TCP ports that permit and deny traffic. Prevention policies can deny access to startup folders. Prevention policies define the actions to take when unacceptable behavior occurs. Prevention policies protect against inappropriate modification of system resources. The policies confine each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls; generic behavior controls provide compatibility for other services and applications.

- **A detection policy** is a collection of rules that are configured to detect specific events and take action. For example, detection policies can be configured to generate events when files and registry keys are...
deleted, when USB devices are inserted and removed from computers, and when network shares are created and deleted.

IM SecaaS should have both policy management and policy enforcement processes and communications channels in order to integrate with customer systems and infrastructure to centrally report and potentially execute the following capabilities:

- Day-zero protection: stop malicious exploitation of systems and applications; prevent introduction and spread of malicious code
- Hardened systems: lock down OS, applications, and databases; prevent unauthorized executables from being introduced or run
- Integrated firewall blocks inbound and outbound TCP/UDP traffic; administrator can block traffic per port, per protocol, per IP address or range
- Maintain compliance by enforcing security policies on cloud-based servers. Comprehensive compliance helps address various information security regulations and standards such as PCI DSS, NERC, Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLB) and HIPAA
- Policy-based monitoring setup for real-time event notification and alerting features
- Buffer overflow protection
- Log consolidation for easy search, archival, and retrieval
- Advanced event analysis and response capabilities
- File and registry protection and monitoring
- Supports integration with SEIM for long-term storage of event information, event correlation and incident management
5.0 References and Useful Links

5.1 References


5.2 Useful Links

Cloud Security Alliance Guidance
https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf


Intrusion Detection
http://en.wikipedia.org/wiki/Intrusion_detection_system

Intrusion Prevention