Bitdefender® ENTERPRISE

# Bitdefender Enterprise Security Solutions

Overview

㈜ 비에이솔루션즈

# Agenda

1. Bitdefender at a glance
2. Bitdefender's technologies and industry recognitions
3. Bitdefender Enterprise Solutions
   - Gravity Architecture
     - Security for Virtualized Environments
     - Cloud Security for Endpoints
     - New Enterprise Solution (Unified Security)
   - On-premise Business Solutions v3.5
     - Client Security
     - Servers Security
4. Technical Support and Professional Services

# Bitdefender at a glance

# Over a decade of innovation

**2000**

-

-

-

-

**2005**

-

-

-

-

**2012**

-

- 1st antivirus product with **intelligent updating**
- 1st antivirus product with **application firewall**
- IST prize for MIDAS, ***"set to revolutionize AV design"***
- **Linux Samba 3**를 대상으로 antivirus 제품 최초 상업화
- New **hourly update system** from Bitdefender
- New "Behavioral Heuristic Analyzer in Virtual Environments" (**B-HAVE**)
- **Active Virus Control (AVC)**를 통한 미확인 바이러스의 실시간 감지
- 어느 컴퓨터라도 60초에 스캔이 가능한 **Fastest online scanner**
- New **Gravity Enterprise Architecture** for highly scalable services
- 1st VMware vShield 5 integrated solution for **virtualized datacenters**
- Gravity Architecture에 기반한 새로운 **Cloud Security services**

# Bitdefender multi-layer protection

## Certified antivirus engines

다양한 수상 경력의 Bitdefender의 antivirus scan engines은 선도적인 antimalware 방어 능력으로 인해 ICSA Labs, Virus Bulletin, West Coast Labs, Checkmark 와 같은유수의 인증 기관으로부터 인정받았습니다.

Bitdefender는 다음과 같은 다양한 레벨의 수준 높은 보안 서비스를 제공합니다: Antivirus, Antispyware, Anti-phishing, Trojan / Rootkit detection, 침입 탐지 기능을 갖춘 완전 기능의 이중 개인 방화벽.

**Antivirus** - signature 기반의 detection 기능에 더해, Bitdefender는 컴퓨터 내에서 가상 컴퓨터를 가동하는 heuristic detection 기능을 제공하여 모든 파일과 코드를 확인하여 악성코드를 찾아냅니다. 이러한 기술로 인해 zero-day와 알려지지 않은 위협에 대해 오류를 줄어든 대단히 높은 탐지율을 나타내게 됩니다.

**Anti-Spam** – 알려진 스팸 사이트에 대한 상시 업데이트 blacklists와 whitelists를 사용함으로써, Bayesian 방법을 통해 정적인 스팸필터를 우회하는 변종을 탐지하도록  또다른 layer of detection을 제공합니다.

**Antispyware** - Bitdefender Client Security는 modifications, file scanning, cookie control, URL filtering , content inspection하는 registry 를 모니터하는 5 개의 필터링 기법을 통해 이미 알려진 spyware와 adware를 탐지하고 예방하여 외부로 데이터가 새어 나가는 것을 예방합니다.

**Anti-phishing** – 기업체 수준의 위협보다 개인적인 수준의 위협이 많다는 것을 고려하면 phishing sites는 기업체 직원들로부터 정보를 더 많이 빼내갈 수 있습니다. 수시로 업데이트 되는 blacklists와 whitelists를 이용하여 Bitdefender 사용자가 phishing sites에 접근하지 못하게 하며 정보를 누설하는 것을 예방합니다.

**Content Filtering** - Content filtering으로 credit card or account information, report names, client databases, etc 과 같은 사전에 정의된 정보가 회사 밖으로 나가는 것을 탐지할 수 있습니다.

**Firewall** – 사용자가 보안성이 없는 무선 네트워크를 이용하여 외부에서 원격으로 작업을 할 때는 회사의 외곽 방화벽으로 더 이상 보호받지 못합니다. Internet blocking and access by IP address, application, port or protocol 과 같은 Granular settings는 flexible configuration options이 가능하게 하면서 내외부 침입의 위협에 대해 최상의 보안을 유지합니다.

# Bitdefender technologies

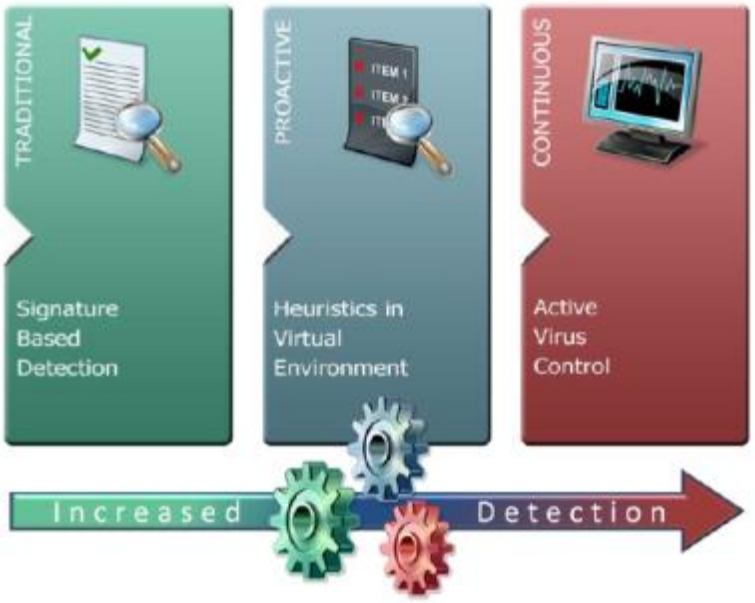
## B-HAVE – ADVANCED HEURISTIC DETECTION

Heuristics는 컴퓨터가 위험에 처해 있을 경우 윈도우를 닫아버리는 사전예방적인 탐지 방법입니다. 기존의 탐지 방법은 signatures에 의존하고 있었습니다. 이러한 signatures란 실제 악성코드 샘플들에서 뽑아낸 단편적인 코드들이며 pattern-matching 을 위해 antivirus programs들이 사용하는 것입니다. 이러한 방법의 문제점은 signature를 생성하는데 시간이 걸린다는 것으로 antivirus 업체들이 악성코드 샘플을 채취하고 signature를 만들어 그 signature를 사용자에게 밀어내야 하는 것입니다. – 이런 일이 앞서 말한 윈도우의 경우를 발생시키는 겁니다. Heuristic detection도 signatures에 의존합니다만 단순한 fingerprint 이상의 것으로 어느 application이 악성이다는 것을 지시해주는 실제 behaviors를 specify 하는 signatures입니다. 이것은 악성 프로그램들은 다른 프로그램은 하지 않는 어떤 action을 불가피하게 시도하기 때문에 의미가 있습니다. heuristic scanners 는 단순히 pattern-matching에만 의존하지 않고 행동적 특징을 찾기 때문에 signature (즉, fingerprint)가 아직 나오지 않은 새로운 미래의 위협을 탐지하고 차단할 수 있습니다.

**B-HAVE** 는 BitDefender의 특허 기술로 만든 heuristic 탐지 엔진입니다. 컴퓨터를 보호하기 위해서 BitDefender B-HAVE heuristic engine을 포함한 heuristic scanners 대부분은 실제 컴퓨터로부터 완벽히 격리된 (sandbox에 저장) 가상 환경에서 code가 실행되는 동안 application이 가동하는 것을 잠시 delay시킵니다. 그 다음에 의심되는 행동이 발견되지 않는다면, 컴퓨터는 해당 applications을 정상적으로 구동하게 됩니다. 반면에, 의심되는 행동이 발견되면, 컴퓨터는 해당 프로그램을 차단하도록 지시를 받습니다. 이런 전체 과정이 수 초 안에 이루어지며, 그렇기 때문에 사용자가 느끼거나 컴퓨터의 성능에는 실질적인 영향이 없습니다.

# Bitdefender technologies

## Bitdefender AVC - Proactive and continuous real-time protection




Bitdefender AVC (Active Virus Control)는 실시간으로 새로운 잠재적 위협을 탐지하는 heuristic methods를 사용하는 혁신적이며 선도적인 탐지 기술입니다. 시스템 상에서 가동하는 각각의 프로세스를 모니터하며 프로그램이 실행되는 동안 그리고 종료 후에도 악성코드 같은 행동들을 주의 깊게 관찰합니다. 의심되는 행동이 탐지되면 해당 프로그램은 위해하다고 선언됩니다. 처음 시작할 때 파일만을 확인하는 다른 heuristic 기술들과 달리, Active Virus Control은 시스템 상에 존재하는 동안 Application이 수행하는 모든 것을 항상 모니터합니다.

모니터링은 프로세스 시작 시에 DLL을 통해 이루어지는데 그것은 각각의 프로세스마다 하나의 감시자가 프로세스 전체 과정 동안 같이 한다는 의미입니다. 이 감시자는 서버에 일정한 행위들을 보고하며 서버는 위해한 행위의 숫자, 진행된 프로세스 형태에 따라 어떤 프로세스가 악성으로 등급을 매겨야 할 지 결정을 해 줍니다.

# Bitdefender technologies

## NEUNET – ADVANCED ATISPAM TECHNOLOGY

Spammers들은 필터를 우회하기 위한 정교한 방법들을 계속 개발합니다. 일반적으로, 이러한 것들은 이전에 보낸 것들보다 새롭고 다양한 이메일 “waves”를 수반하게 되며 spammer들은 각 wave 마다 성공한 것들을 분석하여 다음 번의 spam wave에 반영하게 됩니다.

**NeuNet**은 스팸 메시지 wave에 pre-trained된 일련의 neutral networks를 사용하는 “intelligent” spam filter 입니다. 이 networks 자체는 가장 최신의 spam waves를 이용하여 Bitdefender Labs에서 trained and updated 되었습니다. 이 networks는 연속적인 filtering layers로 기능하도록 만들어졌으며 위해한 메시지로부터 정상적인 메시지를 구분하는 데 탁월하며, 피싱 스팸이나 싸구려 모조품 시계를 광고하는 스팸 등 사전에 파악된 스팸 카테고리를 월등한 정확성으로 구분해내는 subsequent layers를 포함한 최고의 네트워크 입니다.

pre-trained neural networks의 한가지 탁월한 장점은 training set의 동일한 카테고리에 해당하는 새로운 email spam을 구분해 내는 능력입니다. 다른 하나는 여러 경우에 있어 legacy rules-based filters 보다 더 빠르게 기능한다는 것입니다. Bitdefender 고객사 컴퓨터에서가 아니라 Labs에서 training이 이루어지는 이유는 두 가지 서로 다른 이유 때문인데 그것은 성능 (training is quite processor-intensive) 과 정확성(the Labs can gather and classify much more diverse and recent spam than any one client machine could, making the training that more accurate) 때문입니다. Spammers들은 필터를 우회하기 위한 정교한 방법들을 계속 개발합니다. 일반적으로, 이러한 것들은 이전에 보낸 것들보다 새롭고 다양한 이메일 “waves”를 수반하게 되며 spammer들은 각 wave 마다 성공한 것들을 분석하여 다음 번의 spam wave에 반영하게 됩니다.

# Bitdefender today

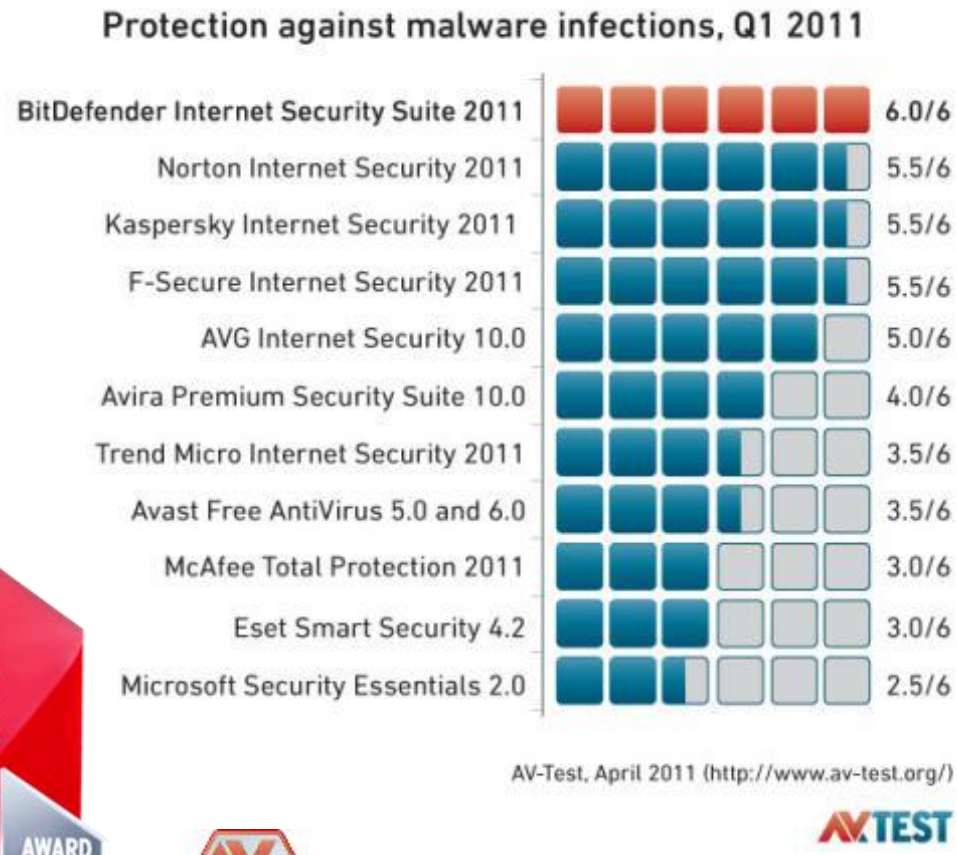
- The #1 Antimalware Security Technology in the world
  - **미국, 영국, 독일**의 주요 기관들의 동시 최고 추천!
  - 유수의 보안업체가 사용하는 기술: **F-Secure, G Data, Qihoo, Bullguard , IBM**
  - 18개의 Virus Bulletin Antispam 전체를 연달아 수상한 유일한 보안 회사
- Bitdefender의 기술은 전세계적으로 4억 명의 사용자를 지켜내고 있습니다
- 20개 이상의 언어로 현지화

# 1위 등극 보안 기술

On average, Bitdefender detects and shields against **120,000** new e-threats **per month** and adds over **4,000** new signatures **every day**

Bitdefender customers get around-the-clock protection with more than **16 updates per day,** or nearly **every hour**

The **only vendor** to score full 6 points AV-Test in Q1/2011 against malware infections and the winner of “Best Protection 2011” award



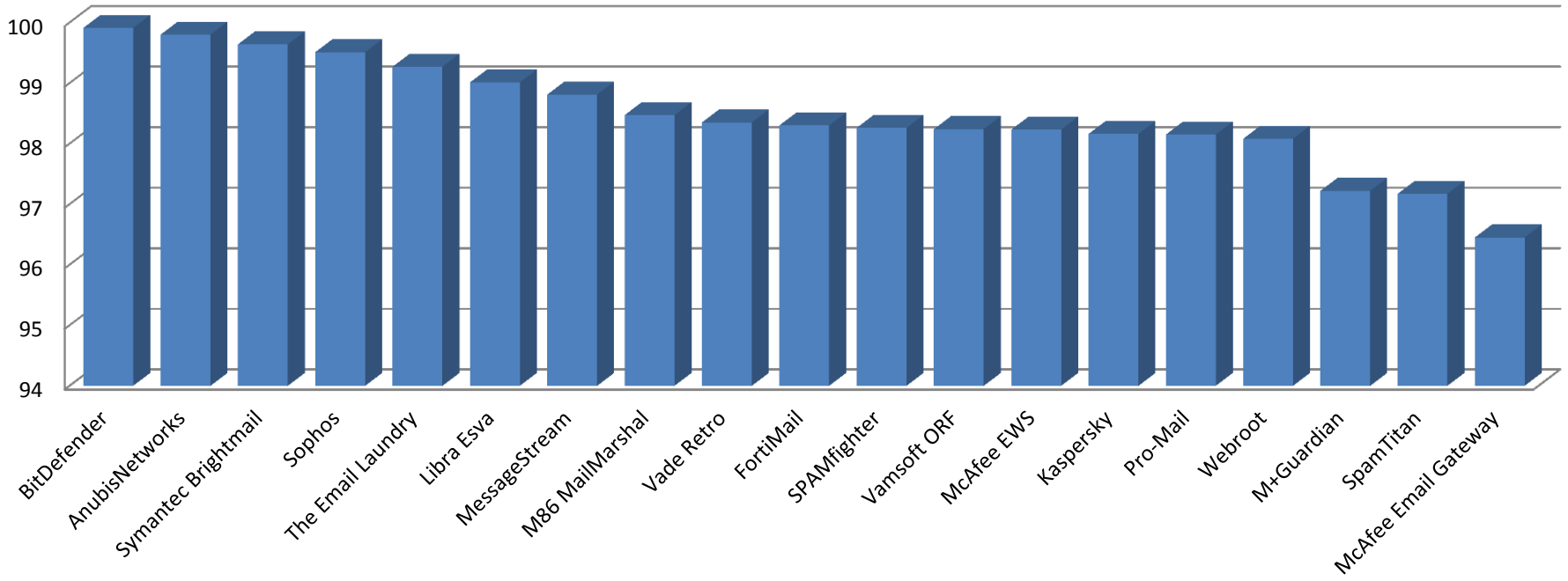






# VBSpam award in every single anti-spam test

- Bitdefender analyzes and issues protection for **5 million** spam messages **every day,** or about **35 million per week**
- Bitdefender has continuously ranked top in Virus Bulletin's (VB) tests for SPAM winning in September 2012 the **21st VBSpam award in a row**




**Virus Bulletin VBSpam September 2010**

# 수상 및 인증

## CRN: The Best Security Product of the Year 2011 Award

Bitdefender Business Solutions 3.5, December 2011

## AV-Comparatives “Seal of Approval”

Bitdefender Business Solutions 3.5, September 2011

## Virus Bulletin’s VB100 Awards

Bitdefender Client Security 3.5, File Servers 3.5, Samba 3.1.2

## Virus Bulletin’s VBSpam Awards

Bitdefender Security for Mail Servers 3.1.2, September 2012

### CITRIX READY

XenDesktop, XenDesktop Security for Virtualized Environments (April 2012)

### MICROSOFT CERTIFIED

for Windows 2010, 2008 R2 and Exchange 2010. Security for Windows Servers (December 2010)

### MICROSOFT COMPATIBLE

with Windows 7, Client Security 3.1.9 (December 2010)

### INTEROPERABILITY CERTIFIED

Business Solutions v3.5 (December 2010)

# Bitdefender Enterprise Solutions

- **GRAVITY ARCHITECTURE**
  - Cloud Security for Endpoints by Bitdefender
  - Security for Virtualized Environments by Bitdefender
  - **New Bitdefender Enterprise Security** (to be released in Q1, 2013)

- **(ON-PREMISE) BITDEFENDER BUSINESS SOLUTIONS (v3.5)**
  - **Centralized management**
  - **Endpoint protection**
    - Bitdefender Client Security
    - Bitdefender Antivirus for Mac
    - Bitdefender Antivirus Scanner for Unices
  - **Critical Server Protection**
    - Bitdefender Security for File Servers
    - Bitdefender Security for Samba
    - Bitdefender Security for SharePoint
  - **Gateway Services Protection**
    - Bitdefender Security for Mail Servers
    - Bitdefender Security for Exchange

# Overview of the current business solutions

| Bitdefender Enterprise Solutions | Primary Target Market | | |
|---|---|---|---|
| | Small | Medium | Enterprise/ xSP |
| On premise solutions (v3.5) | | √ | |
| Cloud Security for Endpoints | √* | | √** |
| Security for Virtualized Environments | | √ | √ |
| New Enterprise Security *** | | √ | √ |

* Service hosted by Bitdefender. Also, may target larger organizations with geographically distant sites or remote workforce.
** Very Large Enterprises and Services Providers can host their own Cloud Security Solution.
*** New on-premise solution, to be released soon.

# Bitdefender Gravity Architecture

# Bitdefender Gravity Architecture

Gravity Architecture는 Bitdefender Enterprise security solutions의 관리자용으로 광대한 확장성을 가진 platform을 제공하기 위해 Bitdefender가 개발한 독특한 혁신 기술의 집합체입니다.

Gravity Architecture는 그러한 기반과 cloud / 가상화 기술을 최대한 이용하여 설계되었으며 Bitdefender 가 물리적인 / 가상화된 / 모바일 환경 하의 모든 조직에 적합한 보안 솔루션과 서비스를 제공할 수 있도록 platform을 제공합니다.

Gravity Architecture가 탑재된 새로운 Bitdefender 기업용 솔루션은 아무리 거대한 조직이라고 하더라도 단 하나의 console로 고객 needs에 대응할 수 있습니다. 또한, Gravity Architecture는 security를 service (SaaS) offerings, Bitdefender 또는 service provider가 hosting하는 public cloud solutions, 중/대기업용의 private cloud deployments로 가능하게 합니다.

# CLOUD COMPUTING

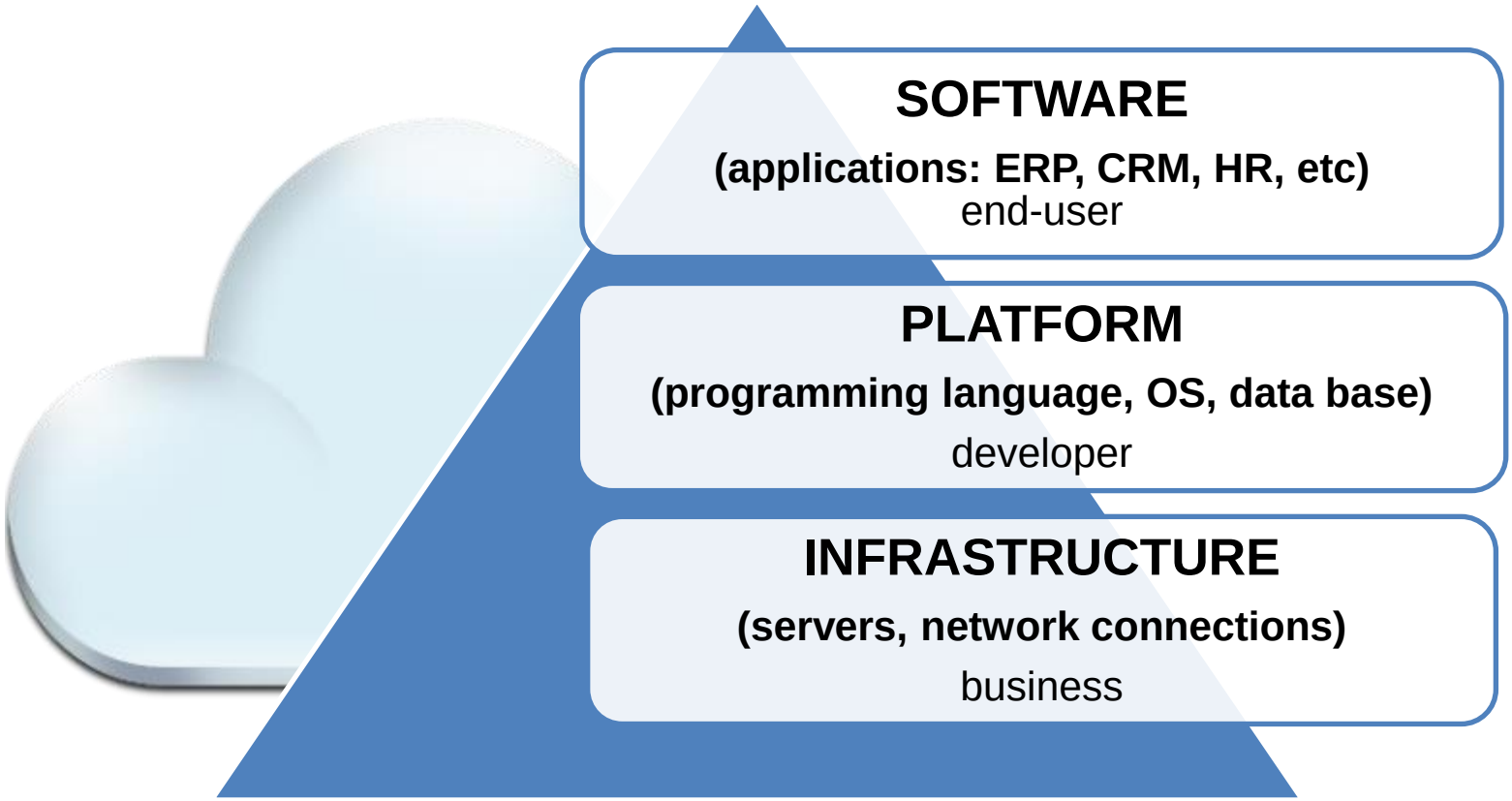
***Cloud Computing 이란?***

온라인 기술, 소프트웨어, 서비스를 사용하는 것입니다. 인터넷을 통해 제공되는 computing이며 on-demand computing 입니다.

- 인터넷과 원격 서버를 사용하여 데이터와 application을 유지하는 computing technology 입니다
- 설치하지 않고 applications를 사용할 수 있습니다
- Cloud resources는 필요할 경우에만 제공되는 (on an as needed basis) 서비스입니다
- 대량의 computing resources는 web browser와 같은 user interface를 통해 접근하는 가상 데이터센터로부터 공급됩니다
- 대규모 applications의 확장성에 대응하는 적절한 방법입니다
- 귀중한 IT 자원을 낭비하지 않고 다른 필요한 application을 사용할 수 있게 해 줍니다

**“It is an Internet infrastructure service where virtualized IT resources are billed on usage basis and can be provisioned and consumed on-demand using standard web-based interfaces”**

# The 3 Cloud Computing layers



# Cloud Service models:

**IaaS (Infrastructure as a Service)**

Cloud infrastructure services (즉, "Infrastructure as a Service (IaaS)“)는 가상화 환경의 platform으로 컴퓨터 infrastructure를 제공합니다. 서버, 소프트웨어, 데어터 센터의 space, 네트워크 장비 등을 구매하는 대신 고객사는 완전히 아웃소싱된 서비스로써 그러한 resources를 구매하는 것입니다. 서비스 비용은 utility computing basis와 사용한 resources의 합계를 기반으로 청구하기 때문에 비용은 실제 사용량만을 바용하게 됩니다. 이것은 web hosting과 virtual private server offerings의 진화된 내용이며 이러한 infrastructure는 장비를 실제로 구매하지 않아도 되는 것입니다.

**PaaS (Platform as a Service)**

운영체제 같은 computing platform이 인터넷을 통해 서비스되는 것입니다.

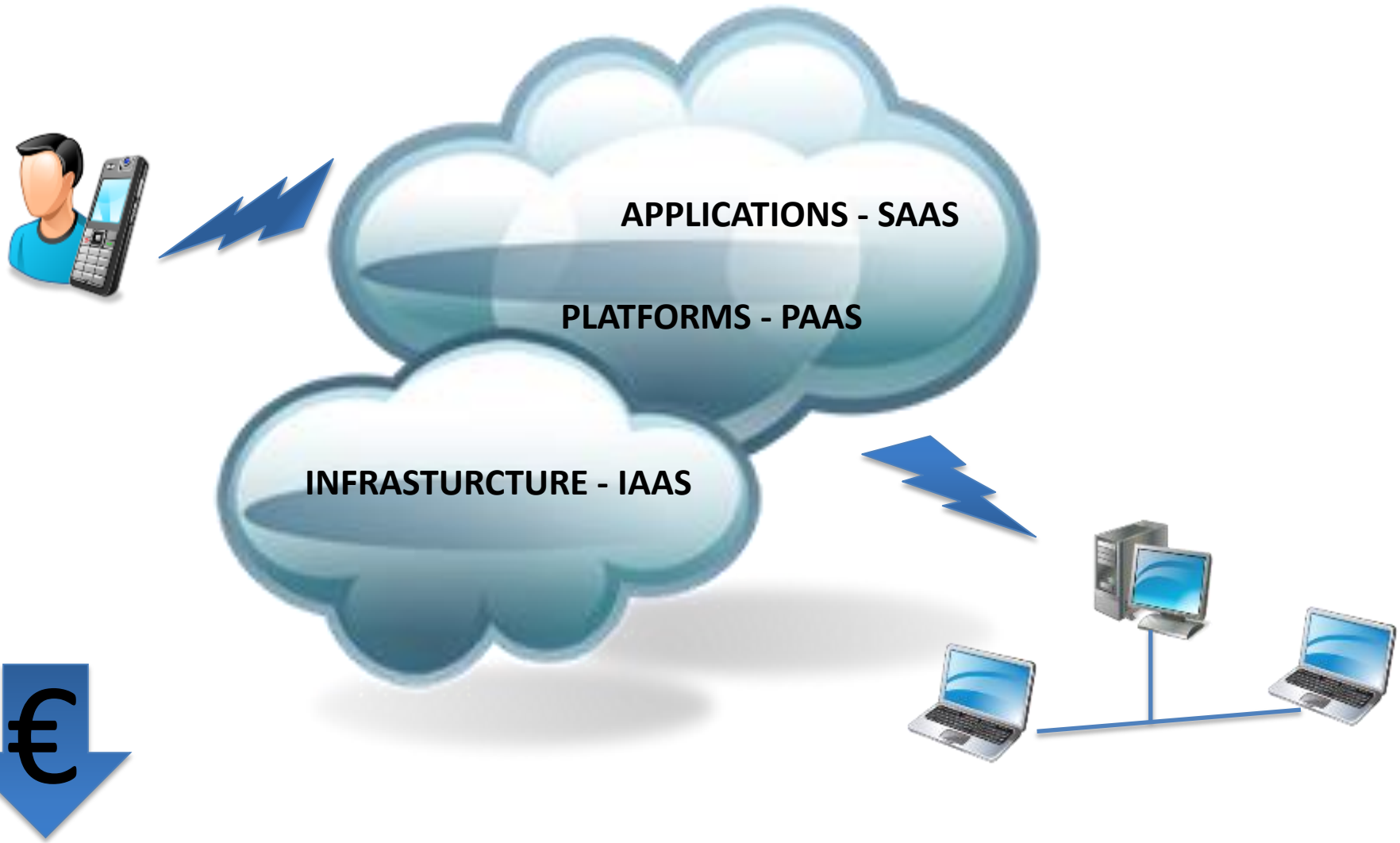
**SaaS (Software as a Service)**

인터넷을 통해 application이 서비스 되는 것으로 SaaS applications는 고객의 컴퓨터에 설치할 필요도 그러므로 실행할 필요도 없습니다.

SaaS software 공급업체는 자신들의 web server에 application을 올려놓거나 고객의 디바이스에 해당 application을 upload하면 됩니다. SaaS 공급업체를 Application Service Providers (ASP)라고도 부릅니다.

# Regular computing

# Cloud computing



# Cloud computing features

- Massive elasticity and scalability
- Improved performance
- Self service based model
- Highly virtualized and standardized infrastructures
- Inexpensive to purchase
- Consumption based billing (Pay-as-you-go)
- Free applications – wide range of users
- Higher trust, utilization and efficiency
- Reliable instant services
- Accessibility from any location connected to the Internet
- Multi-tenancy
- Simplicity and easy maintenance

# Cloud computing benefits

- Higher utilization at reduced cost
- More applications delivered to a large # of users
- More simple and efficient IT and software management
- No need to update or install software or hardware
- Very few parts to wear out
- Ability to work flexibly from anywhere – remote accessibility
- Instant access from any browser
- Unlimited usage
- Easy to maintain and update
- Cloud computers are more eco-friendly than a regular computer
- Security
- No risks

# Regular vs Cloud computing

| | Regular computing | Cloud computing |
|---|---|---|
| **SET-UP TIME** | days to weeks | minutes |
| **COSTS** | costly (high capitals), high costs for servers acquisition whether used or not | no upfront costs, pay-per-use, servers rent based on usage only |
| **WHAT YOU NEED** | Data center with security<br>Cooling and power supplies<br>Servers and storage<br>OS licenses<br>Security and software patches<br>Software upgrades<br>Equipment upgrades<br>Downgrades<br>Backup power supplies<br>Development, Staging, Production<br>Fail over<br>Disaster recovery<br>Rack space<br>Support<br>Maintenance<br>Replication | **INTERNET CONNECTION is needed**<br><br>**No** servers and hardware required to be bought<br>**No more** boxes<br>**No more** rack space,<br>**No more** costly engineers for support and maintenance<br>**No** wasted resources<br>- Security<br>- Reliability<br>- Scalability |

# Bitdefender Gravity Architecture

가상화와 cloud computing 기술의 광범한 적용은 Information Technology가 어떻게 전달되고, 실행되며 소비되는지에 혼란을 가져왔으며 새로운 보안 접근을 필요로 하게 됐습니다.

- **Virtualization** 은 최근의 데어터 센터, 증가하는 자원 사용, 시스템 지원 방법 등에 대한 새로운 능력자로 떠올랐습니다.
- **Cloud computing** 기술은 그러한 변화를 더욱 촉진하여 on-demand 공급, computing 사용자들의 확장성을 가능하게 하고 있습니다.

보안은 한 단계 올라서야 되며 IT 변화/변천보다 앞서나가서 변화하는 프로젝트를 보안문제를 희생하지 않고 성공할 수 있게 해야 합니다

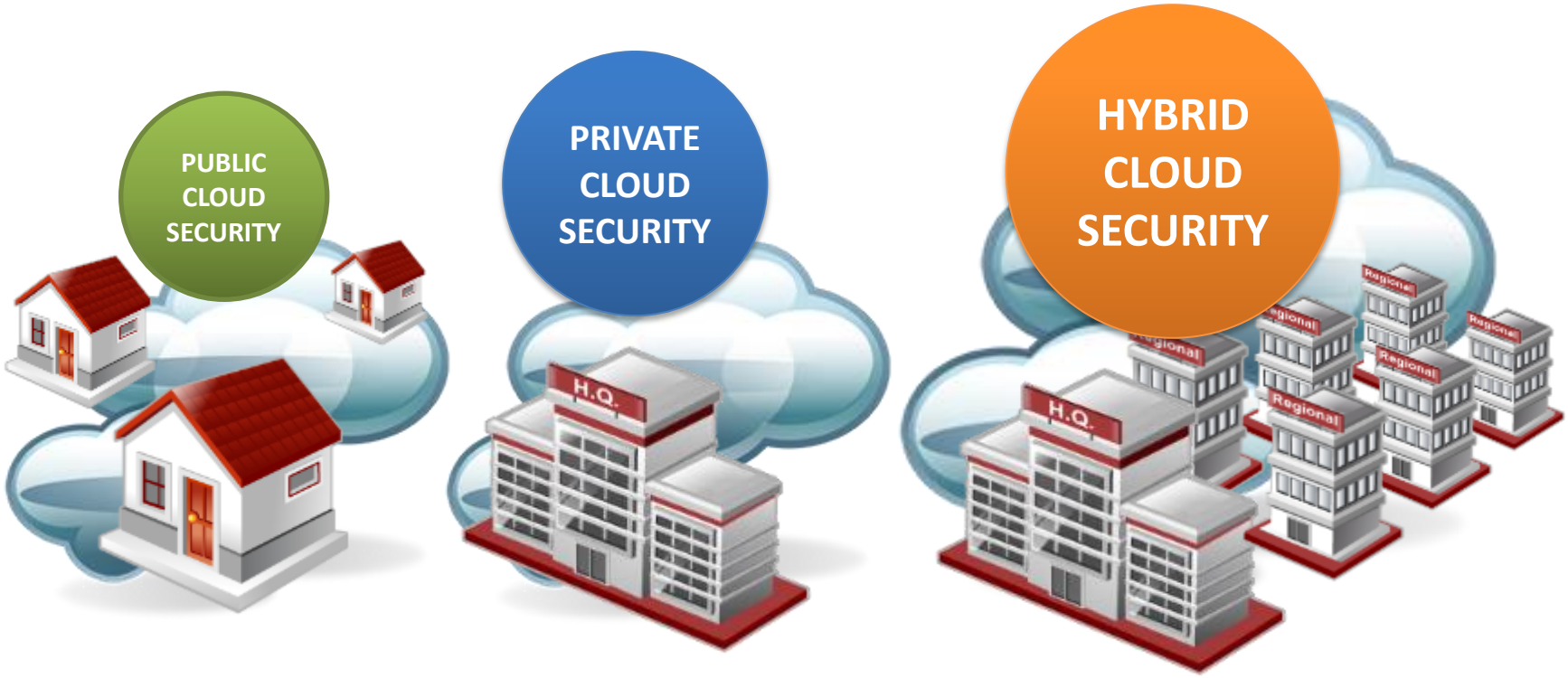
Gravity Architecture를 통해 Bitdefender는 security solutions의 패러다임을 바꾸고 있습니다. Bitdefender는 security solutions는 cloud computing의 특징과 장점들을 충분히 활용하여 폭넓게 확장 가능하며 유용한 platform을 제공하여 cloud computing의 모든 level에서 보안을 가능하게 합니다.

- Bitdefender는 security solutions는 Cloud Security solutions (SaaS offerings)와 infrastructure level에서 최적의 보안, 최근의 가상화된 데이터센터 보안을 가능하게 합니다;
- Bitdefender는 security solutions는 virtual container를 활용하여 Service Providers (xSP's)와 Very Large Enterprises (VLE's)에게 turn-key solutions를 가능하게 합니다.;
- Bitdefender는 security solutions는 여러 고객과 파트너들에게 흩어져 있는 물리적 / 가상 / 모바일 환경 모두를 단 하나의 console로 통합된 관리를 할 수 있게 합니다.

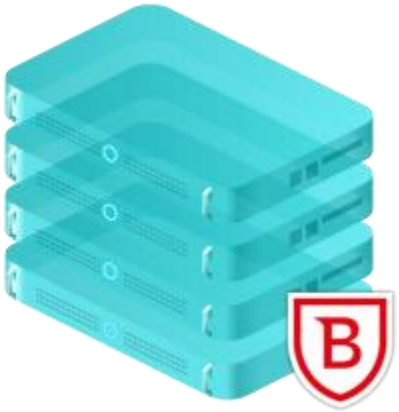
# Architecture for public, private and hybrid cloud

Gravity Architecture 기업체 옵션 3 가지:

1. Public cloud (2 - 100 endpoints 소규모 기업체용)
2. Private cloud (중/대규모 기업체의 1 개 사이트용)
3. Hybrid cloud (중/대규모 기업체의 다량 사이트용)



# New Enterprise-Class Business Solutions



## Security for Virtualized Environments (SVE)

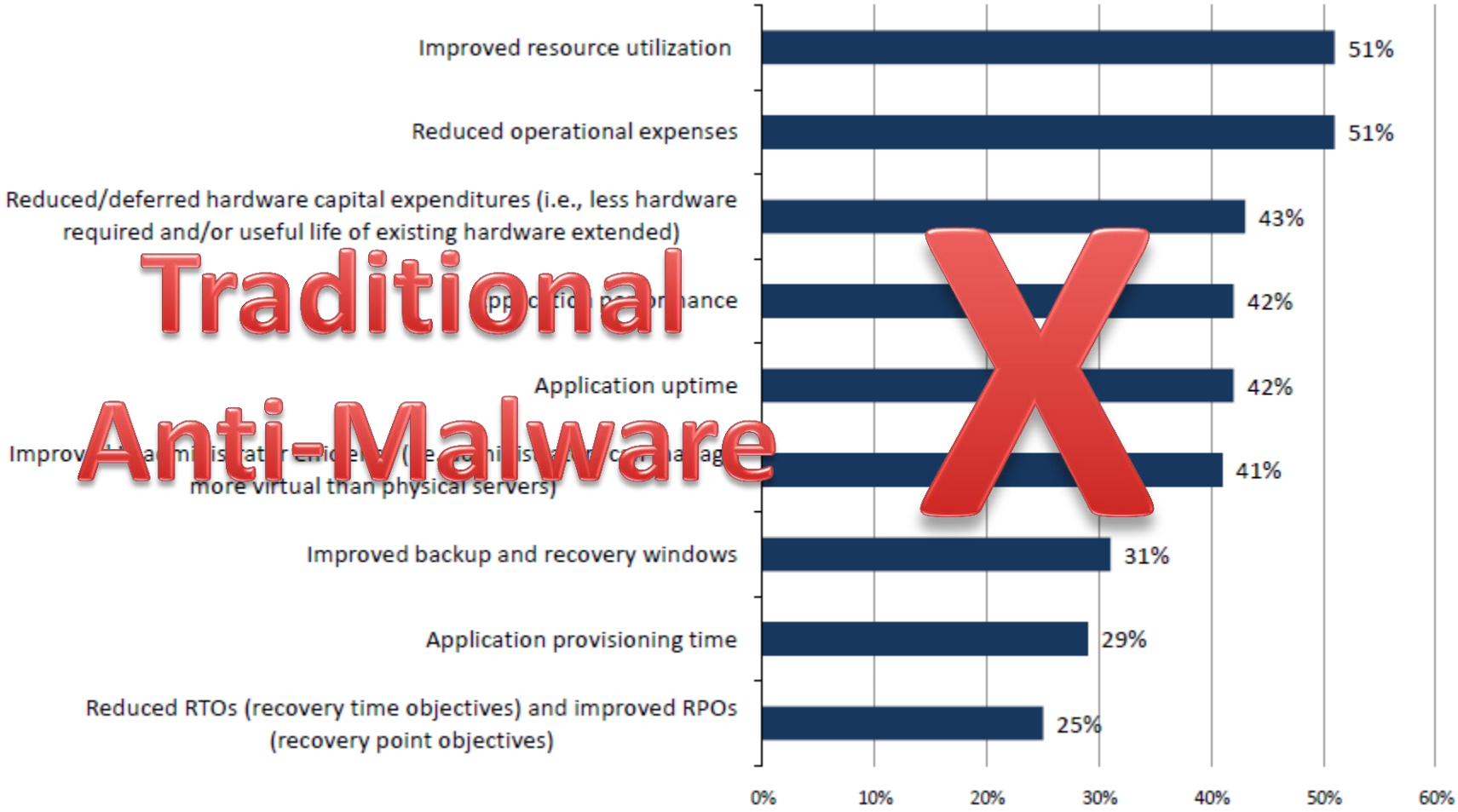
- 가상화 Windows, Unix servers, desktops을 보호
- agentless antimalware용으로 VMware vShield 5 Endpoint와 최초로 통합
- Citrix, Microsoft, 기타 다른 가상화 환경까지 보안을 확대

## Cloud Security for Endpoints

- laptop, desktop, server endpoints까지 보호하며 통제
- enterprise-class endpoint 보안 서비스 제공
- 모든 endpoints를 중앙에서 관리

# Security is counterproductive!

# Cloud computing and Virtualization Success Metrics




Ref: Enterprise Strategy Group 2010

# Virtualization Security Challenges

AV storms

Server sprawl

Vulnerable local agents

**Xen**
**vSphere**
**Hyper-V**

Boot latency

Outdated AV on VMs

# Issues with traditional antimalware approach

## VM 상에 위치한 전통적인 antimalware clients

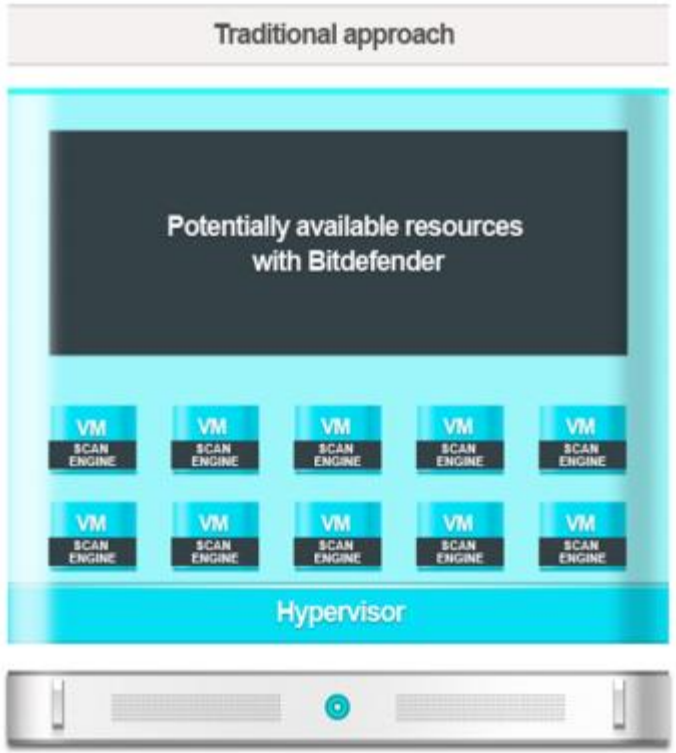
- 가상환경에서 VM 각각에 antimalware agent 또는 client가 설치됩니다
- Antimalware engines, signatures, cache databases가 위치한 곳마다 저장됩니다

➔ 그래서, 하드디스크, 메모리, CPU 자원이 추가로 필요함

평균적으로, 디스크 공간 400MB와 메모리 200MB가 필요합니다

➔ 자원 소모가 너무 많음

➔ 하드웨어가 VM을 많이 가동하기 때문에 자원 소모가 너무 많음



# Issues with traditional antimalware approach

부팅 대기시간과 부팅 시 보안 공백

- 보통의 백신제품은 scanning engines과 signatures database 로딩 시 5 ~ 12 초의 부팅 대기 시간이 필요합니다
- 또한, 부팅 시 업데이트 내용을 확인하면서 추가로 로드가 발생합니다

➔ 이 시간 동안 악성코드가 공격하는데 무방비 상태로 남아 있게 됨

# Issues with traditional antimalware approach

자원 배분 문제

- 모든 VM에 설치돼 있는 antimalware client들이 모두다 호스트 자원을 사용하기 때문에 호스트가 생산적 업무에 사용되는 것에 지장을 초래합니다
- 모든 VM에 설치된 AV client가 동시에 스캔을 할 때마다 호스트의 이러한 성능 저하가 발생합니다

➔ AV client가 동시에 몰아치며

➔ VM 내부에서 전체적인 성능 저하 발생

# Issues with traditional antimalware approach

VM들이 업데이트를 동시에 다운로드함

- 전통적인 antimalware 솔루션들은 antimalware signatures와 제품 업그레이드를 주기적으로 다운로드합니다
- 모든 VM에 설치된 Antimalware agent가 동시에 엡데이트를 다운받고 설치함
- 이렇게 동시에 진행하는 설치는 하드웨어 자원에 충격을 가합니다

➔ 네트워크와 자원 사용 두 측면에서 부하를 줌

➔ Significant performance hits

# Issues with traditional antimalware approach

관리의 복잡성

- 각각 설치되어 있는 antimalware client들을 중앙에서 관리하는 것이 관리를 단순화하지만 가상 환경에 대해서는 여전히 완벽한 해결책이 아닙니다:
  - 여러 antimalware client들이 동시에 가동하는 것은 자원 활용에 커다란 충격을 가함
  - 각각의 VM별로 별도의 정책을 적용하는 것도 하드웨어 자원에 지대한 충격을 줄 수 있음
- VM별로 설치된 antimalware client들을 원격에서 관리할 수 있는 솔루션이 없는 것은 관리를 더욱 복잡하게 만듭니다.

➔ 별도의 작업을 수행하는 동안 자원의 소모 증가

➔ 작업로드가 증가

# Issues with Traditional Antimalware Approach

VM 스냅샷 사용

- VM을 스냅샷으로 복귀시키게 되면 현재의 AV client virus signatures와 제품 업데이트도 스냅샷이 생성된 지점으로 복귀하게 됩니다

➔ VM은 요청받은 모든 업데이트와 업그레이드를 다운로드함

➔ 자원 소모 증가

# Issues with traditional antimalware approach

공격에 취약함

- VM별로 설치된 antimalware agent와 client들은 컴퓨터를 공격하는 해커가 무력화하려고 하는 1차 방어선을 형성하기 때문에 외부의 공격과 shutdown에 취약합니다

  ➔ 특정 악성코드의 첫 번째 목표가 됨

# Introducing Security for Virtualized Environments (SVE) by Bitdefender

Leading the way in virtualization security:

- ✓ Only **hypervisor agnostic** vendor: VMware, Citrix, Microsoft, AWS, Oracle, & RedHat 가상화 platforms 지원
- ✓ 가상화 Windows, Linux, Solaris systems에 적합한 최초의 통합 솔루션
- ✓ **Amazon Web Services (AWS)**와 통합하여 Windows , Linux AMI instances에 최적의 보안서비스를 제공

- ✓ scanning 기능의 중앙집중화로 인한 **Higher server consolidation**: 물리적 호스트별 VM 최대 30%까지 증가
- ✓ 자원 사용의 최소화로 인한 **Improved performance**

CITRIX ready

vmware PARTNER TECHNOLOGY ALLIANCE

amazon web services | solution provider

# SVE by Bitdefender – Overview

**Bitdefender의 Security for Virtualized Environments (SVE)**는 조직이 데이터센터들 간의 높은 수준의 통합율을 유지할 수 있도록 가상 환경에 특화된 보안을 제공합니다.

VMware 환경에 설치되면 SVE는 **vShield Endpoint**를 활용합니다. **하지만, SVE는 가상 기술에 의존하지 않으며**; 여느 가상 기술에 따른 가상 환경을 보호합니다.

SVE는 **linux 서버에서 동작하는 Security Virtual Appliance에서 실시**되며 **Bitdefender Security Console**에 의해 관리됩니다.

SVE는 많은 스캐닝 기능들을 각각의 물리적 호스트에 존재하는 전용 Security Virtual Appliance에서 복제 및 중앙집중화 합니다.

# Centralized Scanning Functions

- Bitdefender의 독특한 Architecture는 많은 스캐닝 기능들을 중앙집중화할 수 있도록 합니다.
- 이런 기능들을 **리눅스 기반의 virtual appliance**에서 중앙집중화를 함으로써, Bitdefender의 솔루션은 업데이트, 스캐닝, 관리와 관련된 antimalware load를 효과적으로 제거합니다.


- non VMware vShield 환경에서는 centralized Security Virtual Appliance (SVA)에 antimalware processing을 offload를 해주는 VMs Silent Agent 설치가 필요합니다.

# Centralized Scanning Functions

- 스캐닝 엔진이 SVA에 로딩되므로 부팅 대기시간이 없습니다.
  - ➢ 부팅 시간 동안의 보안 공백이 없음
  - ➢ OS boot 이후 즉시 VM을 사용할 수 있음
- virus signatures를 snapshot을 채취한 시간대로 되돌리지 않고 snapshot을 사용할 수 있음
  - ➢ Signatures는 SVA에만 업데이트됨
- antimalware processing이 SVA에서만 일어나기 때문에 이러한 방법만이 AV storms을 막을 수 있음
  - ➢ Significant performance improvement


- non VMware vShield 환경에서는 VMs에 Silent Agent 설치가 필요합니다.

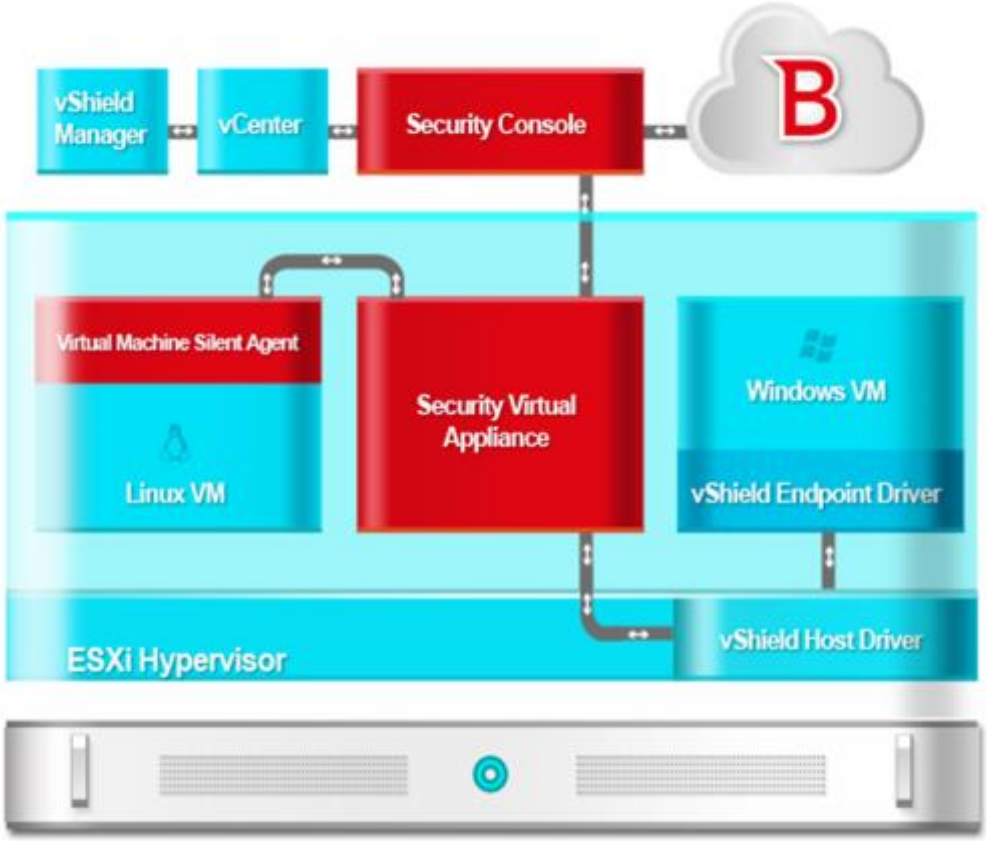
# Centralized Scanning Functions

- 중앙화된 caching mechanism (알려진 파일들의 database)으로 인해 각각의 VM별로 여러 차례 똑같은 파일을 스캐닝하는 문제를 피할 수 있음
  - ➢ 각각의VM별로 antimalware agent가 존재하는 전통적인 방법에 비해 기록적인 성능 향상

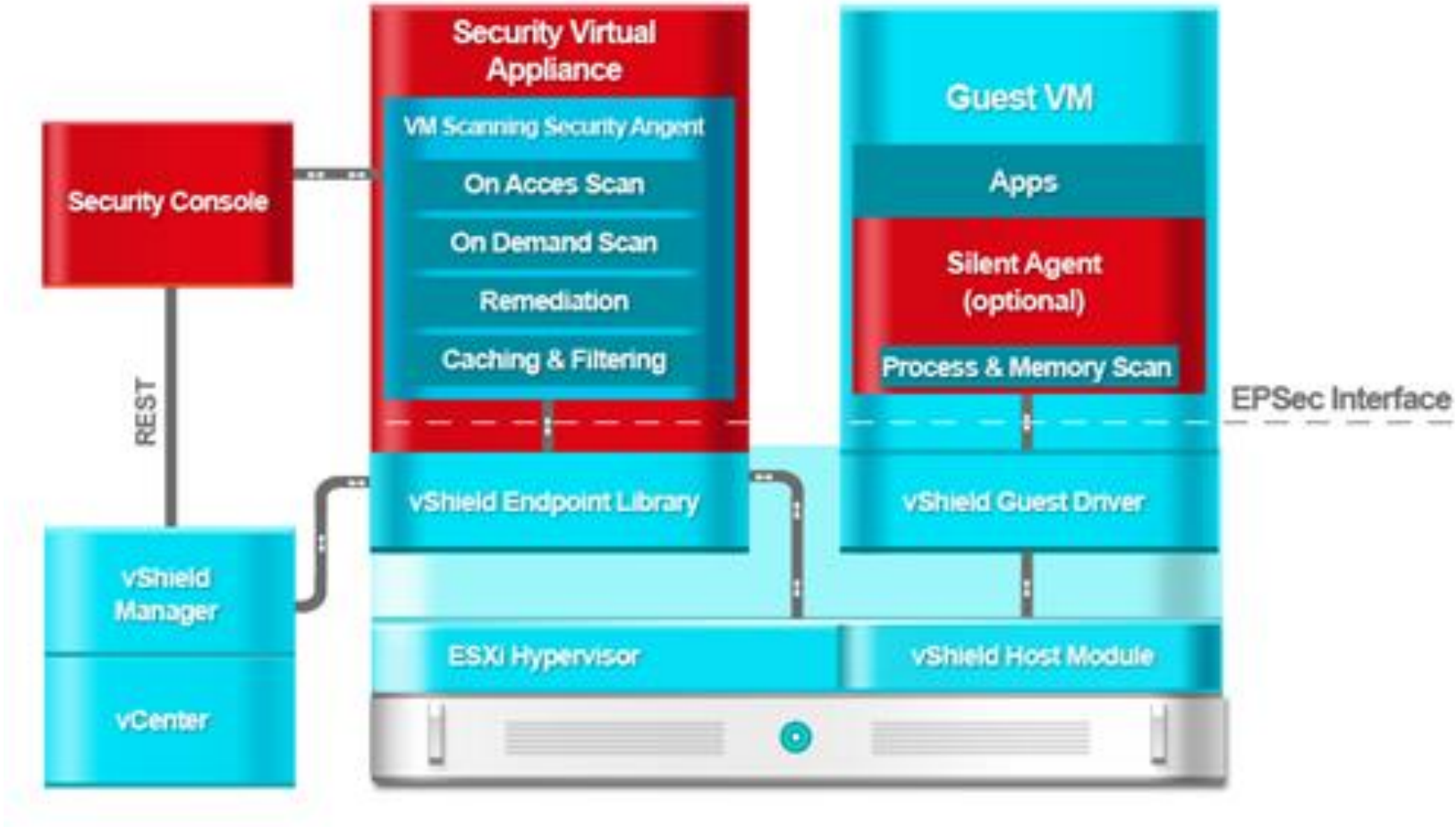

- guest machines에 security footprint를 남기는 것을 줄일 수 있음
  - ➢ VM환경에서의 VM별 디스크 공간: 15 MB / non-VM 환경에서의 VM별 디스크 공간: 60 MB
  - ➢ VM환경에서의 VM별 메모리 공간: 20 MB / non-VM 환경에서의 VM별 메모리 공간: 30 MB
- 기존의 일반적인 endpoint 솔루션들은
  - ➢ 디스크 공간이 400 MB 이상
  - ➢ 메모리가 200 MB 이상 필요함

# Architecture for agent-less protection in VMware Environments with vShield Endpoint

- **vShield Endpoint**는 Bitdefender가 제공하는 전용 secure virtual appliance로 antivirus, anti-malware agent processing의 부담을 넘깁니다.
- hypervisor 내에서 파일들의 활동을 감시하는 기능을 제공하여 Bitdefender SVA는 **EPSEC API**를 통해 vShield Endpoint와 통합이 가능하게 합니다. 핵심적인 anti-virus 기능들은 이 API를 통해 지원됩니다.

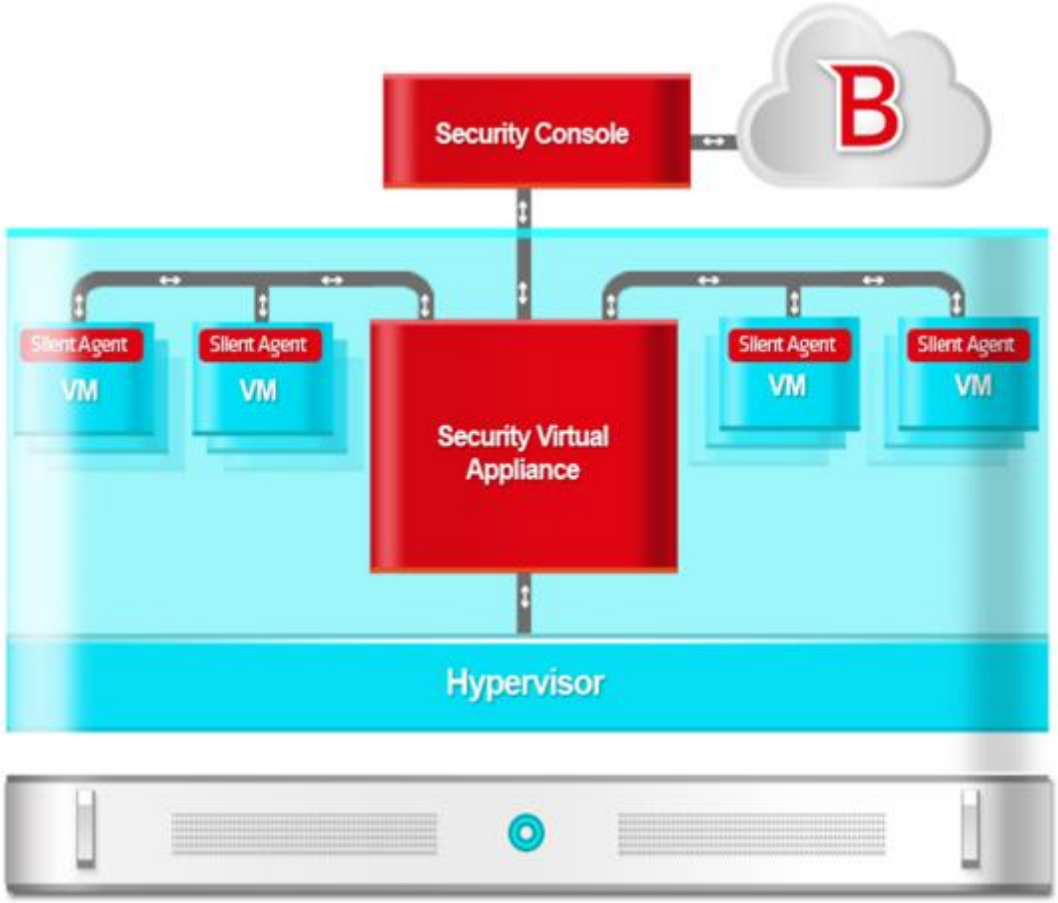


# SVE in VMware environments with vShield



# Architecture – Multi-Platform approach

- VM Silent Agent은 **TCP/IP** 를 통해 anti-malware processing을 Security Virtual Appliance로 offload 합니다.
- SVA와 local Silent Agent의 caches는 **네트워크 부하를 최소화 합니다**
- 여느 가상화 환경과 접목이 가능합니다.
- 특허출원 중인 기술:
  - Pre-trained
  - Self-learning



# Virtualization Environment / Hypervisor compatibility

- VMware vSphere 4.1 Patch 3, 5.0 Patch 1 (incl. ESXi 4.1, 5.0) for vShield Endpoint는 다음 내용이 꼭 필요합니다:
  - VMware vCenter Server 4.1 and 5.0, VMware vShield Manager 5.0, VMware vShield Endpoint installed from vShield Manager on the host/hosts
  - VMware Tools 8.6.0 being released with ESXi 5.0 Patch 1 in complete mode or vShield Endpoint driver, installed on all VMs to be protected
- VMware vSphere 4.0 and less for Scanning De-duplication Protocol integration

생산 환경에서 지원되는 다른 하이퍼바이저:

- Citrix Xen Desktop, Xen Server 5.x, 6.x with Xen Hypervisor
- Microsoft Hyper-V Server 2008 R2 or Windows 2008 R2 (Hyper-V)

다음의 다른 환경에서도 지원됩니다:

- Oracle VM 3.0
- Red Hat Enterprise Virtualization 2.2 and 3.0 with KVM

# Supported Guest Operating Systems

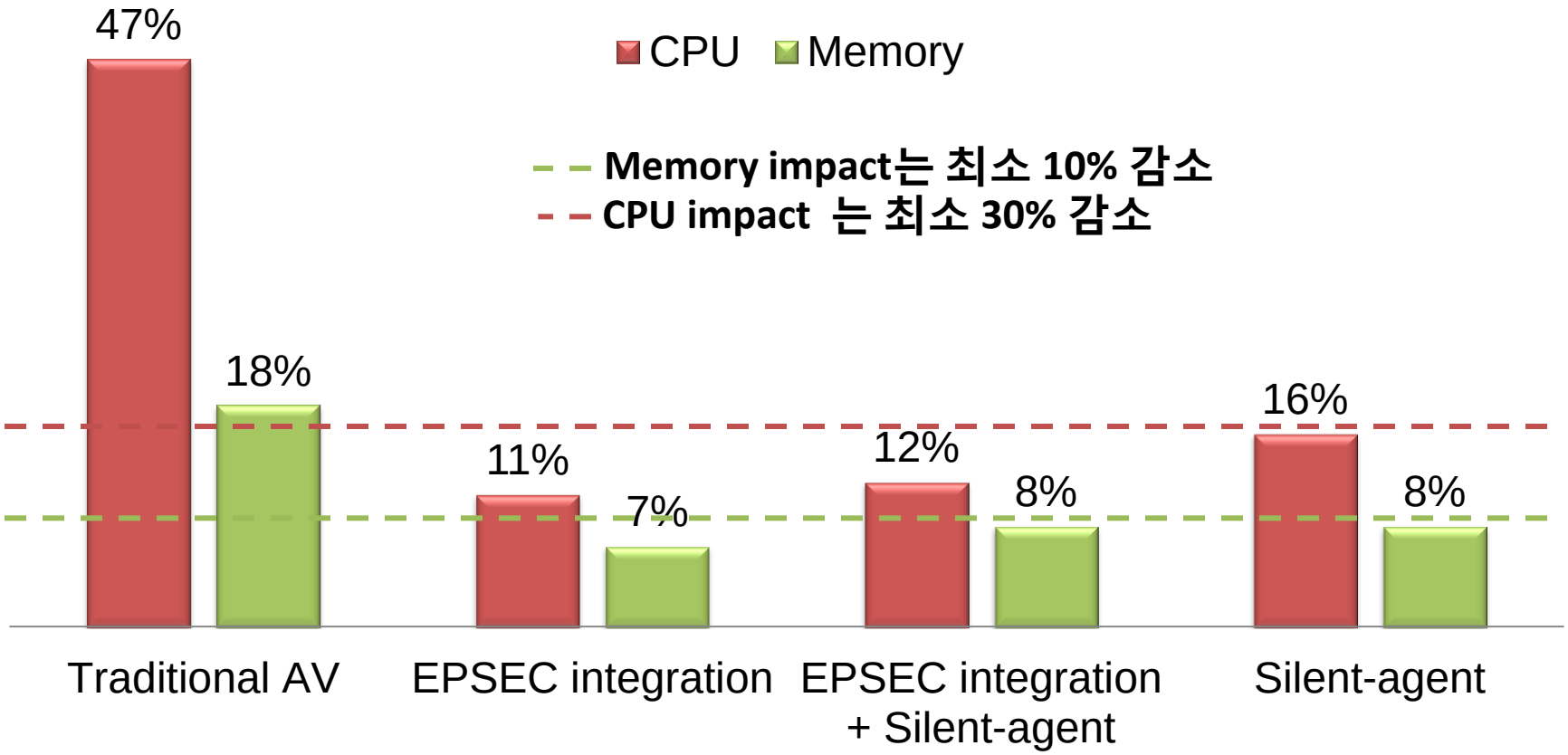
- 가상화 환경의 보안이 지원하는 OS:
  - Windows Vista (32bit), Windows 7 (32/64bit), Windows XP SP2 (32bit) or higher
  - Windows Server 2003 (32/64bit), Windows Server 2003 R2 (32/64bit), Windows Server 2008 (32/64bit), Windows Server 2008 R2 (64bit)
  - Red Had Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6
  - Ubuntu 11.04, 10.04
  - SUSE (SLES) 11
  - OpenSUSE 12, 11
  - Fedora 16, 15
  - Oracle Solaris 11, 10 x86

# SVA / SCA (Database) Requirements

- **Bitdefender Security Virtual Appliance** 설치 권장 사양:
  - Processors: 2 Processor(s)
  - Memory: 2 GB RAM
  - HDD: 8 GB
- **Bitdefender Security Console Appliance** 설치 권장 사양:
  - Processors: 2 Processor(s)
  - Memory: 2 GB RAM
  - HDD: 15 GB thick provisioned disk
- **Security Console**에 접근 가능한 web browser:
  - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome 8+

# Traditional antimalware vs. SVE

- Host running 72 virtual machines
- Local cache and server cache used

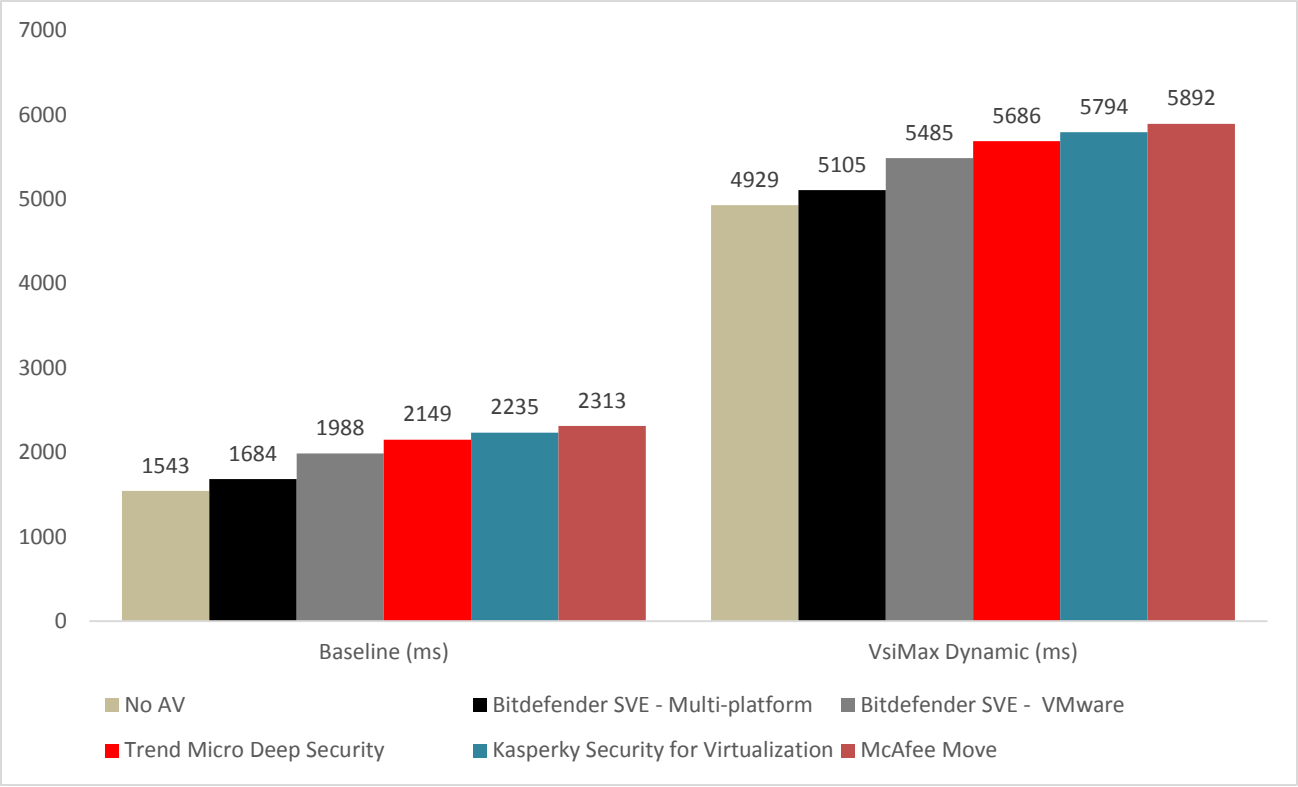


# Best performance in front of top virtualization security vendors

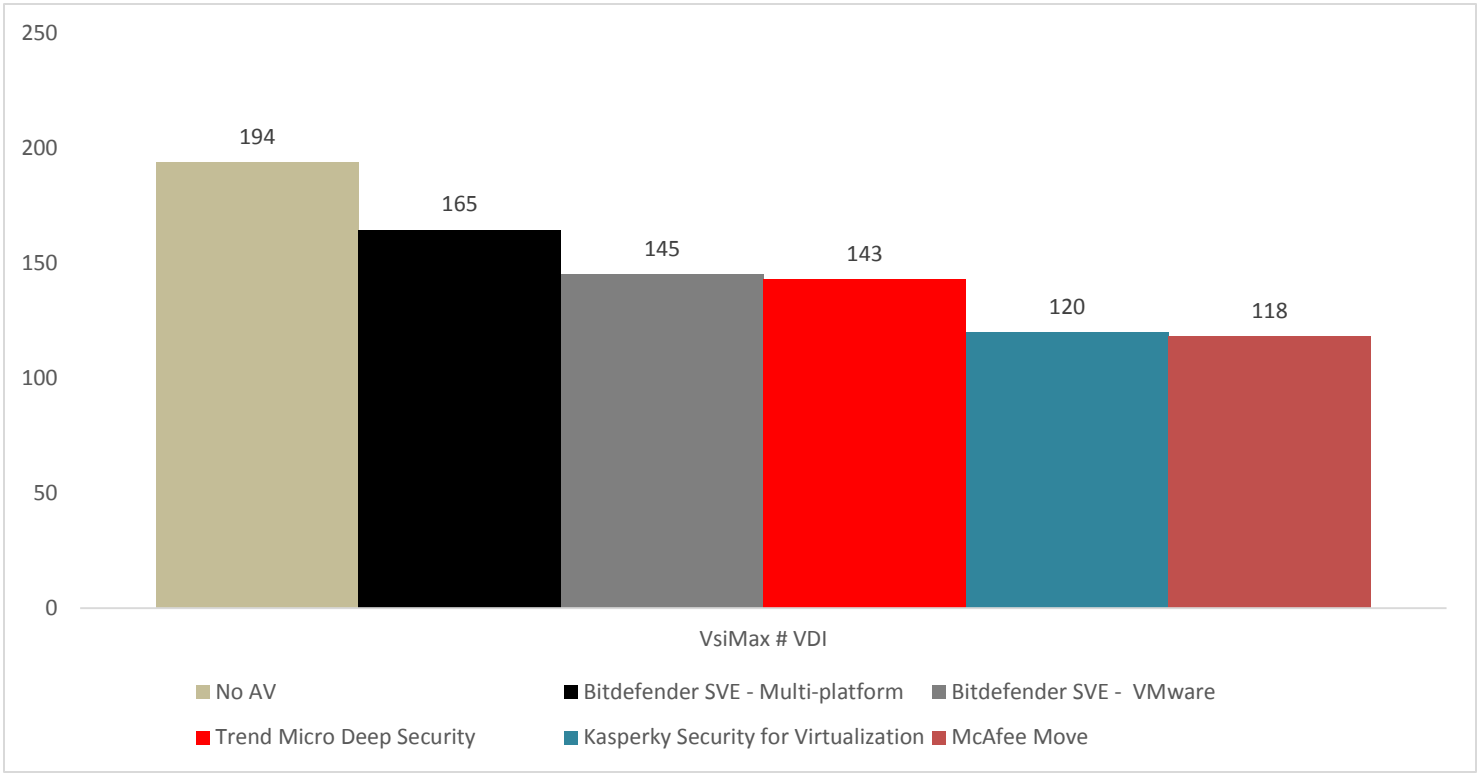

- Bitdefender는 현재 시장에 나와 있는 4 개의 가상화 보안 솔루션들이 VDI 환경에 어떤 영향을 미치는지 테스트 하기 위해 Login Virtual Session Indexer (Login VSI)를 사용했습니다.

Login VSI는 VDI 환경에서의 전형적인 user behaviour를 simulate하는 산업 표준 VDI benchmarking tool이며 script loop의 데스크탑 workload 내에서 동작하는 특정 사용자의 operations 반응 시간을 측정합니다.

# VSI Login results for SVE – Multi-platform



# VSI Login results for SVE – VMware with vShield Endpoint



# SVE on Amazon Web Services

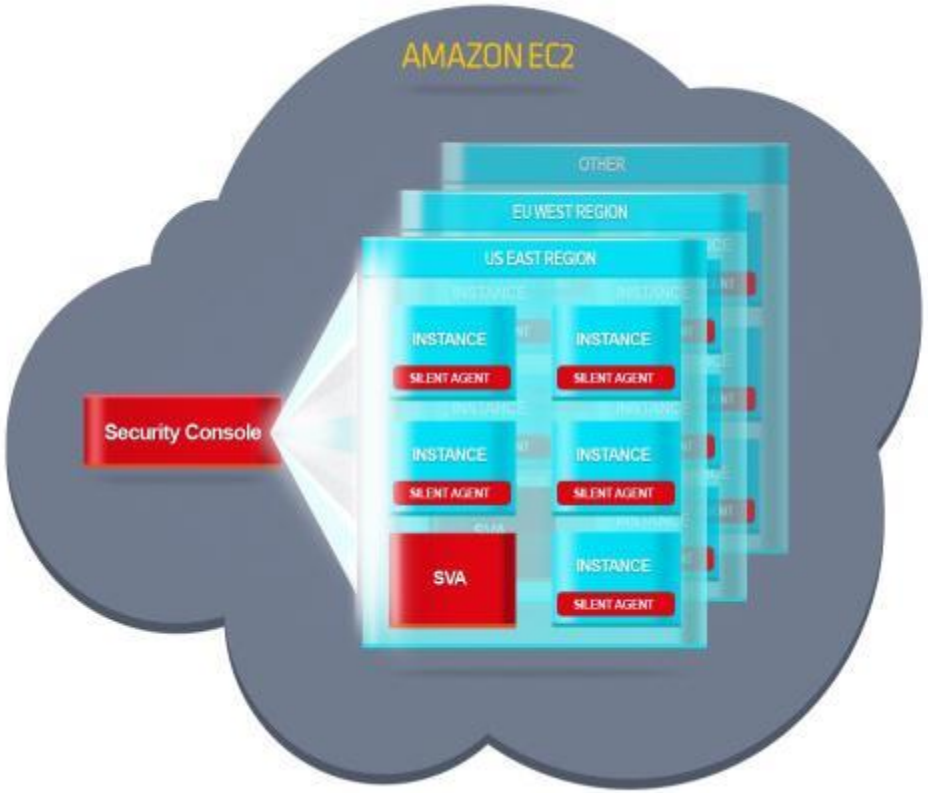
On September 5, 2012, Bitdefender released the SVE Security-as-a-Service on Amazon Web Services


- Provides hosted, largely-scalable antimalware, specifically tailored for virtualized and cloud-based environments
- Meets the requirements of on-demand provisioning and auto-scalability with high-optimization security technologies
- Integrates with Amazon EC2 to enable centralized management and monitoring of the protected AMI instances from the Security Console
- Complements (and does not replace) the existing AMI-based solution offered by Bitdefender on the Amazon Marketplace

**Available on Amazon Marketplace at: aws.amazon.com/marketplace**

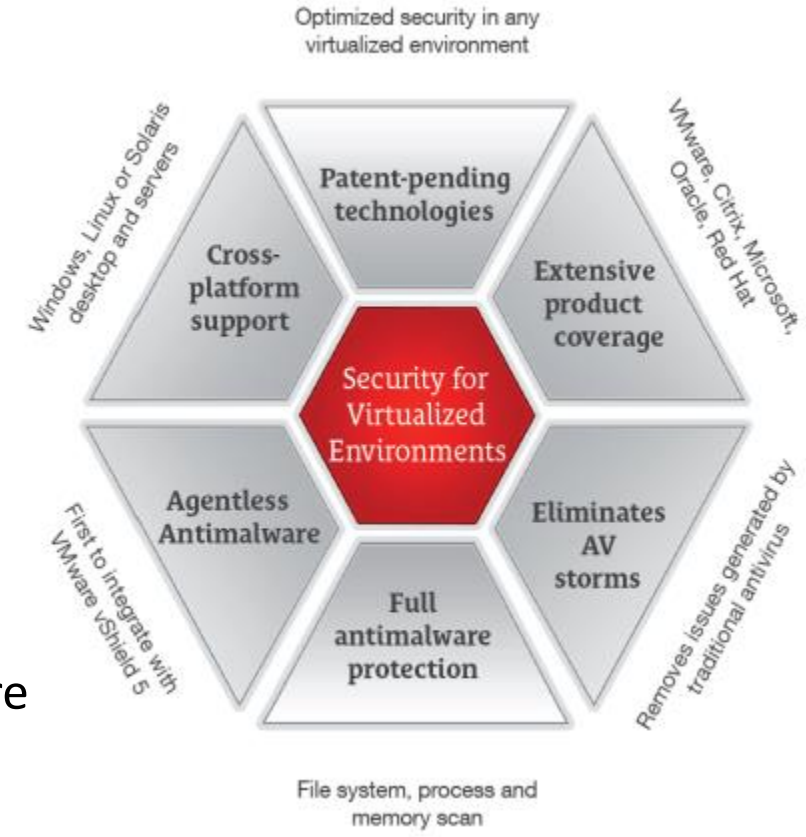
# SVE on Amazon Web Services – how it works

- Automatic deployment of lightweight SVE Silent Agents through AWS tagging
- Web-based public Security Console accessible at: amazon.bitdefender.net
- Hosted scanning servers (SVA), currently deployed on US-EAST1 and US-WEST1 zones
- Pay-as-you go pricing model: hourly, usage-based billing through integration with Amazon Flexible Payment System (FPS)



# Security for Virtualized Environments by Bitdefender

- **Intuitive deployment and management**
  - Integration with VMware and Citrix management provides easy deployment and management.
- **Hypervisor agnostic**
  - Supports VMware, Citrix, Hyper-V, Red Hat, Oracle, Amazon EC2, etc.
- **Comprehensive platform support**
  - Supports Windows, Linux, & Solaris servers & desktops.
- **Clear ROI**
  - Cost savings on datacenter hardware and cooling due to increased efficiencies.



# Cloud Security for Endpoints by Bitdefender

# Cloud Security for Endpoints

## 관리 부담 없이 엔터프라이즈급 보안 서비스를 제공합니다

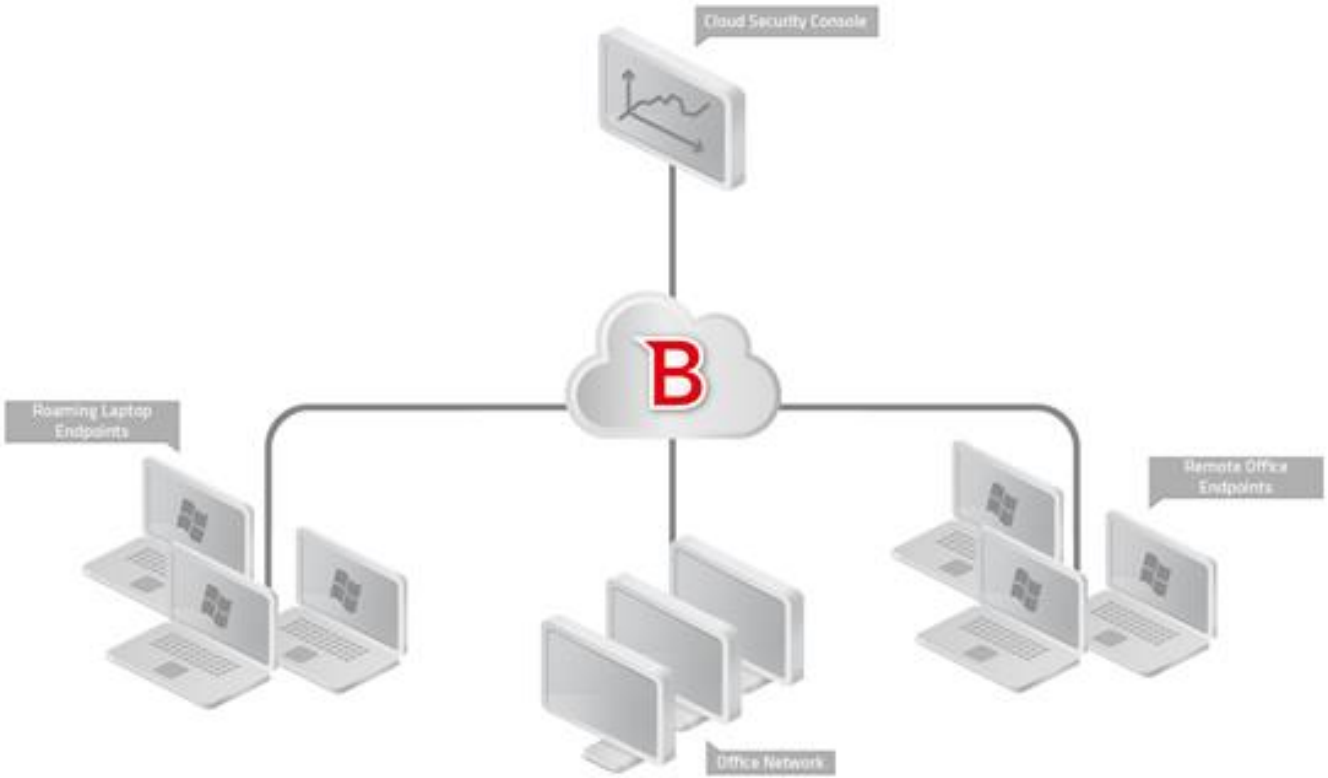
- 보안문제를 귀찮지 않게 하며 IT 전용 자원이 부족한 중소기업을 대상으로 효과적인 중앙집중식 보안 관리를 가능하게 합니다.

- on-premise solutions 처럼 엔터프라이즈급 보안 서비스를 제공하지만 서버 유지보수 비용과 오버헤드가 들지 않게 합니다

# Cloud Security for Endpoints

**Cloud Security for Endpoints** protects systems using security technology that has been rated first time and time again.

시스템을 보호하며, 언제 어디서나 endpoints 숫자에 구애 받지 않는 효과적이며 사용하기 쉬운 인터페이스인 Cloud Security Console을 통해 관리하기 때문에 현장에 하드웨어가 필요하지 않습니다.



# Main solution features

## Local scanning and Cloud-based console

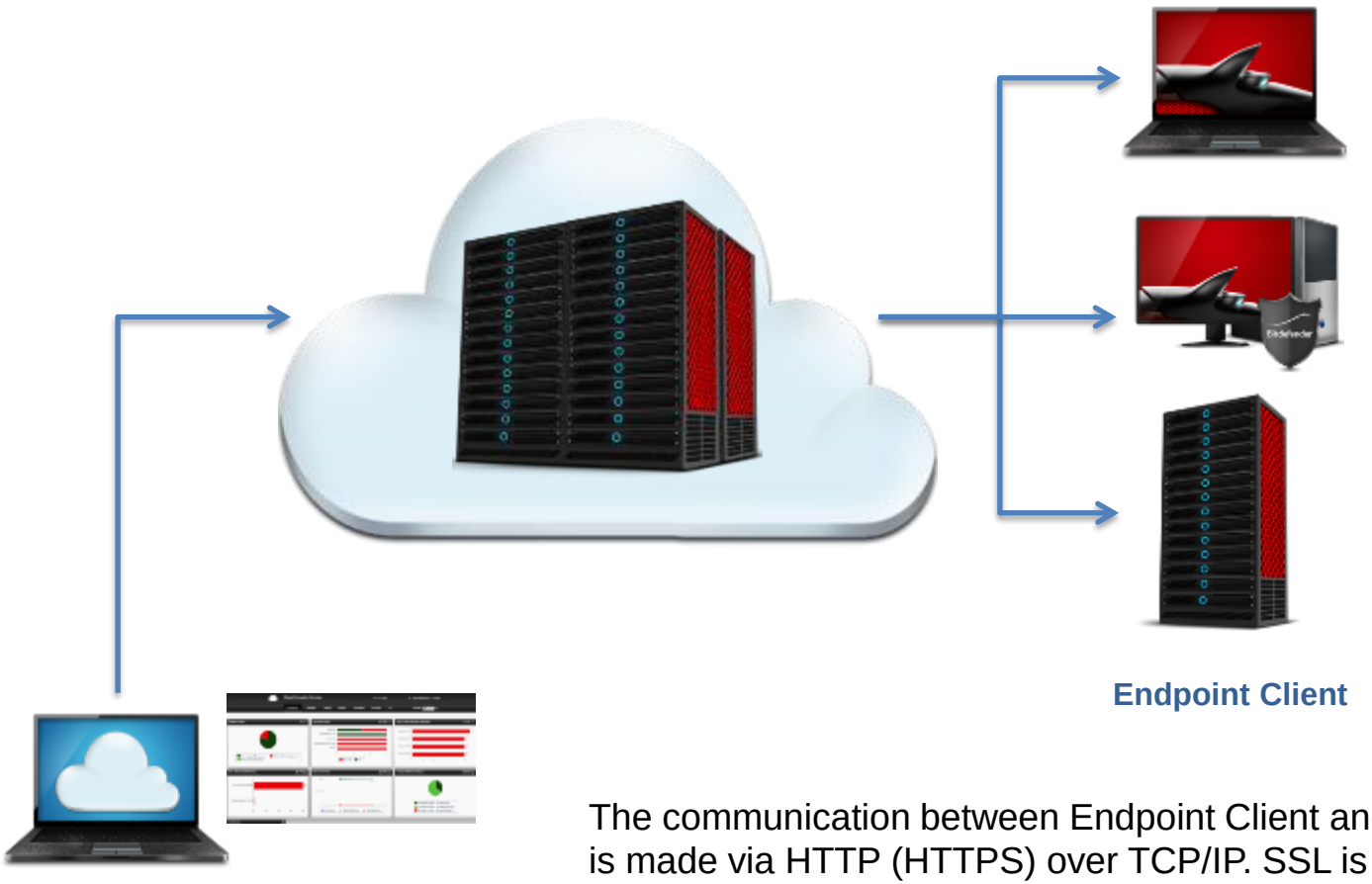
- local scanning과 중앙집중식 관리 console을 사용하여 강력하지만 비용효율이 높은 중소기업의 바이러스/악성코드 보호 수요에 대응하고 있습니다.
- 언제 어디에서나 윈도우 기반의 컴퓨터, 서버 endpoint를 관리합니다.
- 솔루션의 이러한 설계와 실행 모델은 Managed Security Providers (MSPs)와 ISPs에 딱 맞습니다.

# Key benefits

## Mitigates risks and improves security posture

- 자동 업데이트, 소프트웨어/하드웨어가 필요하지 않은 중앙집중식 보안 관리로 기업이 시간과 비용을 절감하게 해 줍니다.
- 직원들의 생산성을 높여주고 보안 관리를 위한 필요성을 없애줍니다.
- 언제 어디서나 실시간 관리의 최고 보안 기술을 통해 모든 시스템에 대한 보안상태를 높여줍니다.

# Cloud Security for Endpoints – Architecture



Endpoint Client

Cloud Security Console

The communication between Endpoint Client and Console/Server is made via HTTP (HTTPS) over TCP/IP. SSL is used.

# System requirements

## **Cloud Security Console** (the web based console)

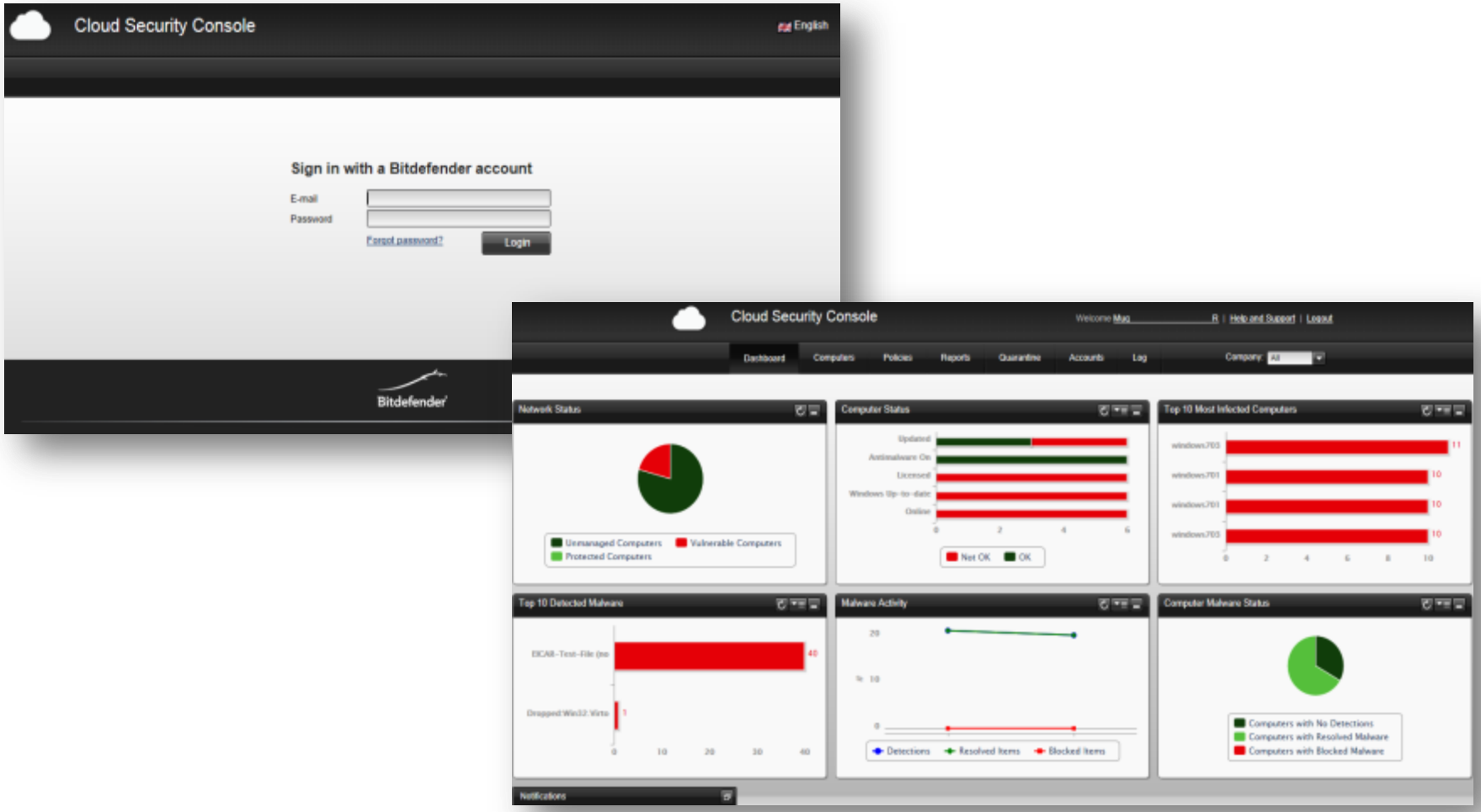
- Internet connection is needed
- Internet Explorer 8 or higher
- Firefox 4 or higher
- Google Chrome 8 or higher
- Safari 4 or higher

## **Endpoint Client** (the fully-automated computer security program)

- Intended for workstations, laptops, servers running on MS Windows
- **Workstation**: Windows 7, Vista (SP1), XP (SP3), Embedded Standard 7
- **Server:** Windows SBS 2011, 2008 R2 / SBS, 2003 SP1 / R2 / SBS, Home Server
- **CPU:** Intel® Pentium compatible (32/64-bit), 800 MHz (Windows XP), 1 GHz (Windows Vista, Windows 7), 1.5 GHz (Windows Servers)
- **Memory**: 256 MB (Windows XP), 1 GB (Windows 7, Vista, 2008, 2003), 1.5 GB (SBS 2003), 4 GB (SBS 2008), 8 GB (SBS 2011)
- **Hard Disk**: 1 GB
- **Internet connection:** Internet Explorer 7+, Mozilla Firefox 4+, Google Chrome, Safari or Opera for endpoint browser security.

# Cloud Security Console

A central web interface used for installing, configuring, monitoring, and reporting on the security status of datacenters and end-user systems.



# Cloud Security Console - Login mechanism

LINK for accessing Cloud Security Console:
https://cloud.bitdefender.net/

- For **PARTNERS**: Bitdefender 직원이나 다른 파트너가 계정을 만들어 줍니다.
- For **CUSTOMERS**: 파트너가 계정을 만들어 줍니다.
- 파트너와 고객의 credentials / login 정보는 이메일을 통해 전달합니다.

# Account (user) types

**Partner**

- Cloud Security for Endpoints service를 다른 회사(end users, distributors or resellers of the service)에 판매하는 회사

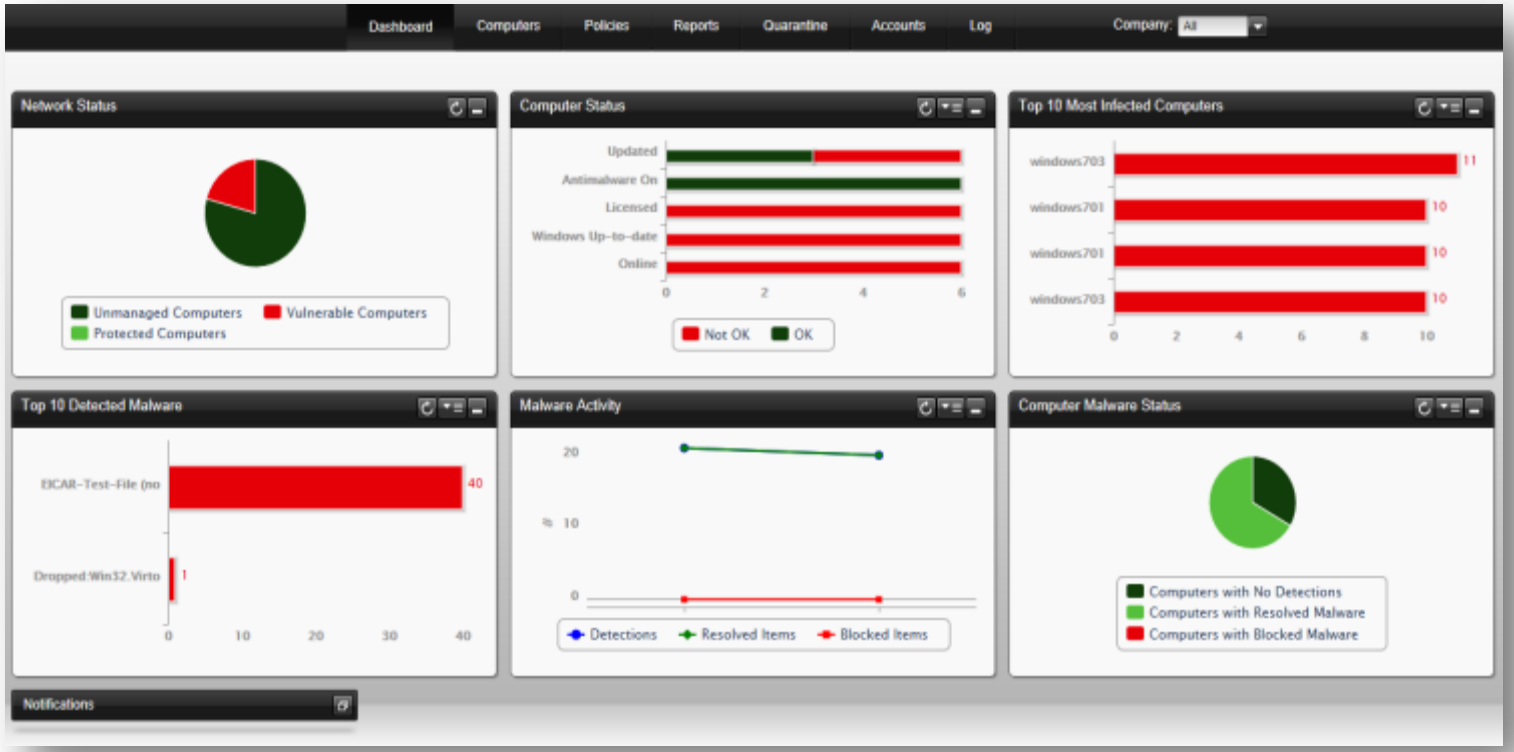
**Company (Customer)**

- 네트워크를 보호하기 위해 Cloud Security for Endpoints services를 사용하는 회사로서 계정은 보안서비스의 설치, 설정, 관리, 모니터를 위해서만 사용됩니다.
- 고객 계정 관리자는 내부 용도로만 사용하기 위해 다음 2 가지 계정만을 생성합니다:
  - **Administrator accounts**
  - **Reporter accounts**

# Dashboard overview

**Cloud-based dashboard**는 portlet 7 개로 구성된 단순한 상태표시 창으로서 여러 네트워크와 지리적으로 흩어져 있는 사이트들로부터의 여러 가지 보고서들을 포함하여 보안서비스를 받고 있는 워크스테이션이나 서버 endpoint의 보안 개요를 신속히 볼 수 있습니다.

The security dashboard는 개인적 선호도에 따라 설정할 수 있으며 세계적인 보안 문제에 대한 개괄적인 설명도 보여줍니다.

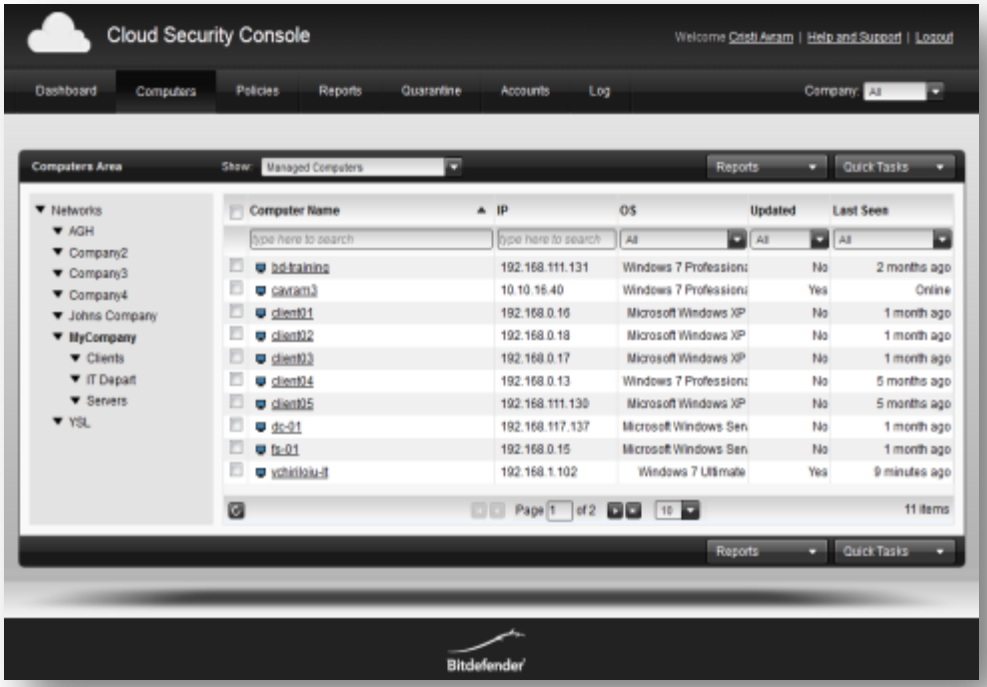


# Managing Computers

Computers Area는 관리 계정에 있는 컴퓨터 리스트를 보여줍니다. 만약 여러 회사(company)의 계정을 관리하고 있다면, 하나의 회사를 선택하여 거기에 관련된 컴퓨터를 볼 수 있습니다.

Here you will be able to:

- 컴퓨터를 그룹으로 묶기
- 컴퓨터와 보안서비스 내용 확인
- 보안 정책 확인 및 변경
- 빠른 실행
- 보고서 작성



# Client Security vs Cloud Security for Endpoints

| | Client Security v3.5 | Cloud Security for Endpoints |
|---|---|---|
| **Description** | On-premise solution. | - **not** an on-premise solution<br>- does not replace Client Security 3.5 or older version<br>- does not require on-site hardware |
| **Management and Update Server** | On premise | Cloud (same kit used for workstations and servers.<br>No on-site management server installation) |
| **Components** | Management Server, BDAgent, Update Server, Console, Business Client | Cloud Security Console and Endpoint Client |
| **Remote Management** | MMC Console | Via web console – Cloud Security Console (only Internet access needed) |
| **Active Directory Integration** | Yes | Not yet implemented |
| **WMI Scripts** | Yes | Not yet implemented |
| **Audit Reports** | Yes | No |
| **Client Antispam** | Yes | No |
| **Local Backup** | Yes | No |
| **Client mode** | Power user and restricted user | Configured and managed remotely by the network administrator or Service Provider |
| **Categories based web traffic control** | No | Yes |
| **Policy management** | 1 policy template / security module | 1 policy template for all security modules |

# New Bitdefender (on-premise) Enterprise Security

# Bitdefender®
# GravityZone™

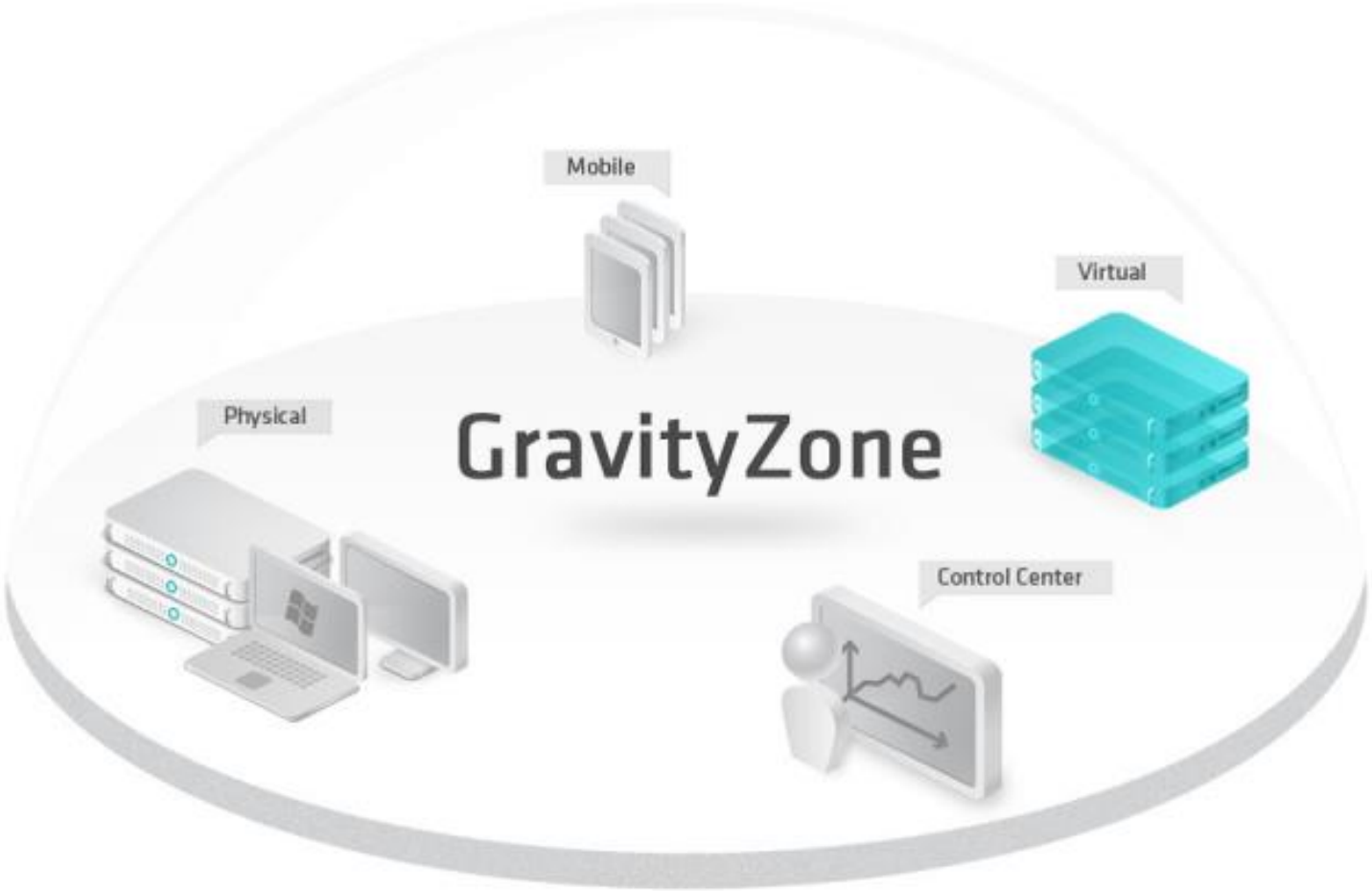
- ✓ Complete, Integrated, Best, Right
- ✓ Physical, Virtual, Mobile
- ✓ Single pane of glass into security
- ✓ Virtualization, Cloud, On-premise
- ✓ Unlimited, Extensible, Cloud architecture

# Bitdefender® GravityZone™

## Bitdefender®

Control Center
Security for Endpoints
Security for Mobile Devices
Security for Virtualized Environments

# Bitdefender GravityZone



# Bitdefender GravityZone

## Control Center

GravityZone 의 control center는 하나의 관리 창으로 물리적, 가상화된 모바일 보안을 관리합니다. Control center는 통합된, 유연한 web-base consol로 dashboard와 함께 통합 보안관리가 가능하며 보안 상태에 대한 drill-down 보고서와 경고 서비스 등을 제공합니다.

Control center는 아무리 복잡한 고객의 기업 환경에서도 고객의 수요에 대응할 수 있도록 높은 수준의 관리, on-demand 시 수천, 수만의 endpoints에게 높은 수준의 관리, 확장성을 제공합니다.

# Bitdefender GravityZone

**Security for Endpoints by Bitdefender**

two-way 방화벽, 침입 탐지, web access control과 filtering, 중요한 데이터 보호와 application control과 결합된 최고의 antimalware 기술을 사용하여 수많은 윈도우 컴퓨터, 서버를 보호합니다. 생산성이란 자원을 적게 사용하며, 사용자가 개입하지 않고도 최적화된 시스템 스캐닝, 자동화된 보안을 통해 보장됩니다.

Bitdefender 는 기존의 관리 시스템 그리고 모니터링 시스템과 결합하여 관리하지 않던 Microsoft Active Directory 에 나타나는 컴퓨터, 서버 또는 모바일 디바이스에 자동화된 보안 서비스를 제공합니다. 더욱이 Bitdefender의 proprietary endpoint discovery는 Microsoft Active Directory 리스트에 나타나지 않는 디바이스도 놓치지 않도록 합니다.

# Bitdefender GravityZone

**Security for Virtualized Environments by Bitdefender**

Windows, Linux, Solaris systems 기반의 가상화 서버, 데스크탑을 보호하는 가상화 데이터센터에 대한 최초의 종합 보안 솔루션입니다. 최첨단의 기술이 탑재된 Bitdefender의 SVE는 오늘날의 역동적인 가상화 데이터센터의 특이한 요구사항에 대응할 수 있도록 특별히 구성하였습니다.

Agent가 없는 보안서비스를 포함하는 VMware vShield Endpoint 5 integration에 더하여, SVE는 어떠한 가상화 platform에서도 antimalware process를 최적화하도록 설계되었습니다. 다른 여타의 가상화 보안 솔루션과 달리 SVE는 platform에 상관없이 VMware ESXi, Citrix Xen, Microsoft Hyper-V, Red Hat KVM, Oracle VM 등의 주요 하이퍼바이저를 지원합니다.

# Bitdefender GravityZone

**Security for Mobile Devices by Bitdefender**

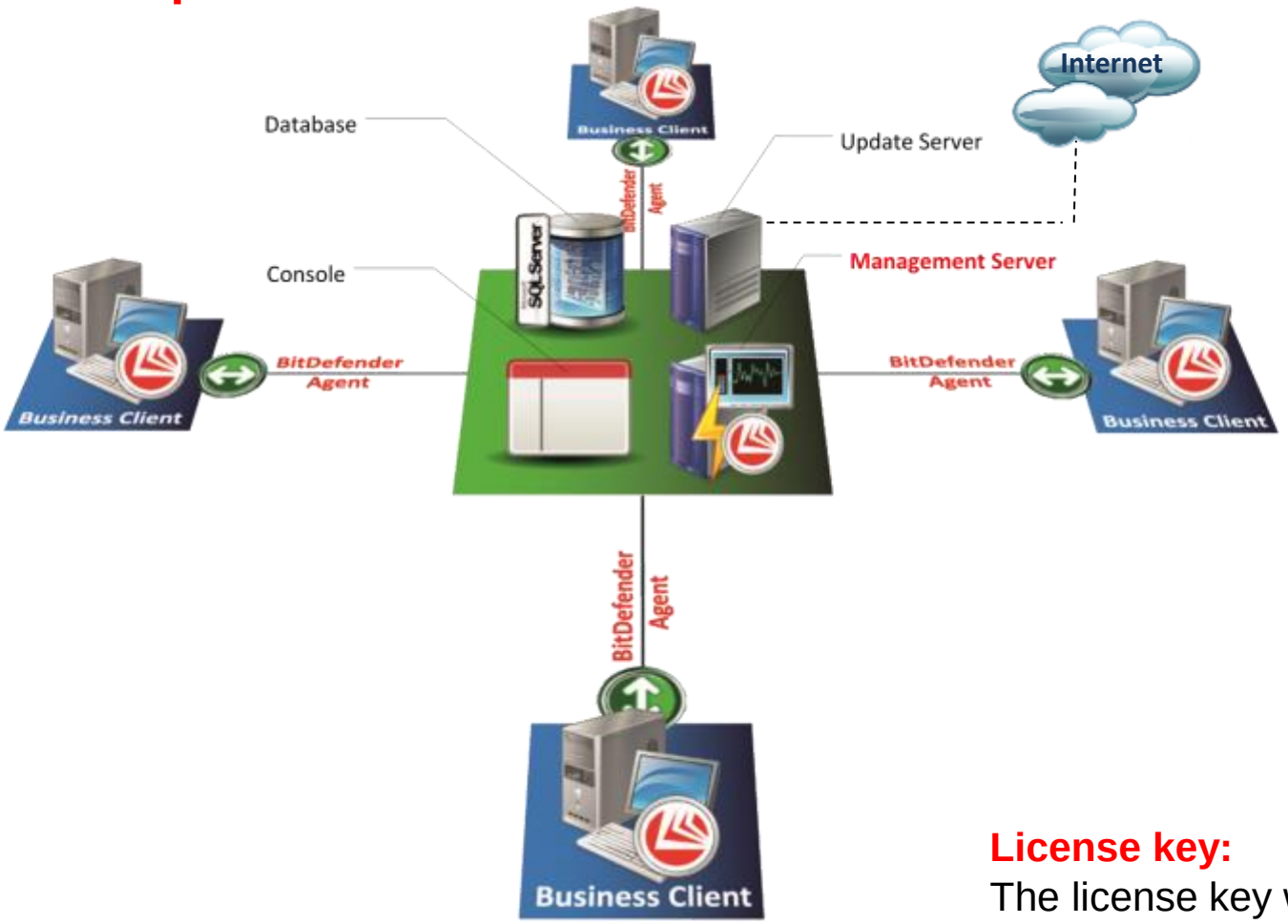
Apple이나 Android marketplaces에서 진행하는 소프트웨어 배포와 업데이트를 통해 iPhone, iPad and Android devices에 대해 전사적으로 보안과 관리, compliance control을 통합합니다.  또한, 모든 사용자의 디바이스에 보안 정책을 강제하여 BYOD 개념에 대해 통제된 채택을 지원하도록 설계되었습니다.

그 기능으로는 screen lock, authentication control, device location, remote wipe, 고정 또는 분실 디바이스 탐지, security profiles이 있습니다. On Android 디바이스에서는 실시간 스캐닝과 삭제 가능한 media encryption으로 보안 레벨이 행상되었습니다.  결과적으로, 모바일 기기들을 통제할 수 있으며 모바일 기기에 존재하는 민감한 정보들을 보호할 수 있습니다.

# Bitdefender Business Solutions Client Security v3.5

# Bitdefender Client Security

## Components:




Management of all client features:

- Antivirus
- Antispam
- Firewall
- Privacy Control
- User Control
- Update

**License key:**
The license key will be generated for the number of managed client computers

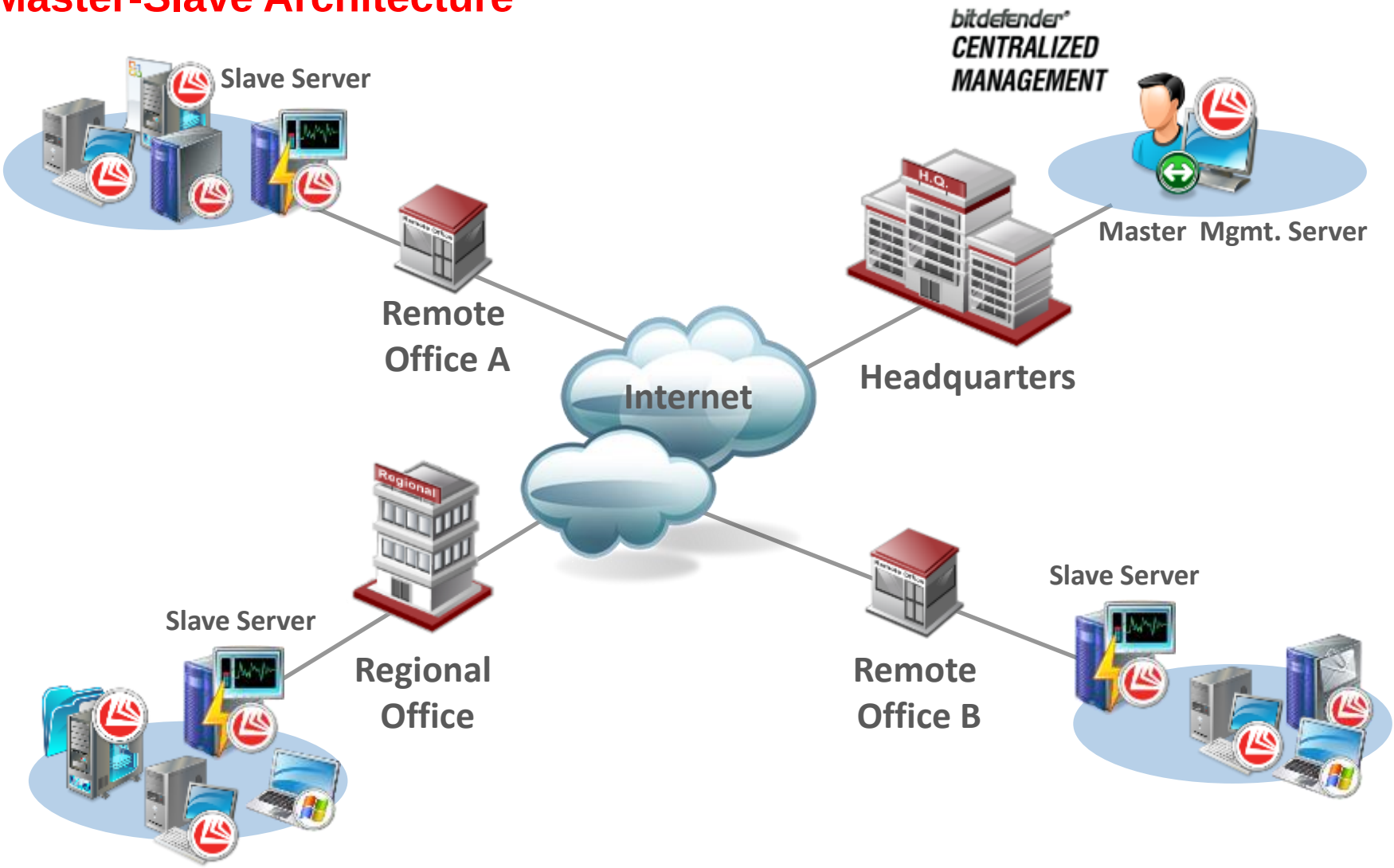
# Bitdefender Client Security

- **Centralized Administration, Protection and Control of workstations inside a network**
  - Business Client (x86 & x64) Add-on
  - Server Add-on
- **Policy based management system**
- **Master-Slave extensible architecture**
- **New station automatic detection and deployment**
- **Integration with Bitdefender products for Windows and Linux servers**
- **WMI Scripts**
- **Network Audit**
- **Real-time status of the server and clients presented on the console Dashboard**
- **Graphical Reports**

- **Considerably reduces administration costs for networks, ensuring centralized management of the antivirus protection in complex networks**
- **Use the integrated WMI scripts to access, configure and monitor Windows resources.**

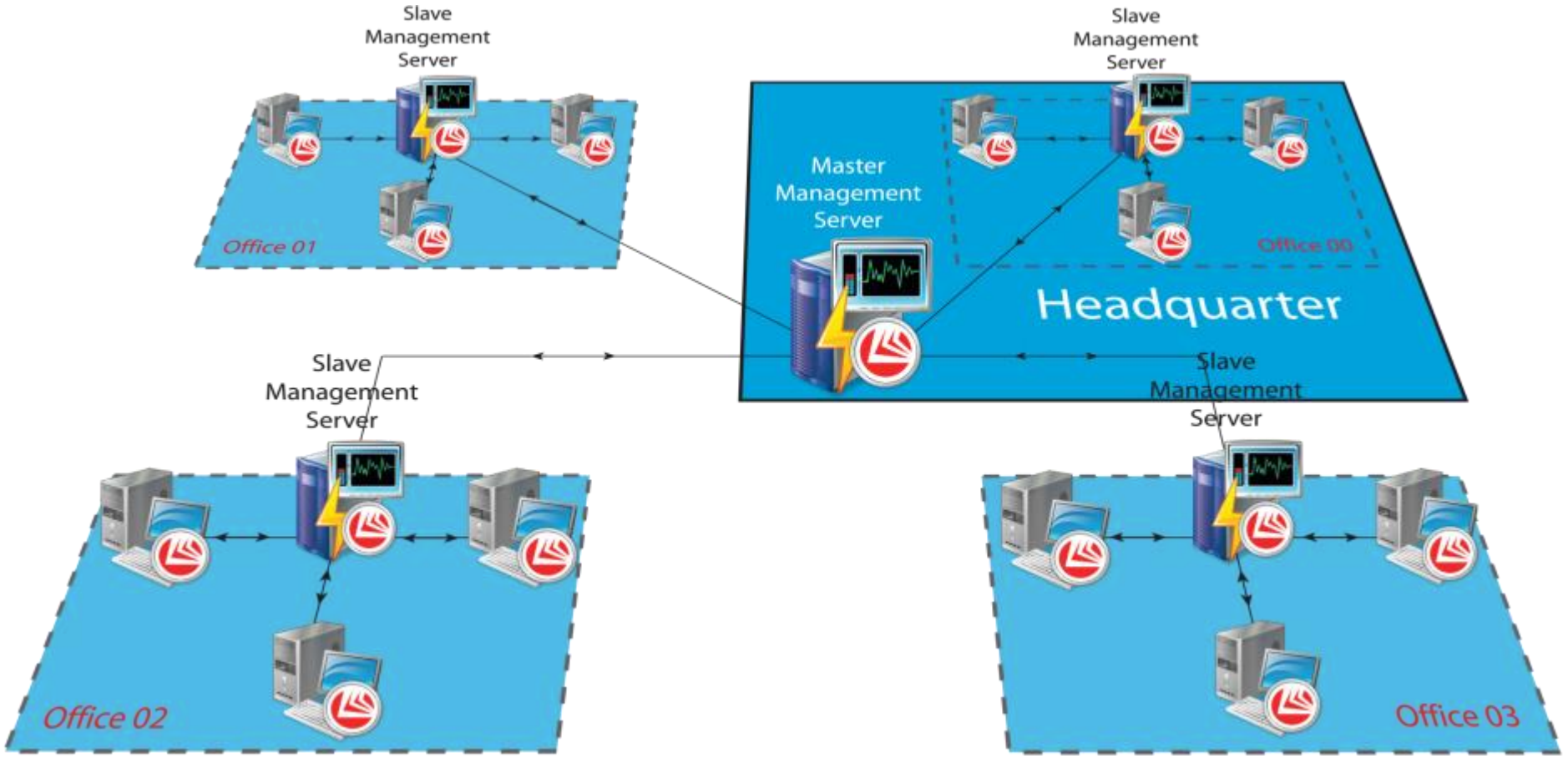
# Bitdefender Client Security

## Master-Slave Architecture



# Bitdefender Client Security

## Master-Slave Architecture



# Bitdefender Client Security

## Bitdefender Business Client

- **Real-time Antivirus and Antispyware protection**
- **On-demand Antivirus and Antispyware protection**
- **Firewall**
  - Automatic Network Detection and Configuration
  - Application Control
  - Stealth Mode
- **Antispam**

  Outlook / Windows Mail / Thunderbird integration (Bayesian-, Heuristic filter, Friend/Spammers lists)
- **Privacy Control**
- **User Control**
- **Backup (local)**
- **Power Mode / Restricted Mode**

  Restricted mode will allow the administrator to maintain the policies he has enforced

- **Complete protection for workstations, ensuring clean accessed files and received emails, antispyware protection, antispam filtering and user control.**

# Bitdefender Client Security

## System Requirements

### BD Management Server

- Intel Pentium compatible processor 1 GHZ (2 Ghz Multi Core recommended),
- 768 MB RAM (1,5GB recommended) for Windows XP and Windows 2003
- 1,5 GB (3 GB recommended) for Windows Vista, Windows 2008, Windows 7
- **Windows 2000 SP4 / XP SP2 / 2003 SP2 / Vista / 2008 Server / SBS 2008 / 2008R2 / Windows 7**

### BD Management Console

- Intel Pentium compatible processor 1 GHz (1,6 GHz recommended), 512 MB RAM (1 GB recommended)
- **Windows 2000 SP4 / XP SP2 / 2003 SP2 / Vista / 2008 Server / SBS 2008 / 2008R2 / Windows 7**
- **Internet Explorer 6.0(+), MMC 3.0(+)**

### BD Management Agent

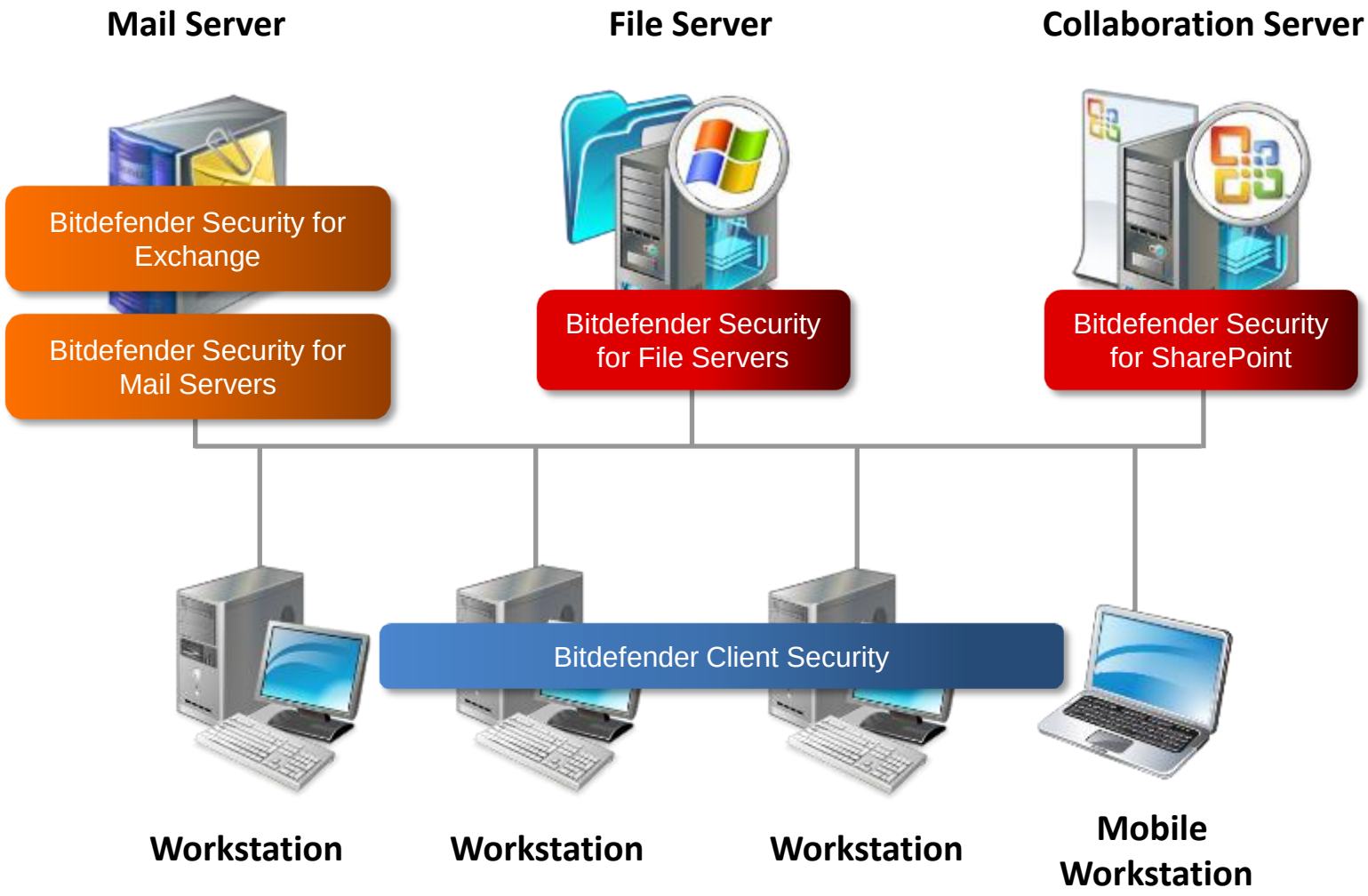
- Intel Pentium compatible processor 1 GHz (1,6 GHz recommended)
- 512 MB for Windows 2000, Windows XP, Windows 2003
- 1 GB (1,5 GB recommended) for Windows Vista, Windows 2008, Windows 7
- **Windows 2000 SP4 / XP SP2 / XP Home Edition SP2 / 2003 SP2 / Vista / 2008 / 2008R2 / SBS 2008 / Windows7**
- **Linux 2.4.x / 2.6.x** with glibc 2.3.1 and libstdc++5 from gcc 3.2.2 or newer

### BD Business Client

- Intel Pentium compatible processor
- 256 MB RAM (512 recommended) for Windows 2000
- 512 MB RAM (1GB recommended) for Windows XP
- 1 GB RAM (1,5 GB recommended) for Windows Vista / 7
- **Windows 2000 Professional SP4 / XP SP2 / XP Home Edition SP2 / Vista / Windows 7**

# Bitdefender Business Solutions Server Security v3.5

# Server Security Solutions - Windows



# Bitdefender Security for Mail Servers (SMTP)

## Antivirus

- Real-time scanning of attachments and message bodies.

## Antispam

- Ipmatch, RBL filter, White list, Black list, Charset filter, URL filter, Heuristic and LiveQuery filter.
- Directory Harvesting protection

## Content Filtering

- Filters and blocks messages by subject line, message body, sender or recipient.

## Attachment Filtering

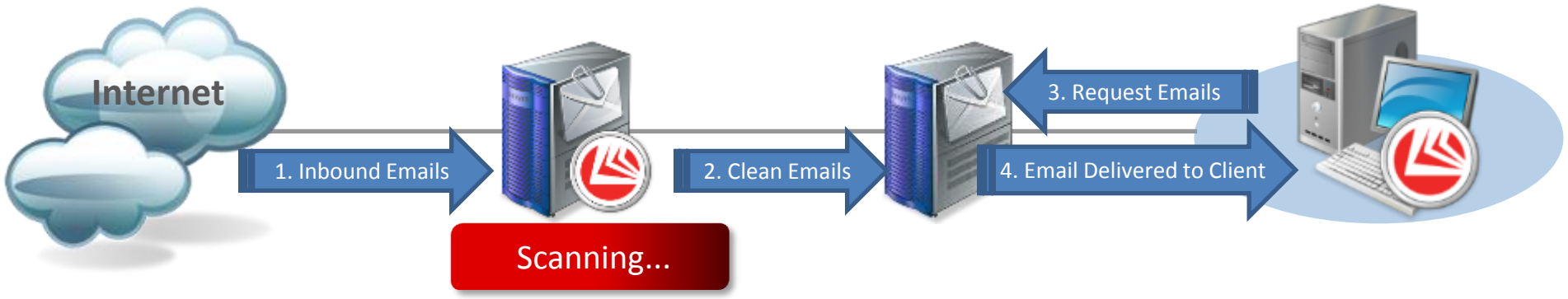
- Filters and blocks messages by attachment size, name or extension.

- **Designed for any mail server running on a Windows platform.**

**Note**

**Protects the mailboxes against malware but not the whole server**

# Bitdefender Security for Mail Servers (SMTP)




- **Scan / Filtering policies by user groups**
- **Detailed Reports and Statistics**
- **Centralized Management Support**

  Integration with the Management Server of Bitdefender Client Security
- **Protects more mail servers**

  Bitdefender Security for Mail Servers can act as a multiple mail server proxy through interfaces capable of filtering the traffic routed to different mail servers.

# Bitdefender Security for Exchange

## Antivirus

- Real-time scanning of attachments and message bodies
- On-demand scanning of the Exchange mailboxes
- Configurable VSAPI or SMTP scanning

## Antispam

- Incorporates different filters like: Ipmatch, RBL filter, White list, Black list, Charset filter, URL filter, Heuristic and LiveQuery filter.

## Content Filtering

- Filters and blocks messages by subject line, message body, sender or recipient.

## Attachment Filtering

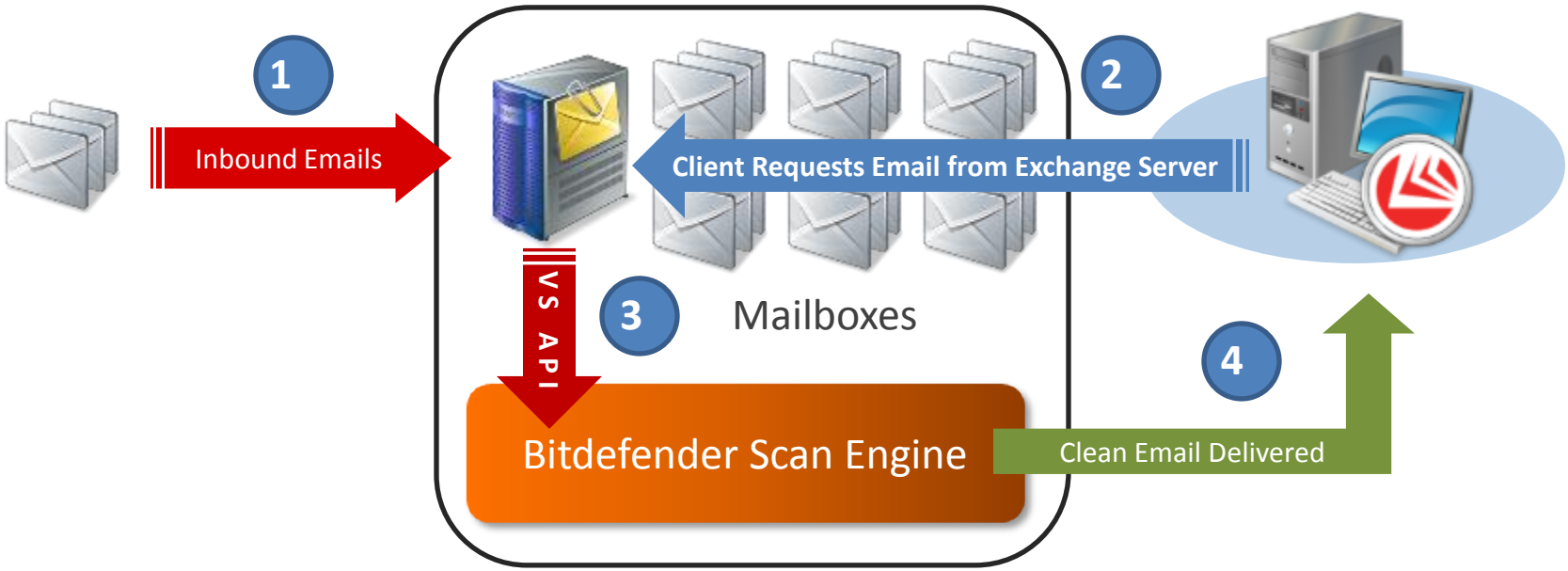
- Filters and blocks messages by attachment size, name or extension.

- **Due to the VS-API technology, it seamlessly integrates with the e-mail server, assuring advanced filtering of e-mail messages without affecting server performance or e-mail traffic.**

**Note**

**Protects the mail storage folders (mailboxes) against malware but not the whole server**

# Bitdefender Security for Exchange




- **Scan / Filtering policies by user groups**
- **Detailed Reports and Statistics**
- **Centralized Management Support**
  Integration with the Management Server of Bitdefender Client Security

# Mail Server Security Solutions

## BD Security for Mail Servers (SMTP):

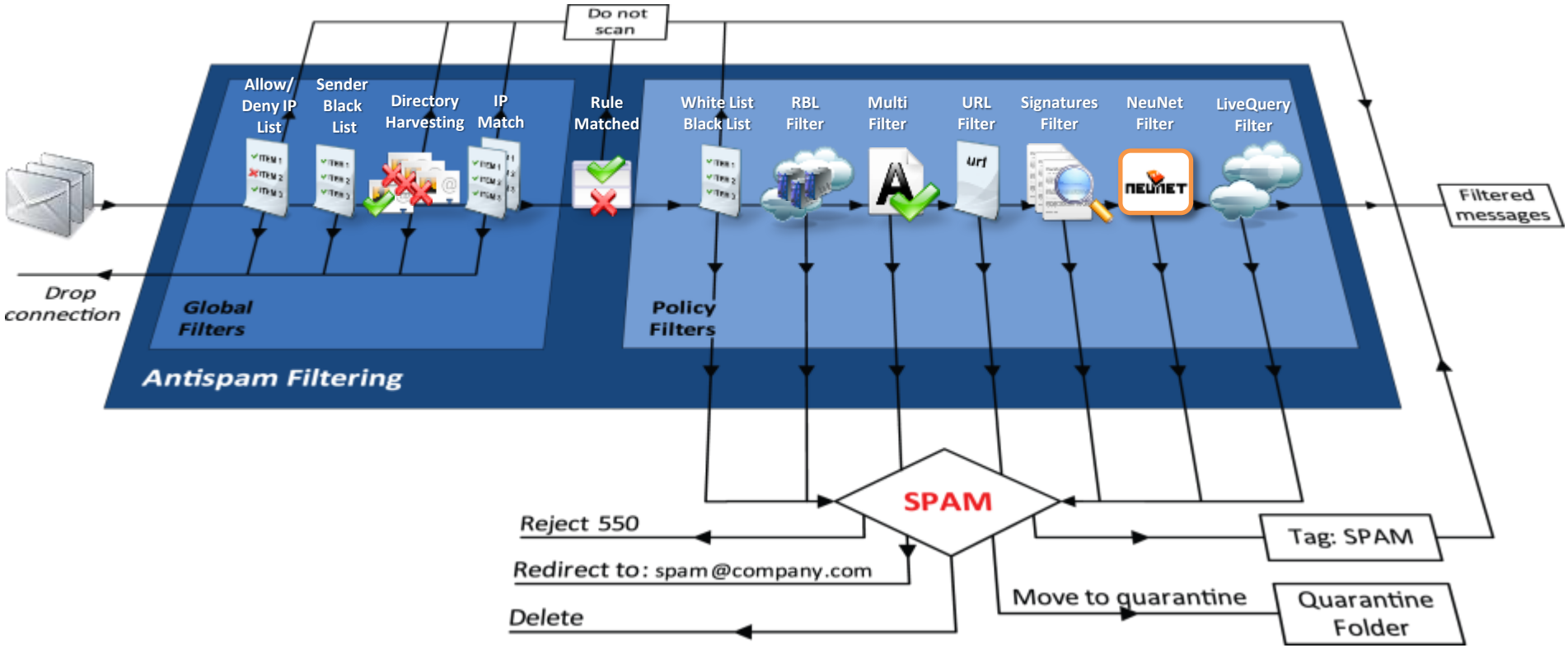
- Internet Explorer 6 or higher;
- Windows 2000 SP4 + Update Rollup 1 / Windows 2003 SP1 Server / Windows 2008

## BD Security for Exchange:

- Internet Explorer 6 or higher;
- MS Exchange 2010
- MS Exchange 2007
- MS Exchange 2003
- Windows 2000 SP4 + Update Rollup 1 for MS Exchange 2000 / Windows 2003 SP1 / Windows 2008

# Mail Server Security Solutions

## Antispam Features



# Bitdefender Security for File Servers

## Antivirus

- **Antivirus, Antispyware, Antirootkit Protection**
- **On-Access & On-demand Scanner**

  Scans each accessed or copied file in real-time with no impact upon file server performance.

  Scans also inside archives, packed files, boot sectors and registry.
- **Scheduled Scan and Update Tasks**
- **Multithread Scanning**

  Multiple instances of the engines are used to shorten the scanning process.
- **Optimized Scanning**

  Avoids scanning files known to be safe, therefore improving the scan speed and reducing the system load.

- **Solution implemented especially for file-sharing servers running on the Windows platform.**
- **Requirements:** Windows 2000+ SP4 / Windows 2003+SP1 Server (32 / 64 Bit) / Windows 2008 Server

### Centralized Management Support

Integration with the Management Server of Bitdefender Client Security

# Bitdefender Security for SharePoint

## Antivirus

- **On-demand Scanning**

  Includes an on-demand scanning module which provides the possibility to scan whole document libraries or lists.

- **On-access Antivirus Protection on uploads and downloads**

  Detects viruses in real-time when a user adds or retrieves a document to/from a document library or list.

- **Predefined or Personalized scanning profiles**

  Available for both on-access and on-demand scan

- **Scheduled Scan and Update Tasks**

- **Multithread Scanning**

  Multiple instances of the engines are used to shorten the scanning process.

- **Session based scan optimization**

  Reduces performance overhead by scanning files once unless accessed again

- **Seamlessly integrates with Microsoft's Virus Scanning API**

- **Compatible with SharePoint Portal Server 2003/2007 and with Microsoft Windows SharePoint Services v2.0/3.0**

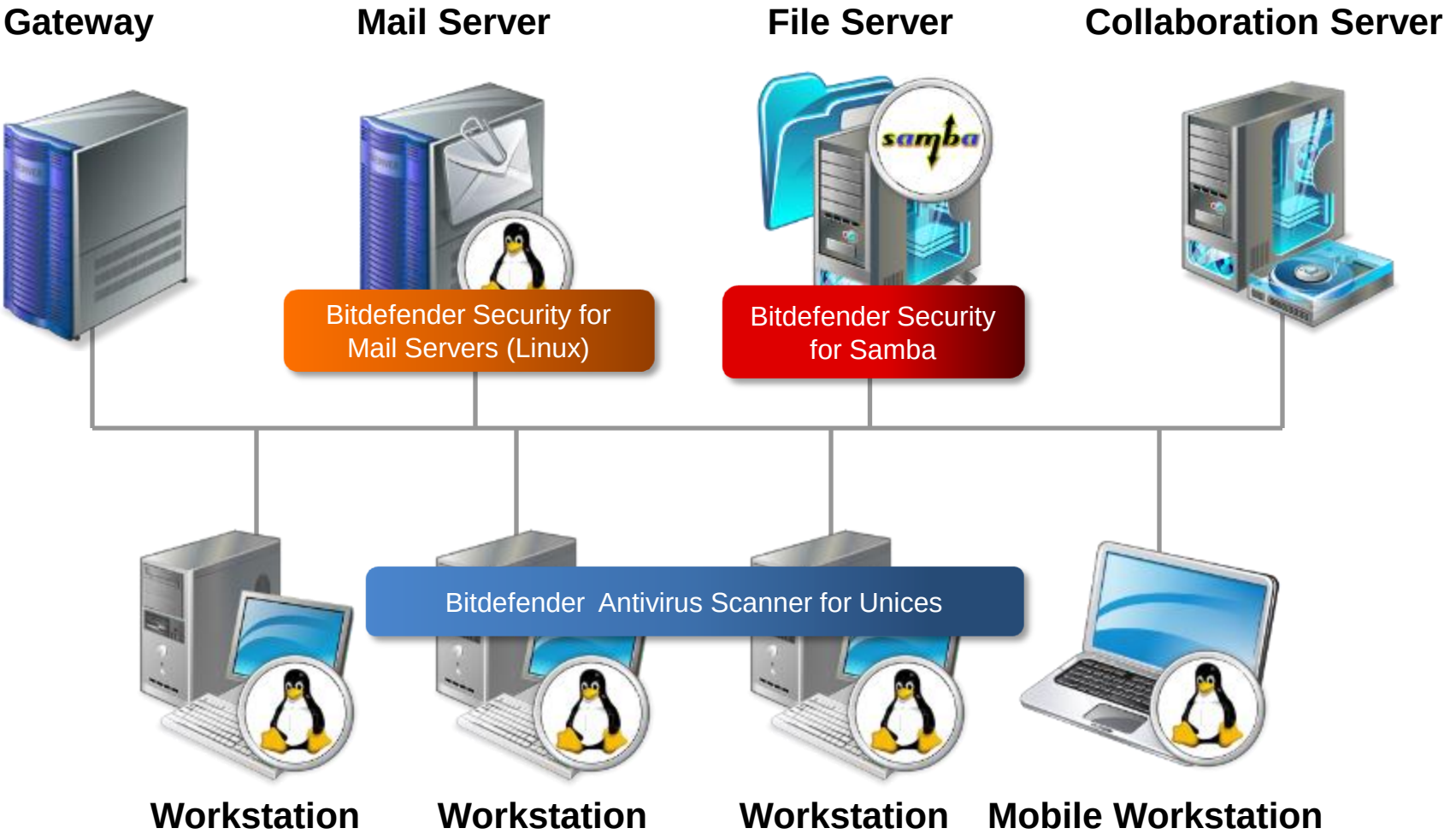
**Note**

**Protects the document libraries against malware but not the whole server**

### Centralized Management Support

Integration with the Management Server of Bitdefender Client Security

# Bitdefender Business Solutions – Linux



# Bitdefender Security for Mail Servers (Linux)

## Antivirus

- Real-time scanning of attachments and message bodies, without slowing down e-mail traffic.

## Antispam

- Ipmatch, RBL Filter, White list, Black list, Charset Filter, URL Filter, Heuristic & LiveQuery Filter.

## Content Filtering

- Filters and blocks messages by subject line, message body, sender or recipient.

## Attachment Filtering

- Filters and blocks messages by attachment size, name or extension.

- **Compatible with almost every Linux distribution that is not older than 3-4 years (including RHEL, Novell Linux, Mandriva, Slackware)**
- **Supports FreeBSD and OpenSolaris**
- **Dedicated software agents for SendMail, Communigate PRO, Qmail, Postfix, Courier**

- Web-based Interface (Radmin)
- BDSAFE-tool for command line configurations

# Bitdefender Security for Samba

## Antivirus

- **Antivirus, Antispyware, Antirootkit Protection**
- **Real-time & On-Demand Scanner**

  Scans each accessed or copied file in real-time with no impact upon file server performance. Scans also inside archives, packed files.
- **Share-Management**

  Create different scan policies for the shares protected by Bitdefender
- **BDSAFE**

  A small, yet powerful tool designed for post-install configuration and administration tasks. Fully scriptable, it is also easy to use for common tasks, and easier to integrate in a set of scripts and tools based on it.
- **Remote Administration Interface**

  Flexible and friendly interface based on webmin, accessible from anywhere.

- **Provides protection for network users by scanning all accessed files on Samba shares.**
- **Due to Samba's flexibility, the open source Bitdefender vfs module can be compiled against any Samba version, making the product the best choice for your favorite Linux distribution or FreeBSD branch.**

# Bitdefender Technical Support and Professional Services

# Technical Support and Professional Services

Trained in-depth on Bitdefender's Business Security solutions, as well as third-party technologies, our antivirus support experts are committed to being responsive to partners and customers needs and to providing them with the highest level of technical support.

More details about Bitdefender's technical support and professional services can be found in the following files:


Business_Support_Datasheet


SVE_Technical_Support_Packages

# Thank you!


enterprise.bitdefender.com