FOREGENIX

White Paper

Amazon GuardDuty Security Review

Prepared by:

Andrew McKenna, Principal Consultant
Dimitris Kamenopoulos, Information Security Officer
Keith Lee, Senior Penetration Tester

Foregenix Inc. | 75 State St., 1st Floor, Boston, MA, 02109 | USA | +1 (877) 418 4774

1 Executive Summary

Cloud Technologies are largely subject to the same attack vectors seen in more traditional on-premise deployments, and therefore when it comes to cyber security, they require the same level of attention. However, Cloud Technologies like Amazon Web Services (AWS) also introduce new opportunities for more effective defence, and the correct understanding of this is critical for a successful cyber security strategy.

Cloud providers can sometimes struggle to provide a granular level of access to internal security events and other interesting system behavior indicators, but when these are available, cyber security vendors can consume them and use them to generate appropriate security responses. AWS provides a dedicated service for this task, Amazon GuardDuty.

Foregenix has been engaged by AWS to perform an independent cyber security assessment of GuardDuty and produce an opinion in relation to how the service compares with other recognised industry solutions in relation to three specific areas:

1. Ability to detect suspected intrusions and alert personnel to suspicious activity
2. Ability to support PCI DSS compliance requirements
3. Ability to deploy and activate without expert skills

The Testing Environment

Foregenix configured a lab environment to perform testing using extensive and complex attack playbooks. The lab environment simulated a real world deployment composed of a web server, a bastion box and an internal server used for centralised event logging. The environment was left running under normal operating conditions for more than 45 days in order to allow all tested solutions to build up a baseline of patterns for standard environmental behaviour, from which to detect anomalies later on.

The test, initially focused on Amazon GuardDuty, also included Host-based IDS solutions from other vendors available in the AWS marketplace.

Our findings

Amazon GuardDuty demonstrated being a very effective tool in any organisation's AWS Cloud defensive arsenal; it was found to be extremely simple to deploy and activate, and required no specialised skills to operate. GuardDuty, by operating at the AWS plane and analysing DNS requests, VPC traffic flow and CloudTrail events, was able to identify threats which could not be identified by other tools without extensive customisation. While the combination of these features make GuardDuty a unique offering, there is still space for improvement and collaboration with other tools when it comes to threat detection for other layers of the attack plane. As a result, Foregenix believes that GuardDuty presents an ideal solution for AWS customers facing compliance challenges, but that in order to achieve a comprehensive in-depth defensive posture within the AWS Cloud, the use of GuardDuty should be lightly complemented by other threat detection technologies.

2 An overview of current Intrusion Detection Systems

Intrusion Detection and Prevention Systems (IDS & IPS) are tools which are used to detect malicious activity or threats within networks and/or systems. These solutions are generally network-focused or host-based and each implementation addresses a subset of the threat landscape. That is to say, these implementations are not interchangeable and act on different inputs and, therefore, will detect different threats. From a compliance perspective, the requirement is typically to ensure an IDS/IPS is in place. From a security perspective, one may favour one over the other for a given threat profile or both can be used to address different threats.

To further develop on the above, implementations are generally signature-based or behaviour-based.

- **Signature based** - the tool maintains an inventory of indicators of compromise or threat vectors and generates alerts once such is identified.
- **Behavior based** - the tool learns what is normal behavior over time and considers this to be a behavioral baseline for a given environment. Anomalous activity which deviates from the baseline is flagged as a potential threat.

GuardDuty's functionality is similar to that of a Network IDS and uses a hybrid approach to detection meaning it analyses traffic for signature matches as well as monitors for deviations from baseline activity (AWS recommends a 45 day behaviour learning phase). As GuardDuty spans the entire VPC, it monitors north/south traffic as well as east/west.

GuardDuty analyses events from multiple AWS data sources, such as AWS CloudTrail,

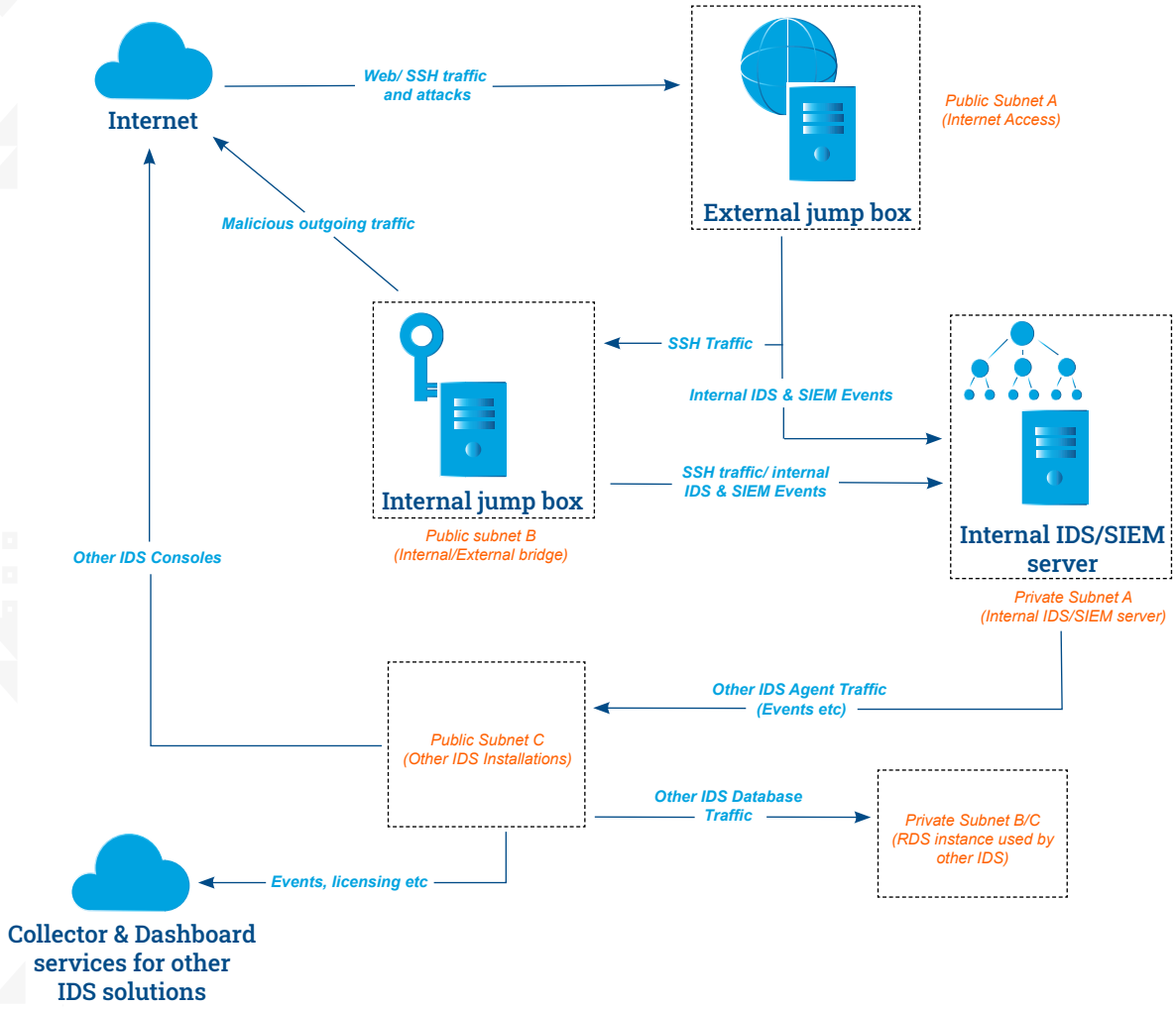
Amazon VPC Flow Logs, and DNS logs and detects suspicious activity based on threat intelligence feeds received from AWS and other services such as CrowdStrike. AWS CloudTrail performs logging and monitoring of account activities related to actions across the AWS infrastructure. VPC Flow captures information about IP traffic going to and from network interfaces. DNS logs DNS queries received by the AWS DNS servers.

There is currently no single IDS implementation which addresses cloud, network and host threat spaces for the AWS Cloud.

Approach to testing and analysis

Foregenix set up a VPC with six subnets (three private and three public). Two of the private subnets were used exclusively for RDS (see below), while the third one was used by EC2.

The VPC layout is depicted below:



Public subnets

On the first public subnet Foregenix deployed a Linux instance running both a web server and an SSH server, and configured it to accept relevant traffic from the internet. This was deemed “the entry point” to our VPC, as no other instance was configured to accept incoming traffic from the internet.

On the second public subnet Foregenix deployed a bastion host, a Linux instance running an SSH server. It was configured to accept SSH traffic from the entry point (above), and all other instances were configured to only accept SSH traffic from the bastion. Although the bastion was deployed on a public subnet its security groups blocked any traffic coming from the Internet; it was deployed in this way to allow for emergency connections from a white-listed public IP address.

The third public subnet was used to deploy several instances of other IDS solutions (both commercial and open source), following their own AWS CloudFormation templates.

Private subnets

The first EC2 private subnet hosted a Linux instance, configured to accept SSH traffic only from the bastion box. This instance was also used for event log collection on port 1514/UDP.

The other two private subnets were created to host an RDS instance.

Four different IDS systems were deployed within the test environment and attacks were run to/from the two public instances.

The inclusion of various IDS systems in testing was intended to provide a performance baseline in order to identify if GuardDuty’s detection and alerting capabilities are consistent with those of other solutions.

Initial Findings

Amazon GuardDuty

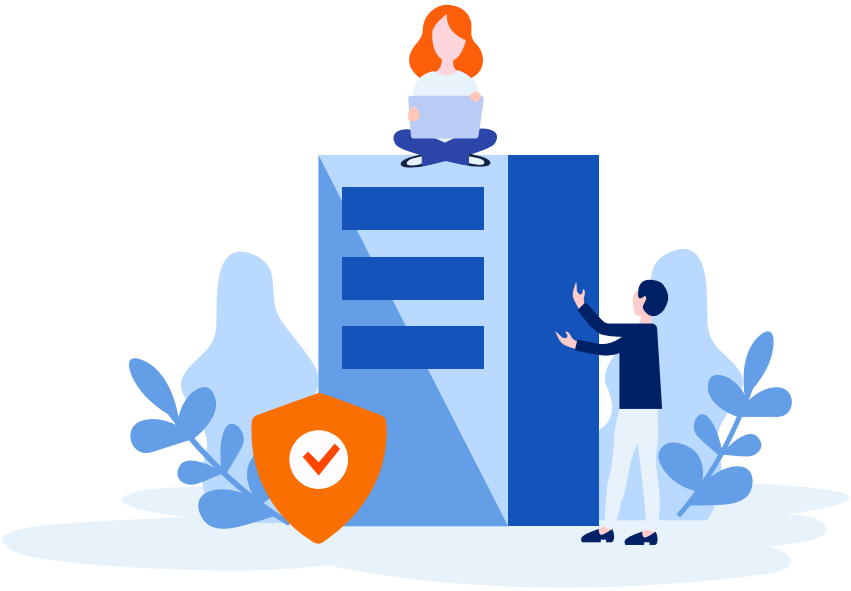
Amazon GuardDuty was unique in detecting DNS-based malicious activity such as lookups for bitcoin domains. It was also successful in detecting IAM-level activity such as attempts at credential exfiltration. Interestingly, it did not report our brute force SSH attacks (run as part of the tests) but did report genuine brute force SSH attacks targeting the same instances from several internet sources.

Amazon GuardDuty specific findings

Amazon GuardDuty classifies threat families in the following “Active Finding Types”. These classes are well documented in the GuardDuty User Guide.

- Backdoor Finding Types
- Behavior Finding Types
- CryptoCurrency Finding Types
- PenTest Finding Types
- Persistence Finding Types
- Policy Finding Types
- PrivilegeEscalation Finding Types
- Recon Finding Types
- ResourceConsumption Finding Types
- Stealth Finding Types
- Trojan Finding Types
- Unauthorized Finding Types

As mentioned above, during the analysis phase it was found that GuardDuty raised alerts in response to both Foregenix’s controlled activity and also real world attacks against the services exposed to the Internet. Details and examples of the GuardDuty events and alerts can be found in the Appendix.



Below is the breakdown of the specific threats grouped by each of the Active Finding Types.

Active Finding Types	Sub Findings
Backdoor Finding Types	Backdoor:EC2/Spambot Backdoor:EC2/C&CActivity.B!DNS Backdoor:EC2/DenialOfService.Tcp Backdoor:EC2/DenialOfService.Udp Backdoor:EC2/DenialOfService.Dns Backdoor:EC2/DenialOfService.UdpOnTcpPorts Backdoor:EC2/DenialOfService.UnusualProtocol
Behavior Finding Types	Behavior:EC2/NetworkPortUnusual Behavior:EC2/TrafficVolumeUnusual
CryptoCurrency Finding Types	CryptoCurrency:EC2/BitcoinTool.B!DNS CryptoCurrency:EC2/BitcoinTool.B
PenTest Finding Types	PenTest:IAMUser/KaliLinux PenTest:IAMUser/ParrotLinux PenTest:IAMUser/PentooLinux
Persistence Finding Types	Persistence:IAMUser/NetworkPermissions Persistence:IAMUser/ResourcePermissions
Policy Finding Types	Policy:IAMUser/S3BlockPublicAccessDisabled Policy:IAMUser/RootCredentialUsage
PrivilegeEscalation Finding Types	PrivilegeEscalation:IAMUser/AdministrativePermissions
Recon Finding Types	Recon:EC2/PortProbeUnprotectedPort Recon:EC2/PortProbeEMRUnprotectedPort Recon:IAMUser/TorIPCaller Recon:IAMUser/MaliciousIPCaller.Custom Recon:IAMUser/MaliciousIPCaller Recon:EC2/Portscan Recon:IAMUser/NetworkPermissions Recon:IAMUser/ResourcePermissions Recon:IAMUser/UserPermissions
ResourceConsumption Finding Types	ResourceConsumption:IAMUser/ComputeResources
Stealth Finding Types	Stealth:IAMUser/S3ServerAccessLoggingDisabled Stealth:IAMUser/PasswordPolicyChange Stealth:IAMUser/CloudTrailLoggingDisabled Stealth:IAMUser/LoggingConfigurationModified

Active Finding Types	Sub Findings
Trojan Finding Types	Trojan:EC2/BlackholeTraffic Trojan:EC2/DropPoint Trojan:EC2/BlackholeTraffic!DNS Trojan:EC2/DriveBySourceTraffic!DNS Trojan:EC2/DropPoint!DNS Trojan:EC2/DGADomainRequest.B Trojan:EC2/DGADomainRequest.C!DNS Trojan:EC2/DNSDataExfiltration Trojan:EC2/PhishingDomainRequest!DNS
Unauthorized Finding Types	UnauthorizedAccess:EC2/MetadataDNSRebind UnauthorizedAccess:IAMUser/TorIPCaller UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B UnauthorizedAccess:IAMUser/MaliciousIPCaller UnauthorizedAccess:EC2/TorIPCaller UnauthorizedAccess:EC2/MaliciousIPCaller.Custom UnauthorizedAccess:EC2/SSHBruteForce UnauthorizedAccess:EC2/RDPBruteForce UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration UnauthorizedAccess:IAMUser/ConsoleLogin UnauthorizedAccess:EC2/TorClient UnauthorizedAccess:EC2/TorRelay

Amazon GuardDuty and PCI Compliance

The PCI DSS is not prescriptive regarding the type of IDS deployed (i.e. network or host-based) nor regarding the categories of events an IDS should be able to detect (we detailed above that there is a separation between what network and host-based deployments can detect). Rather, the PCI DSS requires security controls are in place to detect intrusions at the perimeter and at critical points within the cardholder data environment. GuardDuty, working across the AWS network plane, performing inspection of various event sources and applying a blend of signature-based and behavior-based analytics and detection thereupon, proves to be a robust IDS service which can meet the relevant requirements of PCI DSS, with minimal human support.

The specific controls for IDS within the PCI Data Security Standard are enumerated within Requirement 11.4. The following are the relevant PCI requirements and the results in relation to our testing of GuardDuty:

Requirement	Finding
11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: • At the perimeter of the cardholder data environment. • At critical points in the cardholder data environment.	**In Place** Amazon GuardDuty monitors DNS, VPC Flow and CloudTrail logs - this includes all traffic at the perimeter of, and critical points in, the AWS portion of an organisation's cardholder data environment.
11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	**In Place** Amazon GuardDuty can be configured to notify personnel of suspected compromises via email or SMS message.
11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	**In Place** An organisation leveraging the Amazon GuardDuty service can rely on AWS' PCI Attestation of Compliance including the GuardDuty service. Once the service is enabled, no additional configuration is required by the customer to configure, maintain or update the service. Responsibility for this requirement is assessed within AWS' own compliance and responsibility does not lie with the customer.

3 CONCLUSIONS & RECOMMENDATIONS

After testing a number of solutions available in the AWS marketplace using various intrusion playbooks and technical tools, Foregenix found that no single solution provides complete 'out of the box' coverage across all possible intrusion types. However, as a network or non-host-based IDS, Amazon GuardDuty was successful in detecting and alerting on all intrusion attempts with no customisation required. In this regard, GuardDuty scored much higher than all other competing solutions and was certainly the most successful option in terms of detecting AWS-specific threats.

"Amazon GuardDuty was successful in detecting and alerting on all intrusion attempts with no customisation required."

This is not to suggest other solutions do not have significant or similar threat detection capabilities, however achieving comparable results would require additional customisation effort.

From an optimal cyber security standpoint, in order to achieve the highest possible threat detection rate, Foregenix believes AWS customers should leverage the best of both worlds: deploy a Host-based IDS for protecting the instances from the "inside", and GuardDuty to protect the surrounding "cloud" as well as the host's external environmental behaviour. Testing demonstrated that such a configuration would provide the most effective cyber security alternative for an AWS Cloud environment running both EC2 instances and serverless infrastructure.

Appendix

Below is the list of tools that were used during the review of Amazon GuardDuty.

Tool	Website	Description
Crowbar	https://github.com/galkan/crowbar	Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys
GoldenEye	https://github.com/jseidl/GoldenEye	GoldenEye Layer 7 (KeepAlive+NoCache) DoS Test Tool
Hping3	http://www.hping.org	Hping is a command-line oriented TCP/IP packet assembler/analyzer
Loic	https://github.com/xymostech/loic	Low Orbital Ion Cannon Load Tester
Medusa	http://foofus.net/goons/jmk/medusa/medusa.html	Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer
Minerd	https://github.com/Miniblockchain-Project/Minerd	Multithreaded CPU miner for M7/Cryptonite
Mz	https://github.com/netsniff-ng/netsniff-ng	Mausezahn is a fast traffic generator written in C which allows you to send nearly every possible and impossible packet
Nmap	https://nmap.org/	Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks
Privoxy	https://sourceforge.net/projects/ijbswa/	Privoxy is a free non-caching web proxy with filtering capabilities for enhancing privacy, manipulating cookies and modifying web page data and HTTP headers before the page is rendered by the browser
Proxychains	https://github.com/haad/proxychains	Proxychains - a tool that forces any TCP connection made by any given application to follow through proxy like TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy. Supported auth-types: “user/pass” for SOCKS4/5, “basic” for HTTP
Slowloris	https://pypi.org/project/Slowloris/	Low bandwidth DoS tool
Tcpreplay	https://tcpreplay.appneta.com/	Tcpreplay is a suite of free Open Source utilities for editing and replaying previously captured network traffic
Tor	https://www.torproject.org/download/	Tor is free and open-source software for enabling anonymous communication
Yersinia	https://github.com/tomac/yersinia	Yersinia is a framework for performing layer 2 attacks

Below is a list of threat intelligence feeds that were used during the testing.

- https://data.netlab.360.com/feeds/dga/blackhole.txt
- https://data.netlab.360.com/feeds/dga/dga.txt
- https://openphish.com/feed.txt
- https://osint.bambenekconsulting.com/feeds/dga-feed.txt
- https://precisionsec.com/threat-intelligence-feeds/agenttesla/
- https://precisionsec.com/threat-intelligence-feeds/azorult/
- https://precisionsec.com/threat-intelligence-feeds/lokibot/
- https://precisionsec.com/threat-intelligence-feeds/nanocore/
- https://precisionsec.com/threat-intelligence-feeds/njrat/
- https://precisionsec.com/threat-intelligence-feeds/trickbot/
- https://precisionsec.com:443/threat-intelligence-feeds/emotet/
- https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt
- https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-NEW-today.txt
- https://urlhaus.abuse.ch/downloads/csv_online/
- https://www.circl.lu/doc/misp/feed-osint/

FOREGENIX

Head Quarters

Foregenix Ltd.
8-9 High Street, Marlborough
SN8 1AA
United Kingdom
+44 845 309 6232

MEA

Foregenix (Pty) Ltd.
58 Peter Place, Sandton
2060
South Africa
+27 860 44 4461

LATAM

Foregenix do Brasil
Av. Paulista 2064/2086, 14° andar
Ed. Paulista, São Paulo
Brasil
+55 11 98781 4241

North America

Foregenix Inc
75 State Street, 1st Floor
Boston, MA, 02109
United States
+1 877 418 4774

Europe

Foregenix Germany GMbH.
Betzelsstrabe 27, 55116
Mainz
Germany
+49 6131 2188747

APAC

Foregenix (Pty) Ltd.
1 Market Street, Sydney
NSW 2000
Australia
+61 420 904 914

2019