Check Point
SOFTWARE TECHNOLOGIES LTD

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

EXPOSED
and
UNPROTECTED
In Cloud Environments

Why Modern Threat Prevention Security Needs to Be Part of Your Cloud Strategy

EXECUTIVE SUMMARY

With benefits like increased agility, improved efficiencies and lower overall fixed costs, it's no surprise that nearly 95 percent of businesses are now using the cloud. In conjunction with this rapid adoption, users of cloud services are experiencing a 300% increase in cyber-attacks targeting their cloud environments.

When it comes to protecting sensitive data, extensive measures should be taken to keep information private and secure. However, that's easier said than done, especially in the cloud. The growth and popularity of cloud solutions continues to drive more data beyond traditional IT security protections – into networks no longer owned, managed or controlled by corporate IT teams. On premise IT security controls do not touch the cloud, leaving customer data at risk from the same types of threats targeting applications in corporate data centers.

While cloud providers deliver strong security controls to protect the cloud fabric, they have no knowledge of "normal" customer traffic and thus are unable to determine malicious content or activity from benign. Since the responsibility to protect a cloud environment is now shared between the customer and the cloud provider, that begs the question; what really happens when you spin up a new cloud service and connect it to the internet?

This document will highlight practical examples of the risks associated with moving data and assets to the cloud. Additionally, we will provide guidance on how to leverage IT security to keep your cloud environment protected while staying aligned to the dynamic needs of your cloud network.

TABLE OF CONTENTS

Executive Summary 2

Today's Forecast: Cloudy! 4

Is Your Data Naked in the Cloud? 5

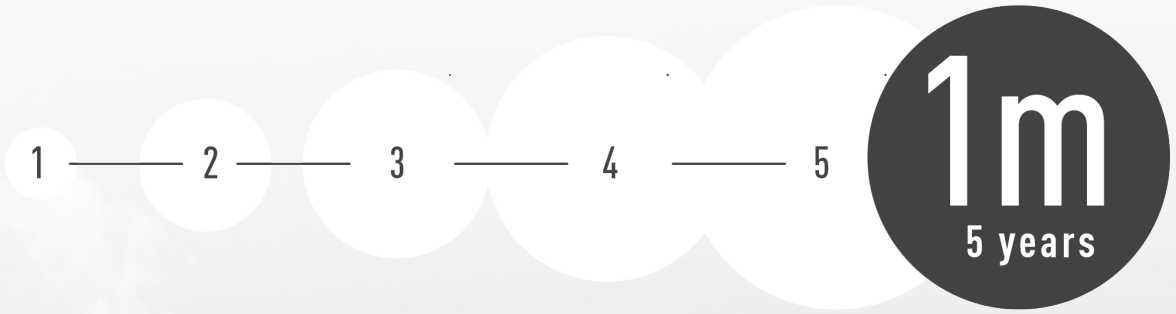
Exposing the Risks 6
- Our New Cloud Environment 6
- Using a Honeypot to Make Things Visible 6
- Let the Hacking Begin: Observations of the First 15 Minutes 8
- Automated Agents of Doom 9
- Long-Term Results 10
- Analyzing the Results: Digging Deeper 11

Closing Your Cloud Security Gaps: Introducing Check Point CloudGuard IaaS 14
- Deploying CloudGuard IaaS with Our TPOT 15

Summary 16

TODAY'S FORECAST: CLOUDY!

What do organizations like Snap Inc., Airbnb, Apple, Netflix, Workday and Pixar all have in common? While they offer distinct business models and vastly different products, they all have significant investments and strategic initiatives in public cloud solutions. In fact, analyst firm Gartner predicts that the appetite for public cloud Infrastructure-as-a-Service (IaaS) is forecast to exceed $71 billion by 2020.



Businesses of all sizes are investing heavily in cloud solutions to improve efficiencies, drive innovation and increase responsiveness to competitors and the market. According to a recent article on businessinsider.com; "Snap Inc, owner of the popular Snapchat app, said it expected to spend $1 billion over the next five years to use Amazon's cloud services, in addition to the $2 billion cloud contract it already has with Google."

Organizations like Snap and countless others could never exist in the past due to the high risks and massive CAPEX investments required to setup and manage their own infrastructures. Startups are now able to bring their products to market faster leveraging shared datacenter resources in the public cloud instead of spending countless resources and time designing, deploying and managing physical infrastructure.

With the digital transformation of business processes, competencies and models now influencing how organizations utilize Information Technology, one thing is clear; the role and importance of the cloud will continue to grow.

IS YOUR DATA NAKED IN THE CLOUD?

Extending infrastructure to the cloud means corporate data is now being driven beyond our traditional IT security protections. What's more, the need to access data from anywhere means cloud-based assets are increasingly connected to the Internet, often times without even the most basic security controls protecting them.

The sad truth is that customer assets in the cloud are at risk from the same types of threats targeting corporate networks and data centers. An unpatched server connected to the Internet is vulnerable to the same threats whether on a customer's network or in the cloud. The key difference is on corporate networks, servers typically would never directly connect to the Internet; at a bare minimum they connect through security controls such as firewall, IPS, Anti-Virus and URL filtering to ensure they don't end up bringing something undesired back onto the network.

Cloud providers, on the other hand, protect their infrastructure, cloud fabric, hypervisors, services and tenant environments. They are NOT responsible for protecting any assets or data that customers place on their networks. It is imperative for businesses to understand that they are responsible for protecting all data, workloads and assets that reside in the cloud. This is what cloud providers refer to as the "shared security responsibility" model.

The security controls cloud providers offer are port filters or access control lists (ACLs) that allow clients to segment their environment and control both inbound and outbound traffic. Beyond that, there is no native mechanism in place to determine whether traffic flowing in or out of a customer environment is benign or malicious. Bottom line; don't be lulled into a false sense of security.

Cloud-based applications provide several access inroads into customer networks and cybercriminals only need to find a way to get in. The rush to the cloud should not outweigh the due diligence required to keep your environment secure.

The following sections highlight real-world examples of the security risks associated with moving data and assets to the cloud as well as provide guidance on how to deploy a security solution that is highly automated and elastic to meet the dynamic needs of public cloud environments.

EXPOSING THE RISKS

We wanted to see for ourselves the security challenges customers are likely facing when adopting public cloud infrastructure, so we simulated a typical customer cloud environment using the services of Microsoft Azure. The concepts explored in this paper also apply to any public cloud provider as well as private cloud solutions from OpenStack, Cisco ACI or VMware NSX.

The ACL-based security controls offered by cloud providers all work roughly the same way: open a specific port to allow access to and from somewhere, for example access to and from the Internet. When setting up a webserver with access to the Internet, port 80 and 443 as well as ports for administrative purposes such as secure socket shell (SSH) or remote desktop protocol (RDP) are typically opened. All popular private and public cloud services have rule sets available to accomplish these basic functions.

As stated previously, cloud providers do not natively deliver advanced security mechanisms for customer data on their cloud; they neither inspect traffic payloads for malicious content nor provide logs to help identify unusual activity. Most of the time customers are blissfully unaware they are lacking these features, leading to a state of complacency or a false sense of security. Without these advanced security controls in place, it is virtually impossible to determine your level of exposure. To illustrate this more closely, let's deploy a new cloud service and observe what happens next.

OUR NEW CLOUD ENVIRONMENT

The first step in setting our new cloud environment is configuring a server. This may take only a few seconds or several minutes depending on the level of automation employed.

While our new service is being prepared, in the background our target operating system is also prepared for first-time use. This process is typically done using prebuilt and readily available templates. Like any template-based operation, all templates need to be maintained and updated regularly though many may not change for months.

Following a successful deployment, we highly recommended to patch your operating system with the latest updates. It is interesting to note that the time between deployment and the point when all updates are successfully installed, your server is unprotected and can easily be compromised. There is a narrow window of opportunity when all new machines risk getting compromised – even by well-known and easily preventable attacks.

Yet, since neither logging nor threat visibility is natively available to identify anomalous behavior, it is next to impossible to recognize if and when something goes wrong with our new virtual server. Of course, this is nothing new in the IT security space, but not all cloud customers recognize this fact.

USING A HONEYPOT TO MAKE THINGS VISIBLE

We wanted to better understand what threats would start targeting our newly deployed cloud service so we deployed a honeypot. The honeypot acts as a security monitor giving us the opportunity to see what's going on behind the scenes.

The challenge with developing a honeypot, especially in the cloud, is that it can take a great deal of time. However, thanks to Deutsche Telekom we were able to use a public honeypot equipped with a variety of analytic tools. This honeypot (TPOT) will be referenced throughout the next sections to highlight the importance of deploying advanced security protections in the cloud.

Technical Background on the Honeypot

The source of our honeypot can be found at the following link: https://github.com/dtag-dev-sec/t-pot-autoinstall.

Our TPOT contains a wide range of security services:

Honeypot	Description	Link to Community
Conpot	Conpot is a low interactive server-side Industrial Control Systems honeypot	http://conpot.org/
Cowrie	SSH and Telnet Honeypot	http://www.micheloosterhof.com/cowrie/
Dionaea	Dionaea is meant to be a nepenthes successor, embedding Python as scripting language	https://github.com/DinoTools/dionaea
elasticpot	Basic elastic search honeypot	https://github.com/dtag-dev-sec/elasticpot
emobility	eMobility is a high-interaction honeynet with the goal to collect intelligence about the motives and methods of adversaries targeting next-generation transport infrastructure.	https://github.com/dtag-dev-sec/emobility
Glastopf	Glastopf is a Python web application honeypot using vulnerability type emulation instead of vulnerability emulation	http://glastopf.org/
honeytrap	Honeytrap is a network security tool written to observe attacks onTCP and UDP ports	https://github.com/armedpot/honeytrap/
Suricata	Suricata is a free and open source, mature, fast and robust network threat detection engine.	http://suricata-ids.org/

System Requirements for Our TPOT

```
############################################################
#
#     How do you want to proceed? Enter your choice.
#
# 1 - T-Pot's STANDARD INSTALLATION
#     Requirements: >=4GB RAM, >=64GB disk
#     Services: Cowrie, Dionaea, ElasticPot, Glastopf,
#     Honeytrap, ELK & Suricata
#
# 2 - T-Pot's HONEYPOTS ONLY (w/o INDUSTRIAL)
#     Requirements: >=3GB RAM, >=64GB disk
#     Services:
#     Cowrie, Dionaea, ElasticPot, Glastopf & Honeytrap
#                                                      #
# 3 - T-Pot's INDUSTRIAL EDITION
#     Requirements: >=4GB RAM, >=64GB disk
#     Services: ConPot, eMobility, ELK & Suricata
#
# 4 - T-Pot's FULL INSTALLATION
#     Requirements: >=8GB RAM, >=128GB disk
#     Services: Everything
```

Installation Script

After setting up and running an Ubuntu 16.04 LTS server, we installed our Honeypot using the following script:

```
git clone https://github.com/dtag-dev-sec/t-pot-autoinstall.git
cd t-pot-autoinstall/
sudo su
./install.sh
```

For our environment, we used the standard installation (1).

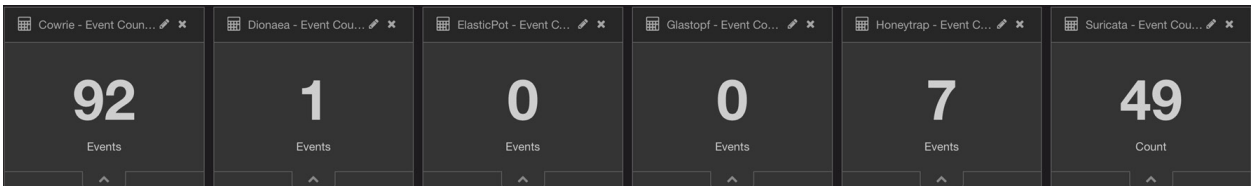
After successfully installing our TPOT, the wizard quits with the following message:

```
### Thanks for your patience. Now rebooting. Remember to login on
SSH port 64295 next time or visit dashboard at port 64297!
```

Now that we've got our TPOT in place, we're able reach it using its public IP Address at Port 64297 (e.g., https://1.1.1.1:64297)

LET THE HACKING BEGIN: OBSERVATIONS OF THE FIRST 15 MINUTES

New cloud services are particularly attractive targets because there is a time lag between when the service is deployed and when patches are installed, and our service was no exception. Within the first few minutes of our service going live, we gathered the following statistics by our honeypot:



- Ninety two (92) attacks are being recognized by Cowie
- One (1) attack is recognized by Dianoae
- Seven (7) attacks are being recognized by Honeytrap
- Forty nine (49) network based attacks are detected by the Open Source IDS Suricata

Without our TPOT in place, we wouldn't even know this activity is taking place on our new cloud service. Lacking that visibility or knowledge, it may already be too late for most cloud services. In the worst case scenario, our new server has already been fully compromised and even installing any available patches will not remedy the damage.

AUTOMATED AGENTS OF DOOM

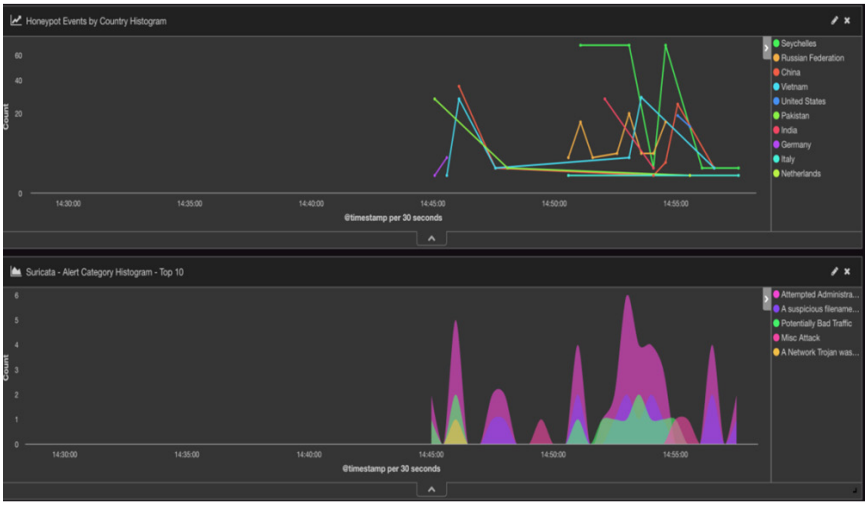
How are these new services being targeted so rapidly? In their recently published Bad Bot Report, Distil Networks noted that unauthorized vulnerability scans take place on 88% of all websites. Cyber criminals are using automated bot armies to attack unprotected web servers. They already know and target ranges of IP addresses affiliated with public cloud providers to find all new servers and services coming online.

These scans not only identify vulnerable hosts but are also able see what else these hosts are connected to, giving the bad guys a clear picture of the overall network and all higher value targets contained within. The scans are made to look like legitimate activity and use common ports (80 and 443 for example), so standard port-blocking techniques aren't able to stop these subtle attacks.

The same report also indicated that bad bot traffic accounted for about 20% of all website traffic in 2016. In addition to scanning and gathering intelligence on unprotected customer environments, these automated nefarious agents of doom can also be used for: "web scraping, competitive data mining, personal and financial data harvesting, brute-force login and man-in-the-middle attacks, digital ad fraud, spam, transaction fraud, and more."

Now that our new service has come to the attention of these bot armies, our TPOT starts logging some rather interesting traffic patterns. One of the first things we witness is brute-force SSH login attempts against our new server.

SSH can be an effective authentication method when configured for secure key exchanges. However, most customers choose password authentication which is much easier to configure, but also easier to compromise. Since new services are often deployed by non-security professionals (DevOps, cloud architects, etc.), best practices techniques like using strong passwords often aren't leveraged, leaving these sites ripe for weak, stolen or misused credentials. The above screen shot shows all failed login attempts within the first 15 minutes of our new service going live.



In conjunction with the brute-force SSH attacks witnessed, we also start to see additional attacks and their toolkits targeting our new service. The following screen capture provides a sample of the additional attacks being detected by our TPOT.

The most interesting aspect of this activity is the fact these attacks are occurring immediately after our new cloud service went live. The time for maintenance or installing any patches just vanished; our new service is under attack.

LONG-TERM RESULTS

The initial attack results were surprising, but the longer we let our TPOT gather information about on-going threats the more it became apparent that native security controls in the cloud weren't enough. This next screen shot was collected after the first 30 minutes our cloud service went live. It shows a variety of attacks occurring simultaneously and among them we are now seeing connections from botnets like the IOT botnet Mirai. (More information on Mirai malware can be found here: https://en.wikipedia.org/wiki/Mirai).

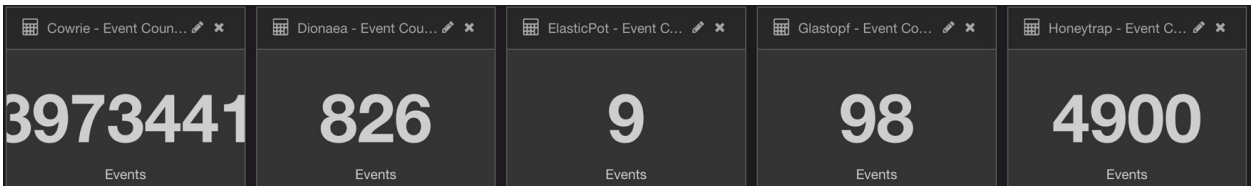
Suricata - Alert Signature - Top 10

Alert Signature	Alert Signature ID	Count
ET TELNET SUSPICIOUS Path to BusyBox	2023016	14
ET TELNET SUSPICIOUS busybox enable	2023018	14
ET TELNET SUSPICIOUS busybox shell	2023017	14
GPL TELNET Bad Login	2101251	12
ET TROJAN Possible Linux.Mirai Login Attempt (7ujMko0vizxv)	2023434	2
ET TROJAN Possible Linux.Mirai Login Attempt (klv1234)	2023444	2
ET TROJAN Possible Linux.Mirai Login Attempt (ubnt)	2023448	2
ET CINS Active Threat Intelligence Poor Reputation IP group 20	2403319	1
ET CINS Active Threat Intelligence Poor Reputation IP group 27	2403326	1
ET CINS Active Threat Intelligence Poor Reputation IP group 87	2403386	1

Export: Raw Formatted

Over the course of seven days, we witnessed constantly running attacks against our cloud environment. Since we did not deploy any advanced security, our service remained at high risk of compromise – a fate that translates to any environment not sufficiently protected.

Within seven days of our service going live, we captured the following details:



- 3.97 Million ssh/telnet based attempts + malware uploaded to the cloud
- 826 attack attemps detected by Dionaea
- 9 attack attempts detected by the ElasticPot search engine
- 98 attempts detected by the web application honeypot Glastopf
- Almost 4900 attacks detected by Honeytrap

Our test simulated a typical cloud environment, thus this is what customers are likely to see in a similar span of time – especially if they just utilize the native ACL filters available through their cloud provider. We can clearly see that cloud assets are vulnerable to the same types of attacks targeting our premises-based networks, but the key difference is that on-premises we deploy advanced security protections to safeguard our assets. We need to start doing the same thing in the cloud.

ANALYZING THE RESULTS: DIGGING DEEPER

For further investigation, we utilized Check Point's Incident Response team to analyze the files used to try and compromise our cloud service. This section summarizes the outcome of that analysis.

- One of the more prominent attacks was the Mirai botnet. After further analysis, it was noted that an ELF based infector installs on a system and looks for an adjacent IoT devices to infect. The infected devices then become part of a Mirai botnet, commonly used for DDoS attacks and distribution of MALSPAM containing the malicious code Dridex that can also include installers for ransomware or wire transfer fraud Trojans. The list of available architectures that can be infected by this watcher Trojan are quite diverse:

- Check Point's advanced threat prevention technology fueled by the SandBlast zero-day and advanced malware solution was able to detect these variations:
  - ARM
  - x86-64
  - PowerPC or cisco 4500
  - Intel 80386
  - MIPS
  - Renesas SH
  - Motorola 68020
  - SPARC version 1 (SYSV)

It is important to note that SandBlast can be configured to not only detect, but to actively block these and other variants from infecting cloud-based environments.

File Information

File Name	apache2
MD5	e5cc377e2846d7d9784b21cfdf26d7d6
SHA256	157fd95e86093c7a3c3a74fce80f2c59165e24dcf326efb0472fac427311cc14
SHA1	8ea289398660f9c17bb04fdfc4869410efd15907
File Type	ELF 32-bit LSB executable, ARM, version 1, statically linked, not stripped
CPU Platform	ARM
File Name	bash
MD5	a1feecf6d44beb6ddd0693774b4818f9
SHA256	7e3fbca5281f0c262ded2a71a6ef4352335a2557ce8b4f75952290b2db048266
SHA1	0502efd6b2409186fe8a6949bcc1c27c0a3b19b9
File Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86-64
File Name	cron
MD5	41deb7eabe1fa56c5d35c2e212c64609
SHA256	04b6cbc5591377b8a8ef052ad9ea06eea115e6e298c7eae2b73d1d1bd6f354bc
SHA1	3d03a3f28309a28ce1f7e90f3d7ab093053e44db
File Type	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86
File Name	ftp
MD5	1d740846e0f1645a731b7e091f54a1aa
SHA256	fd1eab9c72f9fa24d027fec014a4710965b20e5d317b1063447197dadff21572
SHA1	37d204c843358e34c2a2b430725eda0a6442f747
File Type	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86

File Name	ntpd
MD5	4931b45ffdfcce38fbe9603aca2291c5
SHA256	3d240e6f3d15b85e0a8384ed8578ab7dba08d29128119ed93800d99ceb9e9926
SHA1	1be7b77f3ad01391130f2f75dd6319fd525b5680
File Type	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped
CPU Platform	MIPS

File Name	openssh
MD5	aea27832e8c02729b020708c69f9919a
SHA256	f73cf016c222a55710eba41af6db93c37a05d05c0b93e3a427b270572d3b1457
SHA1	36f9a276ed8e6f4c0f5afb5844b2dae8ea33e894
File Type	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86

File Name	pftp
MD5	d27b2a20f19255545d1c644ce7bdd6ba
SHA256	93f4ca1c85819a7cdffff6d03dc9d59b8eac96940466d9be48d1cc0aba503287
SHA1	d0289785ddfb1cf7a927f4425505d21cb04345a9
File Type	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86

File Name	sh
MD5	26474636399eb5c9bd9aa82be949a101
SHA256	c87a41fe466ec211dada8703847a49f4fd8f62479da5b2bf96761cad5b77a19b
SHA1	43bdc5eb71c1e20c89f641d121ac8671bf83d726
File Name	c87a41fe466ec211dada8703847a49f4fd8f62479da5b2bf96761cad5b77a19b
File Type	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86

File Name	sshd
MD5	0627850ef65465a8c76fb71e8ce3a21b
SHA256	3cecc1348bb37ec7dd851d3b4fba657c653e10bd12ac2ec09d3fb4a231462f57
SHA1	ca930dbd42a99c0cc82b077d38af496e4c0206b0
File Type	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped
CPU Platform	MIPSEL

File Name	tftp
MD5	f0e7273aa0a382149dfe86ce93ae911e
SHA256	868bb99faf1e08238d9cc8af48406696e1c434cc3b65e6d39cdbc36d901a7641
SHA1	ce3026f4968e913d59041849aeba5274fff35aae
File Type	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, not stripped
CPU Platform	ARM

File Name	wget
MD5	8ffdc4a4a08a1366a1c3621b0c42499e
SHA256	882fec4e2a601351d03b5fda1c835307aefdaedac5ee6203fd28d3b77114a690
SHA1	114cd29b8680773978bb89d250fe3c76dd1bfc7e
File Type	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped
CPU Platform	X86

Network Analysis

IPs Connected:

Protocol	IP Address : Port
ICMP	94.30.37.233
ICMP	221.121.141.26
ICMP	78.186.33.12
ICMP	103.54.201.70
ICMP	146.88.106.21
ICMP	103.54.24.2
ICMP	202.162.207.14
ICMP	14.181.174.169
ICMP	14.166.252.216
ICMP	203.150.229.92
ICMP	111.39.225.1
ICMP	222.252.96.5
ICMP	62.68.47.230
ICMP	202.164.32.180
ICMP	123.142.92.253
ICMP	103.248.13.154
TCP	117.175.193.174 : 23
TCP	111.9.245.179 : 23
TCP	42.48.142.133 : 23
TCP	112.27.197.159 : 23
TCP	222.252.106.225 : 23
TCP	103.20.3.184 : 23
TCP	202.44.36.182 : 23
TCP	1.56.145.192 : 23
TCP	157.130.170.146 : 23
TCP	14.161.33.209 : 23
TCP	222.252.84.154 : 23
TCP	111.9.115.194 : 23
TCP	36.32.183.242 : 23
TCP	88.248.159.179 : 23
TCP	95.9.148.196 : 23

TCP Raw Streams

111.9.245.179:23 --> 172.16.1.42:51291
[111.9.245.179:23 --> 172.16.1.42:51291]
Login timed out after 60 seconds

172.16.1.33:33847 --> 194.88.105.150:24
[172.16.1.33:33847 --> 194.88.105.150:24]

BUILD HERA
[194.88.105.150:24 --> 172.16.1.33:33847]

! LOLNOGTFO*
[194.88.105.150:24 --> 172.16.1.33:33847]

DUP
103.20.3.184:23 --> 172.16.1.42:35116

CLOSING YOUR CLOUD SECURITY GAPS: INTRODUCING CHECK POINT CLOUDGUARD IaaS

Understanding your role in the shared responsibility model versus that of your cloud provider helps you make the best decisions concerning the security of your cloud. It also ensures that your cybersecurity strategy aligns with your business goals while delivering consistent protections for all corporate data both on-premises and in the cloud.

Check Point's flagship CloudGuard IaaS Cloud Security solution is designed to keep data in cloud networks safe from even the most sophisticated attacks. To help fulfill the customer side of the shared security responsibility model, Check Point partners with leading public IaaS providers and SDN solutions to seamlessly deliver the same comprehensive security protections safeguarding premises-based networks to cloud environments.

With CloudGuard IaaS, customers can enforce consistent security policies for corporate assets across both virtual and physical infrastructures, dramatically simplifying compliance with regulatory mandates. What's more, Check Point provides full threat visibility, compliance reporting and multi-cloud connectivity to help organizations embrace the cloud with confidence.

Private Cloud Security

Supporting leading network virtualization solutions such as VMware NSX and Cisco ACI, Check Point CloudGuard IaaS enhances native micro-segmentation capabilities to proactively prevent the lateral spread of threats within software-defined data centers (SDDCs). Check Point also integrates with private Cloud Management platforms such as VMware NSX, VMware vCenter, Cisco ACI and OpenStack to facilitate automated security service insertion and contextual information sharing as well as automated quarantine and remediation of infected VMs. CloudGuard IaaS delivers the visibility and control to effectively manage security in both physical and virtual data center environments – all from a single unified management solution.

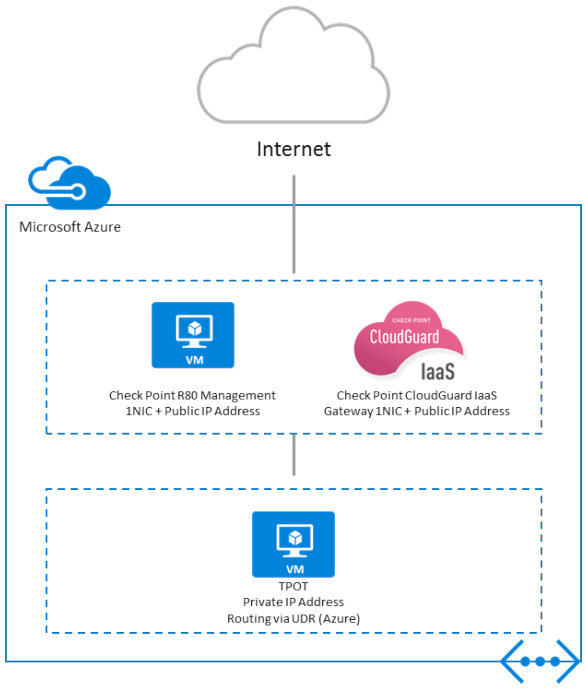
Public Cloud Security

CloudGuard IaaS extends advanced security protections to leading public and hybrid cloud environments such as Amazon Web Services, Microsoft Azure and Google Cloud Platform. Flexible and expandable, CloudGuard IaaS fits the dynamic needs of public cloud deployments, enabling secure connectivity from enterprise premises networks to the cloud while inspecting all data entering and leaving private subnets in virtual private clouds (VPCs).

Data Center Virtualization and Network Function Virtualization (NFV)

Check Point CloudGuard IaaS supports popular hypervisor technologies such as VMware ESX, Microsoft Hyper-V and KVM for virtual data center and Network Function Virtualization (NFV) environments. CloudGuard IaaS equips service providers with comprehensive threat prevention security, zero-day protections, agile delivery, management, and automation across core network function, software-defined WAN and vCPE deployments.

DEPLOYING CLOUDGUARD IaaS WITH OUR TPOT



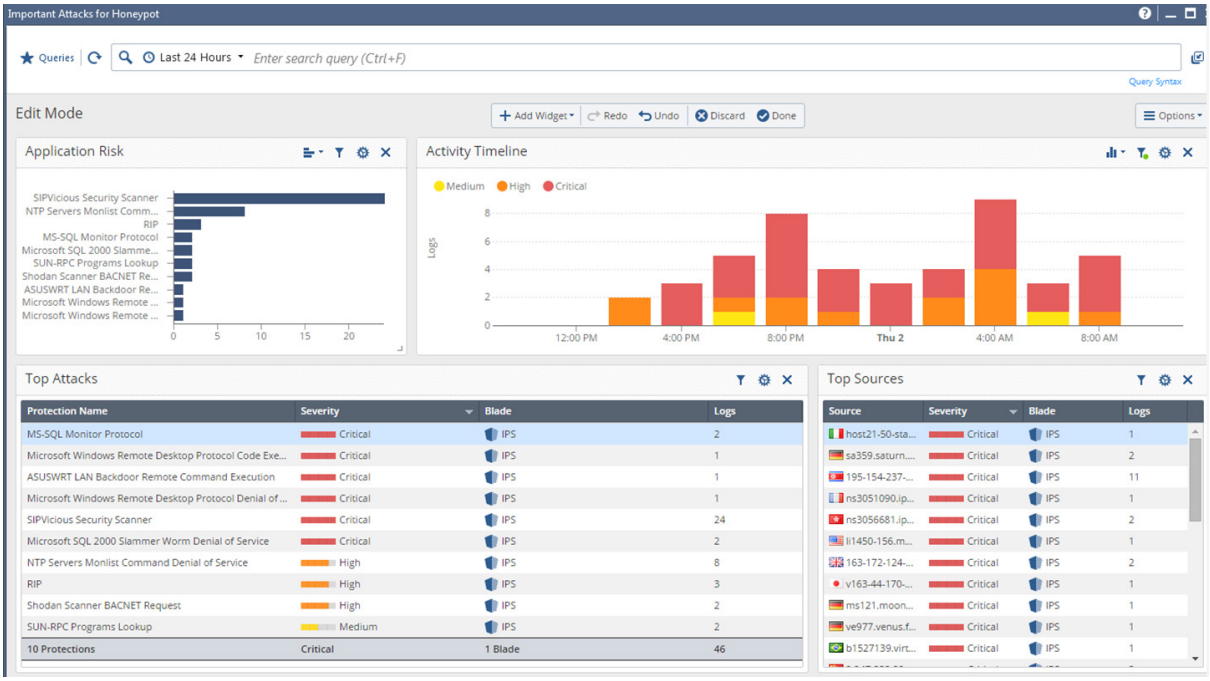
To demonstrate the value of using advanced threat prevention security for the cloud, we placed a Check Point CloudGuard IaaS Gateway in front of our TPOT and connected it to Check Point's Smart Center R80 management server.

The adjacent diagram shows our deployment in the Azure cloud using a single Check Point Security Gateway (1-NIC) and a dedicated R80 Management.

The CloudGuard IaaS deployment in front of our honeypot was configured for inspection only, not for blocking any traffic. For production environments it is highly recommended to configure your CloudGuard IaaS gateway for blocking malware and other malicious payloads to ensure the highest degree of security.

Nonetheless, the attacks witnessed against our TPOT are clearly visible on the Check Point gateway. CloudGuard IaaS was able to easily identify the attacks against our cloud service but more importantly could be easily configured to actively block these and other attacks from affecting our environment.

Below is a sample of the threat data gathered by our CloudGuard IaaS deployment and further analyzed by our Check Point R80 Smart Event manager.



A strong security posture includes not only the ability to identify and block threats but also to manage consistent policies with full logging and reporting across all environments – including on-premises and cloud environments. Check Point's R80 Security Management provides one the industry's most comprehensive solutions to effectively manage the security posture of today's cloud-enabled businesses.

SUMMARY

The appetite for cloud solutions shows no signs of slowing down. Still, security concerns are often cited as a key barrier to wide-scale enterprise cloud adoption. When you move computing resources and data to public clouds, security responsibilities become shared between you and your cloud provider.

Unfortunately, the native security capabilities of cloud providers do not offer the same robust protections customers enjoy on their premises-based networks, leaving cloud environments exposed and unprotected. In this paper, we explored first-hand the challenges organizations face when moving assets to the cloud.

The examples highlighted in this document were based on a typical customer cloud environment and are intended to inform customers of the risks they are likely to face. We also explored how modern IT-based security solutions like Check Point CloudGuard IaaS can help customers close their security gaps in the cloud while fully supporting the dynamic and agile nature of virtualized environments.

CloudGuard IaaS provides industry-leading advanced threat protection and single pane of glass management for easily extending advanced security protections to cloud environments. CloudGuard IaaS ensures that your cyber-security strategy aligns with your business goals while delivering consistent protections for all corporate data – both on-premises and in the cloud.

Discover how customers are leveraging CloudGuard IaaS to enhance their cloud security on leading platforms

Microsoft	Cisco	VMware	AWS

To learn more about Check Point CloudGuard, please visit:
https://www.checkpoint.com/products/cloud-security/