Cloud Security

Prinsip Keamanan

CIA

- Kerahasiaan (confidentiality):
  Pencegahan dari pengungkapan yang tidak sah secara disengaja atau tidak terhadap sebuah konten
- Integritas (integrity):
  Jaminan bahwa pesan terkirim adalah pesan yang diterima dan tidak diubah.
- Ketersediaan (availability):
  keandalan dan stabilitas dalam jaringan dan sistem

What is Cloud Security?

Cloud

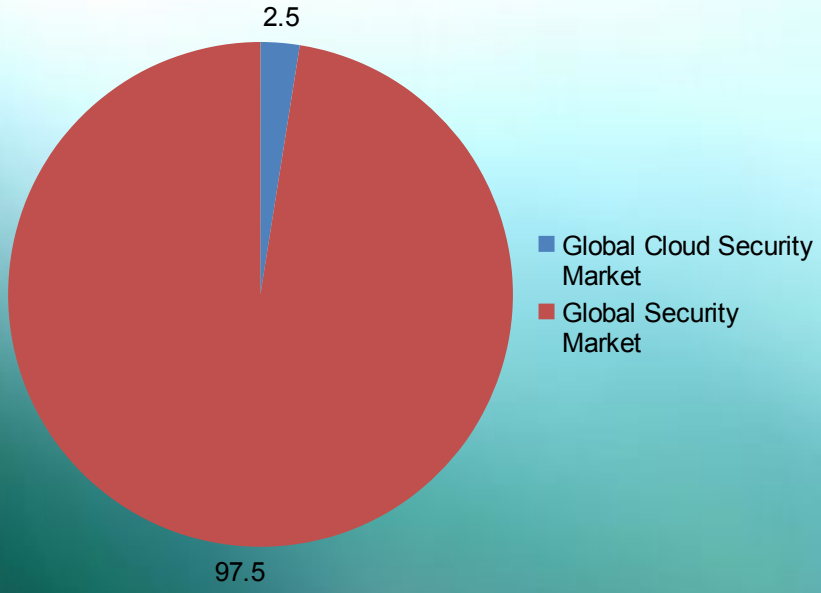
- Agility
- Self-service
- Scale
- Automation

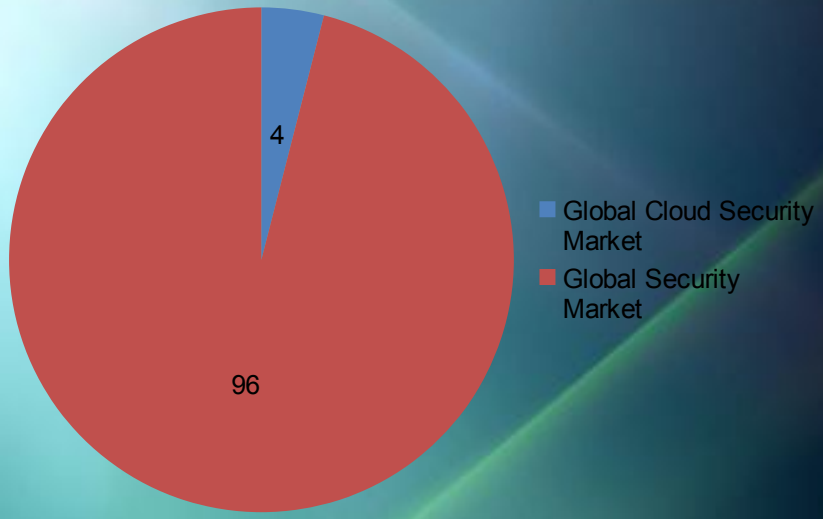
Security

- Gate-keeper
- Standards
- Control
- Centralized

Cloud Security is security principles applied to protect data, applications and infrastructure associated within the Cloud Computing technology.

Global Cloud Security Market in Percentage

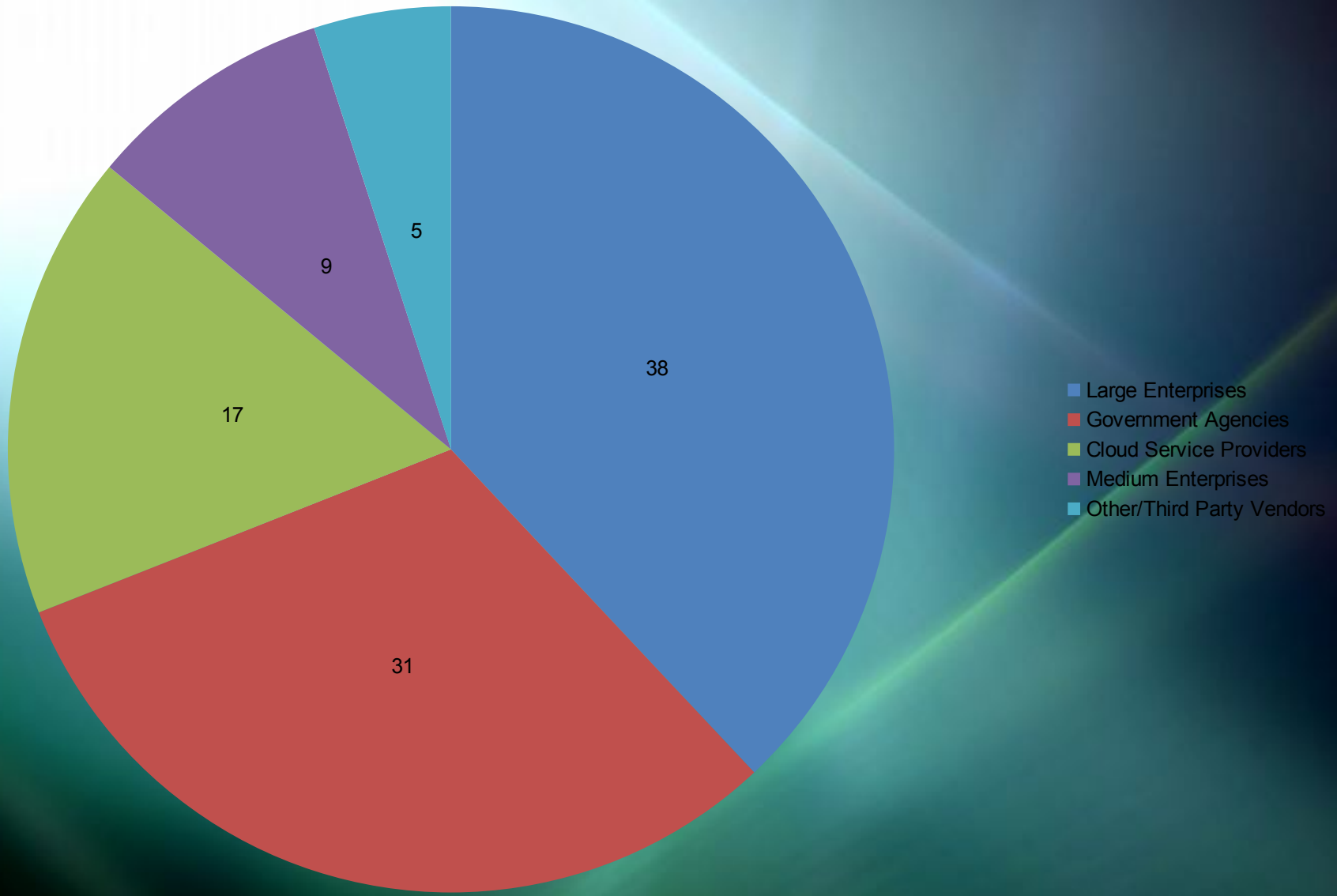




End-Users/Customers

- Large Enterprises
- Government Agencies
- Cloud Service Providers (CSPs)
- Medium-sized Enterprises

Global Cloud Security Market by End-User Segmentation



Trends associated with Cloud Security

- Increasing Partnerships between CSPs and Security Solution Providers Expected
- Increasing Emergence of Cloud Service-specific Security Solution Providers
- Identity Management and Encryption to Remain the Top Cloud Security Solutions Offered
- Increasing Availability of Cloud Security Solutions for Small and Medium-sized Businesses (SMBs)
- Emergence of Strong Cloud Security Standard and Guidelines

Why is Cloud Security Important

- Increasing Usage of Cloud Services in Non-traditional Sectors
- Growing Adoption of Cloud Services in Government Departments
- Rise in Cloud Service-specific Attacks
- Growing Usage of Cloud Services for Critical Data Storage
- Rise in Employee Mobility

What are the challenges?

- CSPs believe that Security is End-users' Issue
- Lack of Awareness about Cloud Security
- Inconsistent Network Connection Issues
- Lack of Proper Cloud Security Standards

What End-users/customers expect from Cloud Security

- Strong Overall Security Offered
- Suite of Security Solutions Offered
- Encryption Key Management Features Offered
- Availability of Fine Granular Control

McAfee Inc.

- McAfee Inc., founded in 1987, is a leading provider of network security solutions. The company is listed on the New York Stock Exchange and is based in California, US. The company provides security services across the globe. The company’s security products are for sectors such as Data Protection, Email and Web Security, Endpoint Protection, Mobile Security, Network Security, Risk and Compliance, Security Software as a Service (Security SaaS), and Security Management.

McAfee acquired by Intel

- On August 19, 2010 Intel acquired McAfee for $7.68 billion in a cash deal. In FY2010, the company reported total revenue of US$2.1 billion. However, in FY2010, the revenue from the Cloud Security segment was low, at only around US$25 million.

McAfee Cloud Security Program

McAfee Security-as-a-Service delivers complete endpoint, email, web, and network protection through the cloud, saving your IT department time, effort, and costs. As part of our Security Connected framework that delivers comprehensive security and integrated management, McAfee Security SaaS leverages the power of the cloud to help organizations realize faster time-to-protection to secure their business.

McAfee SaaS Includes

- McAfee SaaS Email Protection
- McAfee SaaS Integrated Suites
- McAfee SaaS Endpoint Protection
- McAfee SaaS Vulnerability Management
- McAfee SaaS Web Protection

SWOT Analysis

Strengths

- The company's cloud access control solution allows control over the entire lifecycle of cloud access security, providing solutions such as SSO, provisioning, strong authentication and audit.
- Its solution helps in auto-synchronization of identity data between enterprise and cloud applications for change management scenarios
- Centralized management and reporting are provided through integration with the

Weakness

- Despite being an established traditional security solution provider with a wide geographic presence, the company is slow to gain share in the cloud security space
- Some pure-play companies such as Symplified are witnessing much higher growth in the Cloud Identity Management market
- Some of its competitors, such as Trend Micro, provides better key management options/features

SWOT Analysis

Opportunities

- The company has a very long list of partners from various geographic locations, which it can leverage to expand
- It recently launched its cloud security platform, which secures all content and data traffic including email, web and identity traffic; thus, providing a unified solution

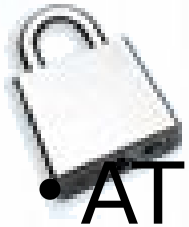
Threats

- Threat from pure-play vendors such as Zscaler, Vshield from VMware and Symplified that have high growth rates
- Threat to its market share from other traditional security solution providers that are expected to aggressively push for expansion in this market

Some Key Competitors

- Trend Micro SecureCloud, and Trend Micro Deep Security
- CA Access Control, and CA Identity Manager
- Symplified Mobile Edition, Symplified Access Manager, and Symplified Identity Manager
- CloudPassage cloud server exposure management
- Okta Cloud Services Platform
- GuardTime Keyless Signature Server
- CipherCloud Data Protection for Salesforce

Major Customers



- AT&T Global Network Services Client
- Citrix
- Microsoft VPN
- Juniper Networks
- Verizon

Other Information

Knowledge base Website
https://kc.mcafee.com/corporate/index?page=home
Security as a service by Mcafee
http://www.mcafee.com/us/products/security-as-a-service/index.aspx

Netflix

Netflix is a commercial entertainment web based company, by online subscriptions they provide website TV shows and movies to subscribers with the online streaming technology and also send DVD’s using US mail service.

In 2010, Netflix started migrating its infrastructure to Amazon EC2. At present Netflix has over 1 Petabyte of data stored on Amazon, and the data are sent to content delivery networks such as Akamai, Limelight etc., that feed the content to local ISPs.

What Netflix is now?

- 24+ million members globally
- Streaming in 47 countries
- Watch on more than 700 Devices
- 33% of US peak evening Internet traffic

Why Did Netflix moved to Cloud

- Netflix is growing and adding subscribers at an unprecedented rate. The company is expanding into global markets, and an ever-growing array of Netflix-ready devices is spurring streaming service to even faster growth. At the heart of Netflix technology is the Cloud Computing platform, which serves as the distributed systems foundation for Netflix application development, and powers the movie viewing experience for millions of customers every day.

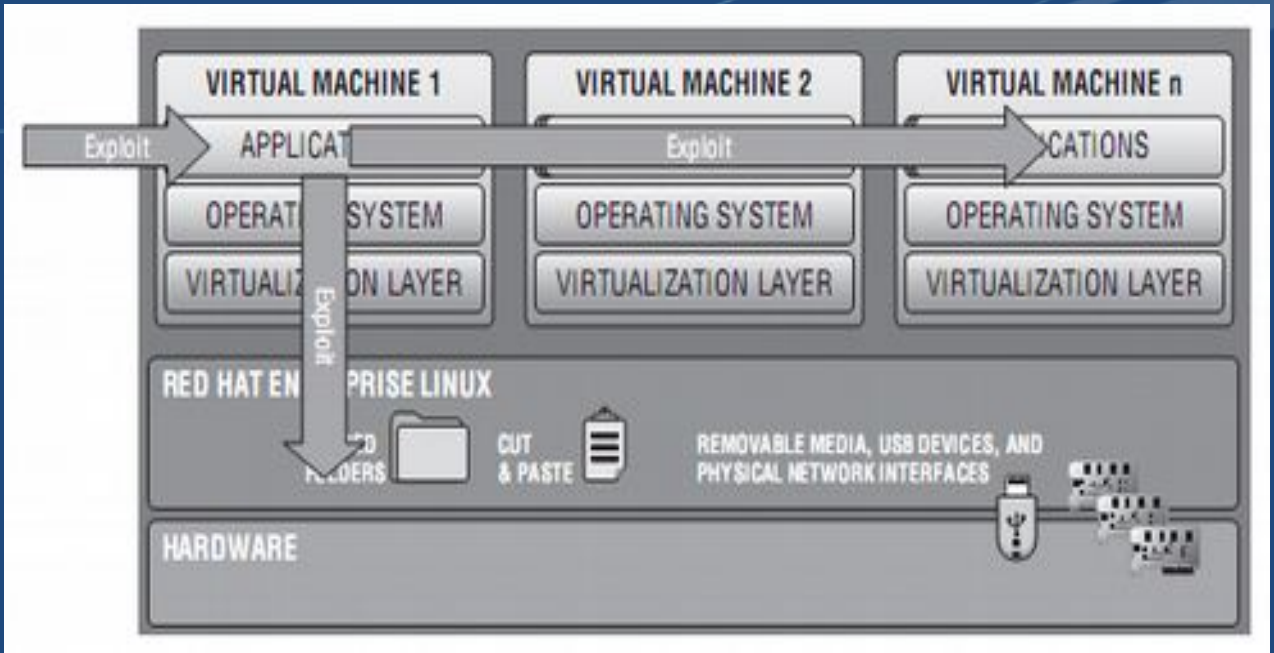
Netflix Cloud Security Strategy

- New deployments and upgrades
- Capacity planning & procurement
- Key management
- Detecting instance changes
- Application ownership, management
- Patching, updating
- Availability, in a failure-prone environment
- Embedding security controls
- Least privilege enforcement
- Testing/auditing for conformance
- Consistency, conformity in build and launch
- Continuous, aggressive monitoring, testing

Kontrol Keamanan

Implementasi kebijakan keamanan	Deteksi dan respon intrusi komputer	Manajemen keamanan virtualisasi

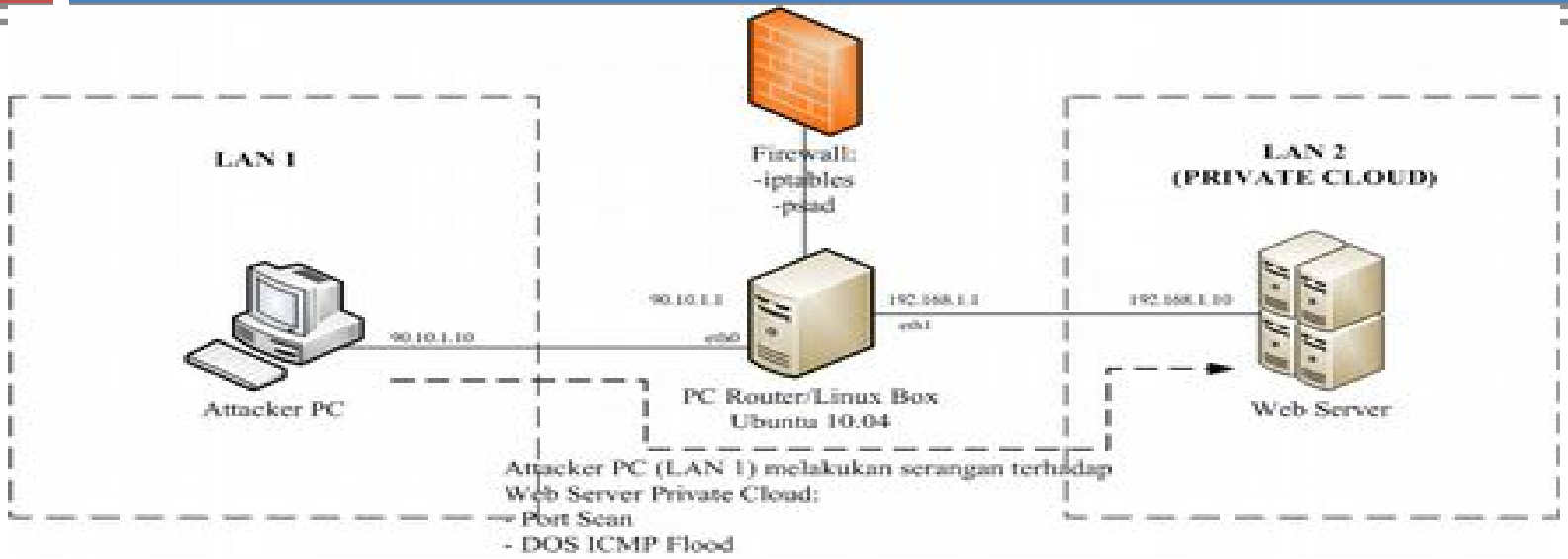
Kerentanan sistem dasar mesin virtual



Idealnya, perangkat lunak kode operasi dalam sebuah virtual mesin tidak mampu berkomunikasi atau mempengaruhi kode yang berjalan baik pada host fisik itu sendiri atau dalam sebuah mesin virtual yang berbeda

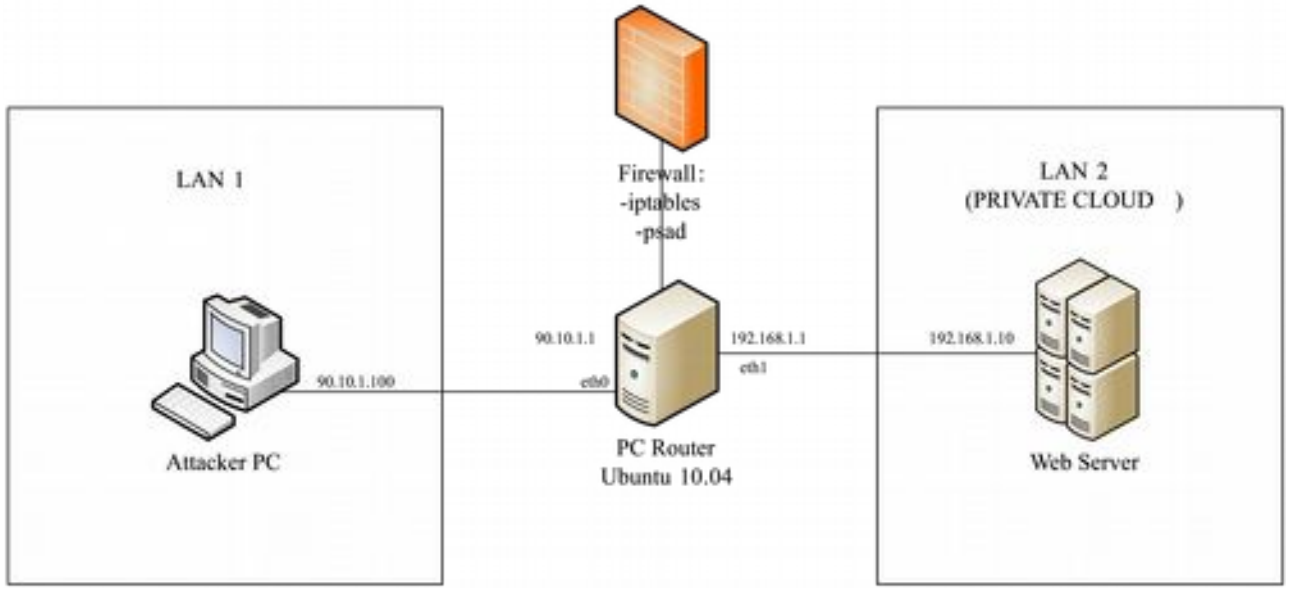
Kerentanan utama yang melekat dalam hypervisor terdiri dari rootkit hypervisor jahat, modifikasi eksternal hypervisor, dan menghilangkan mesin virtual.

- **Pengujian Sistem Keamanan**



1.PC Router Sebagai Firewall (Pengujian 1)
2.PC Router Sebagai Firewall dan Log Analysis (Pengujian 2)
3.PC Router Sebagai Firewall , Log Analysis dan IDS (Pengujian 3)
4.PC Router Tanpa Firewall, Log Analysis dan IDS (Pengujian 4)

- **Contoh Topologi untuk keaamanan**



- **Metode Pengujian:**

1. Setiap pengujian menggunakan tools uji keamanan, dilakukan 2 kali percobaan.
2. Pengujian DOS ICMP dilakukan selama 30 detik setiap 1 percobaan.
3. Untuk kemudahan dalam menganalisa *file log*, setiap pengujian file log akan di-*restart*.

Teknik Penyerangan

- Ancaman Utama _perangkat lunak berbahaya yang memungkinkan virus komputer atau malware lain yang membahayakan sistem satu pelanggan untuk menyebar ke hypervisor dan akhirnya ke sistem pelanggan lain.

Teknik Pencegahan

- Teknik yang bisa digunakan adalah melakukan integritas dari hypervisor yang mendasarinya dengan melindungi dari malware yang mungkin didownload oleh pengguna individu, dengan demikian, kita dapat memastikan isolasi hypervisor

Teknik kuncian yang disebut memori nonbypassable, yang secara eksplisit dan terpercaya dalam pengenalan kode baru oleh pihak lain selain administrator hypervisor. Hal ini juga mencegah upaya untuk mengubah kode hypervisor yang ada dengan pengguna eksternal.

Menggunakan teknik yang disebut pengindeksan pembatasan pointer. Teknik ini melihat perilaku normal ciri sebuah hypervisor, dan kemudian mencegah penyimpangan apapun dan profil itu, hanya administrator hypervisor sendiri bisa memperkenalkan perubahan kode hypervisor.

Tindakan Pencegahan

- Penguatan sistem operasi host
- Pembatasan akses fisik terhadap host
- Menggunakan komunikasi terenkripsi
- Menonaktifkan background task
- Updating dan penambalan
- Mengaktifkan Perimeter Pertahanan di mesin virtual Implementasi pemeriksaan integritas file
- Pengelolaan backup