

Bitdefender®

# Bitdefender GravityZone

**Protection, Detection, Response and Risk  
Analytics Across All of Your Endpoints**

Alexandra SULU NACHT, Pre-Sales Engineer



# AGENDA

## LEARNING OBJECTIVES

- Introduction to Bitdefender
- What is GravityZone?
- GravityZone Platform Differences
- Local vs Hybrid vs Central Scanning
- Security Server Technology
- Machine Learning
- Endpoint Security Features
- Add-on Features
- NTSA
- MDM
- Product Portfolio



# A GLOBAL CYBERSECURITY-TECHNOLOGY COMPANY



**Bitdefender**  
Founded in 2001

Professional  
cybersecurity  
employees in R&D /  
engineering

Enterprise HQ in  
Bucharest, Romania  
with branch offices in  
US, Western Europe  
and Middle East

38% of global cyber  
security solutions use  
Bitdefender software  
in some form

Operates world's  
largest security-  
delivery infrastructure  
consisting of  
500,000,000 sensors  
in 150 countries

# WHAT IS GRAVITYZONE?

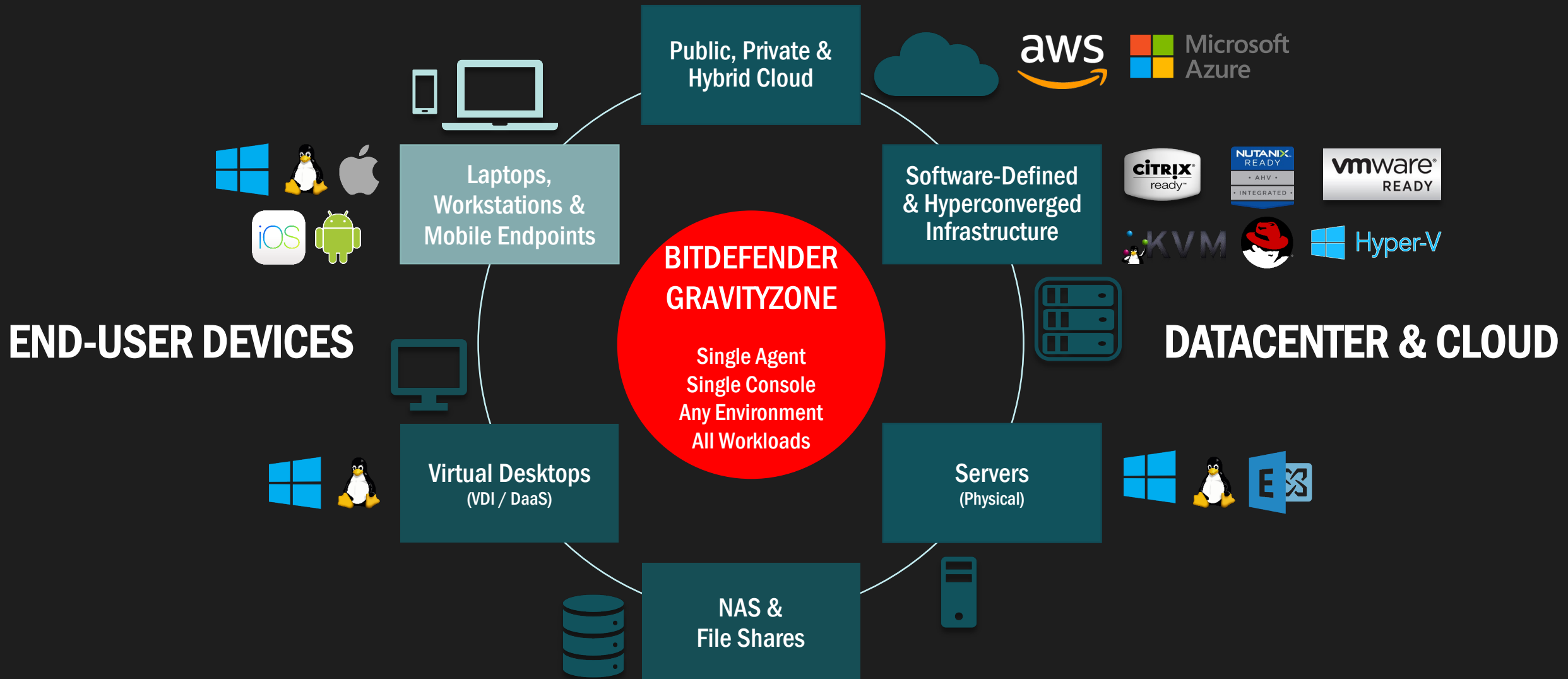
## OVERVIEW

Bitdefender GravityZone addresses the needs of the most demanding enterprises by providing cross-platform security for **physical desktops and servers, virtualized endpoints, mobile devices, Exchange mail servers** and using our newest product, **Bitdefender Hypervisor Introspection (HVI)**, is able to protect XenServer hosts against targeted attacks.





# AN INTEGRATED ENTERPRISE-SECURITY PLATFORM



# GRAVITYZONE PLATFORM DIFFERENCES



# FASTER TIME-TO-PROTECTION WITH FLEXIBLE CONSOLE-DELIVERY OPTIONS

## ON-PREMISES GRAVITY ZONE CONTROL CENTER



- Hardened Linux virtual appliance
- Spins up in <15 minutes
- Web-scale high-availability architecture
- Automatic system upgrades
- No OS or database licenses needed

## BITDEFENDER-HOSTED CLOUD CONTROL CENTER



- Zero deployment time
- No server resources needed
- No administration
- No additional costs

# GRAVITYZONE CLOUD





# COMPANIES

## TYPES

### **Partner Companies** accounts

- Intended for companies that sell the security solution to other companies (service providers, distributors or resellers of the service)

### **Customer Companies** accounts

- Intended for companies that use the security solution to protect their computer networks. Such companies can install, configure, manage and monitor their own protection.
- A customer company must be linked to at least one company administrator user account.

# CREATE COMPANIES ACCOUNTS

## Create COMPANY accounts

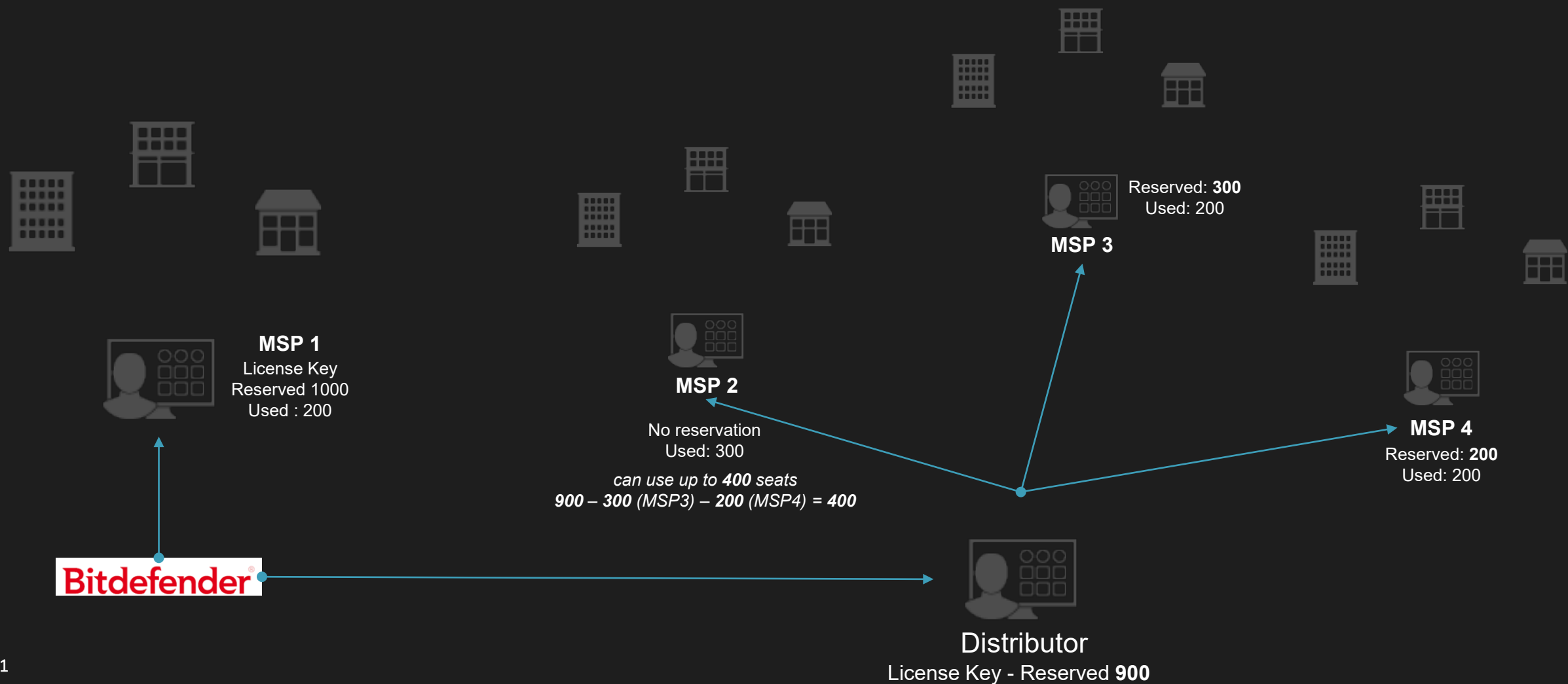
1. Access the **Control Center**
2. Go to **Companies**
3. Click **Add**
4. Add the Company name and fill in the other details requested
5. Under **Company Settings** select the company type (**Partner** or **Customer**)
6. Select the **license type** (**Trial**, **Licensed** or **Monthly subscription**)
7. When selecting **Licensed** you can enter an yearly key or enable “Monthly subscription”. Under “Monthly subscription”, partners can limit the number of seats by entering a specific number in the *Reserve seats* field.

The screenshot shows a form for creating a company account. The 'Type' dropdown is set to 'Partner'. Below it, there are two checked checkboxes: 'Manage Networks' and 'Allow your partner to assist with the security management of this company'. The 'License' section has a dropdown set to 'Monthly Subscription'. Below this, there is a 'Reserve seats' checkbox (checked) and a numeric input field with the value '20' and a note '(40 still available)'. To the right, the expanded dropdown menu for 'Type' shows 'Partner' and 'Customer' options. A blue arrow points from the 'Partner' option in the dropdown to the 'Partner' option in the expanded menu.



# MONTHLY SUBSCRIPTION

## RESERVE SEATS



# MONTHLY SUBSCRIPTION

## FEATURES

Available:

- Security for Exchange
- Email Security
- Full-Disk Encryption
- Security for Virtualized Environments
- Patch Management
- HyperDetect
- Sandbox Analyzer
- EDR



# GRAVITYZONE ON-PREMISE



# COMPONENTS

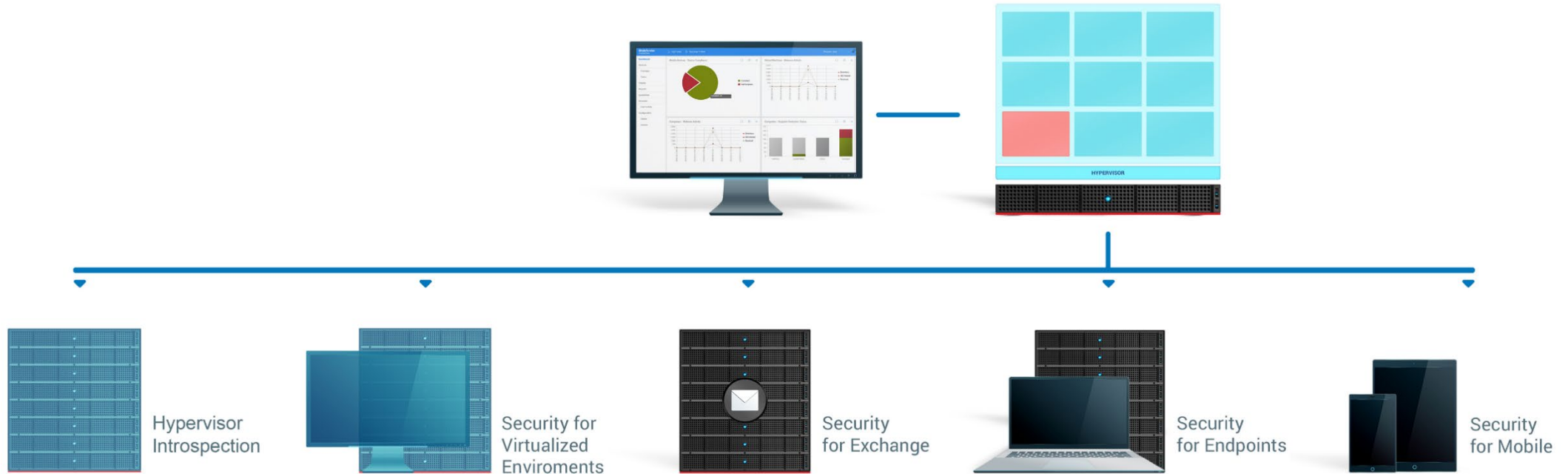
GravityZone Enterprise Security architecture includes 1 management component and 5 Security Services:

- Control Center
- Security for Endpoints
- Security for Virtualized Environments
- Security for Mobile Devices\*
- Security for Exchange\*
- Security for HVI\*\*



Security Services

# COMPONENTS



# ON-PREMISE

## GRAVITYZONE APPLIANCE

GravityZone Control Center is delivered as a virtual appliance, available in several different formats compatible with the main virtualization platforms.

➔ preconfigured virtual machine running a hardened Linux Server distribution (Ubuntu 16.04)

The GravityZone appliance can run **one**, **several** or **all** of the following roles:

- **Database**
- **Update Server**
- **Web Server (Web Console)**
- **Communication Server**

A GravityZone deployment requires running at least one instance of each role.

Depending on GravityZone roles distribution, you will run one to multiple GravityZone appliances.



# ON-PREMISE

## GRAVITYZONE APPLIANCE

Additional GravityZone appliance roles:

- **Role Balancer**

Allows you to install multiple instances of the **Communication Server** role or **Web Server** role.

➔ ensure high availability and scalability

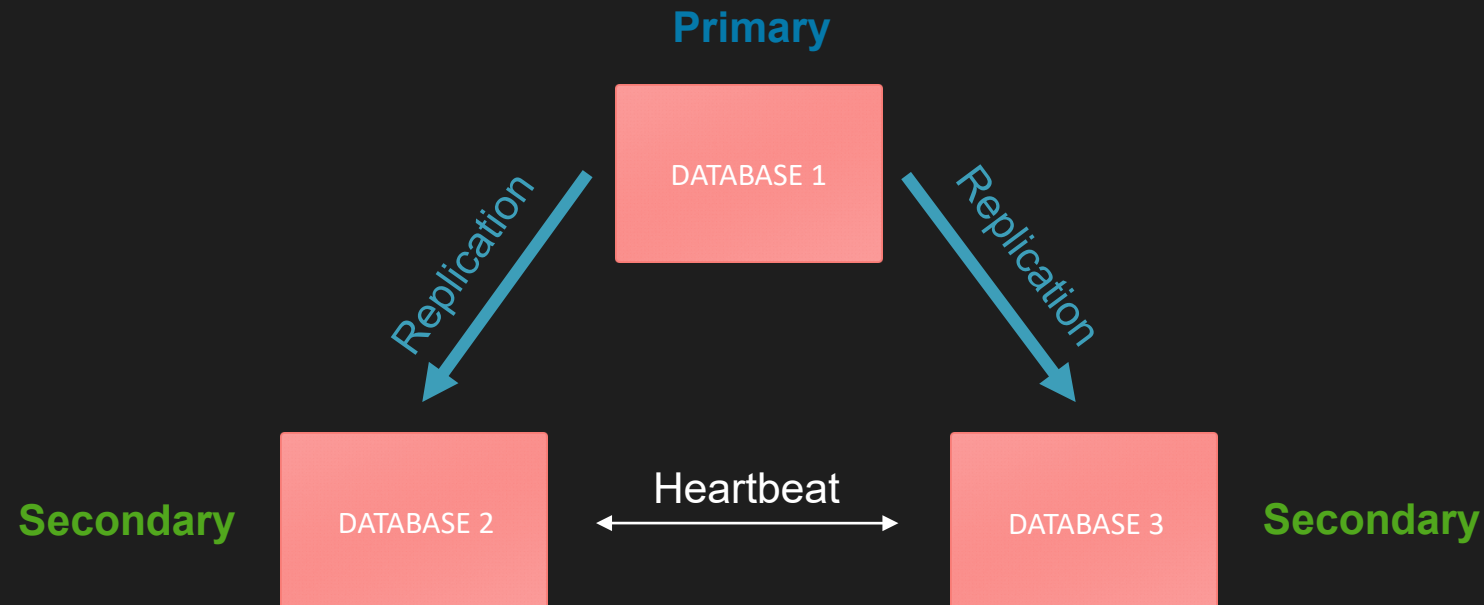
The built-in Role Balancer role cannot be installed together with other roles on the same GravityZone appliance.

3<sup>rd</sup> party software or hardware Role Balancers can also be used.

# ON-PREMISE DATABASE REPLICASET

This mechanism allows installing multiple database instances across a distributed GravityZone environment.

→ ensure high-availability in the case of a database instance failure

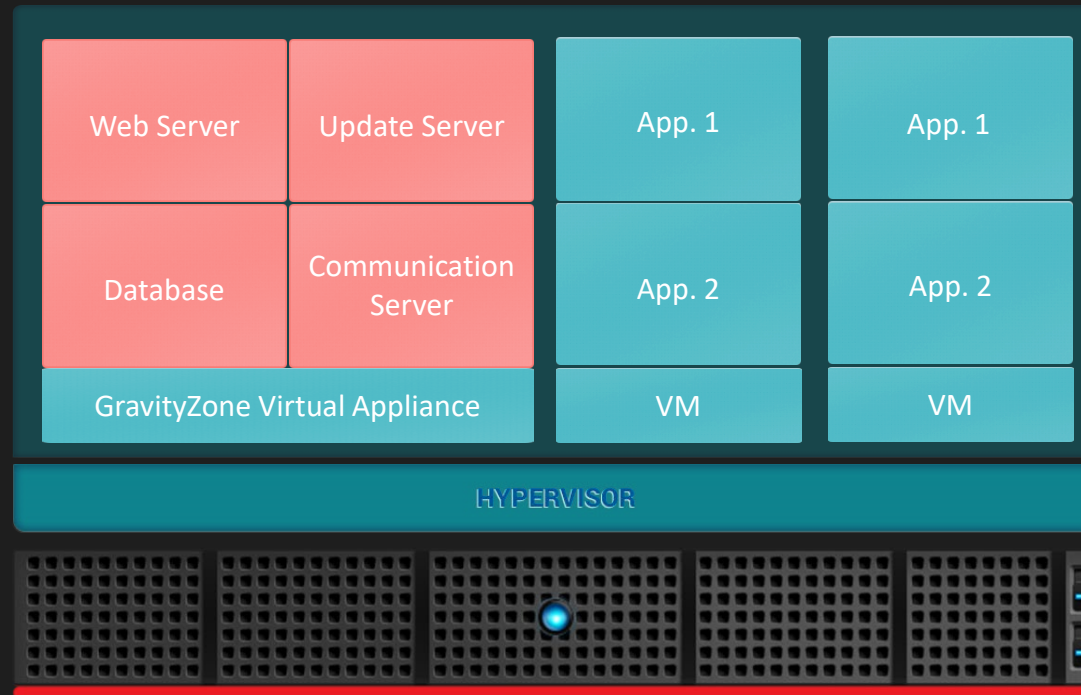


# DEPLOYMENT SCENARIOS



# DEPLOYMENT SCENARIOS

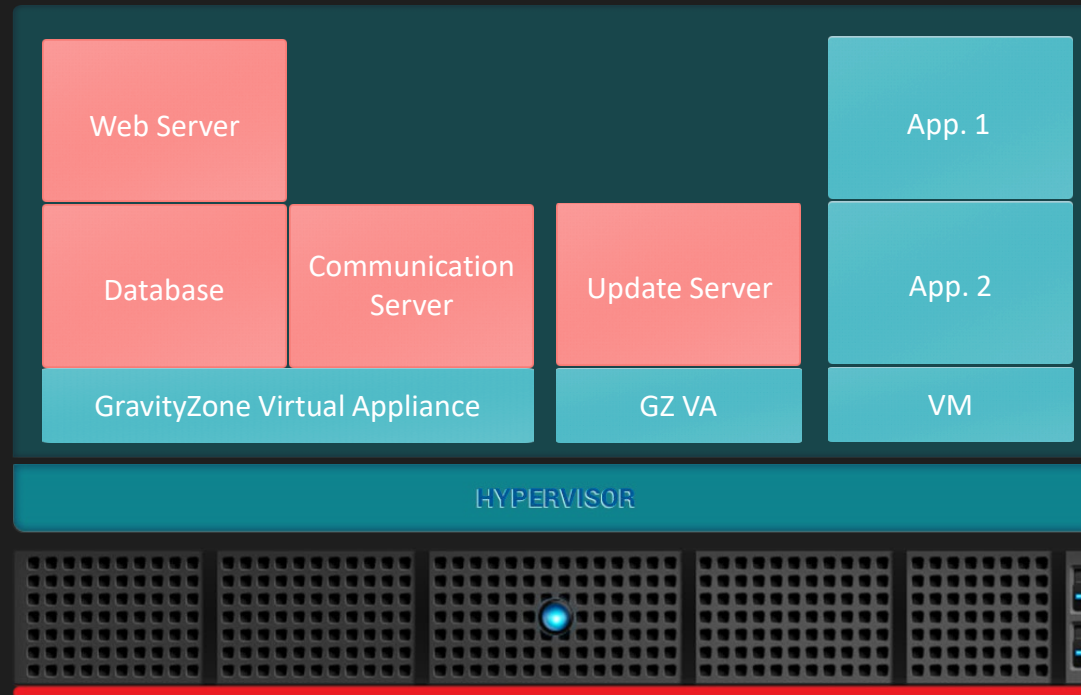
## ALL-IN-ONE DEPLOYMENT





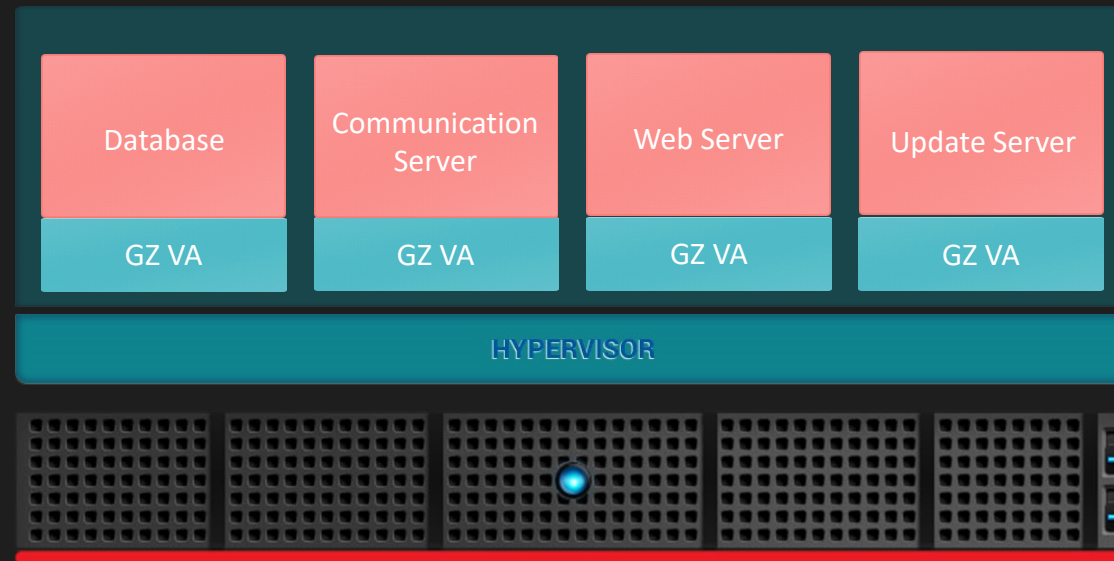
# DEPLOYMENT SCENARIOS

## STAGING



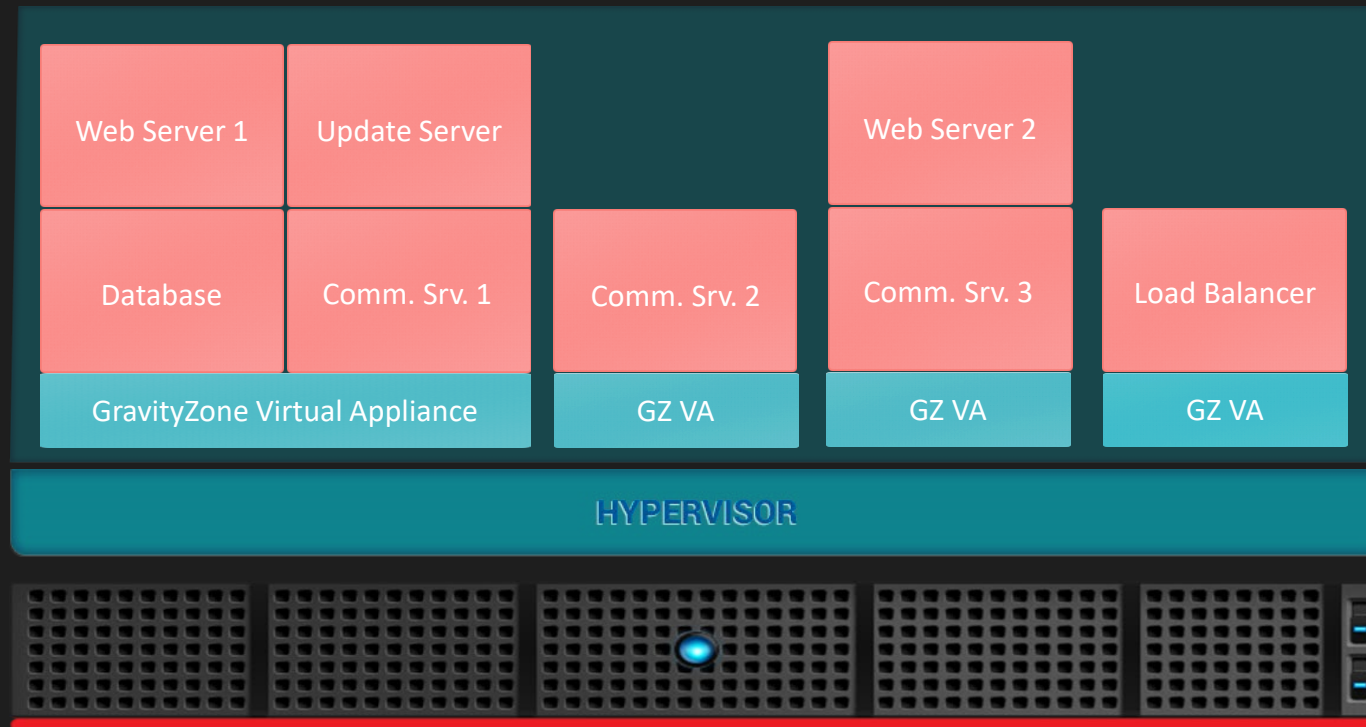
# DEPLOYMENT SCENARIOS

## CLUSTER DEPLOYMENT



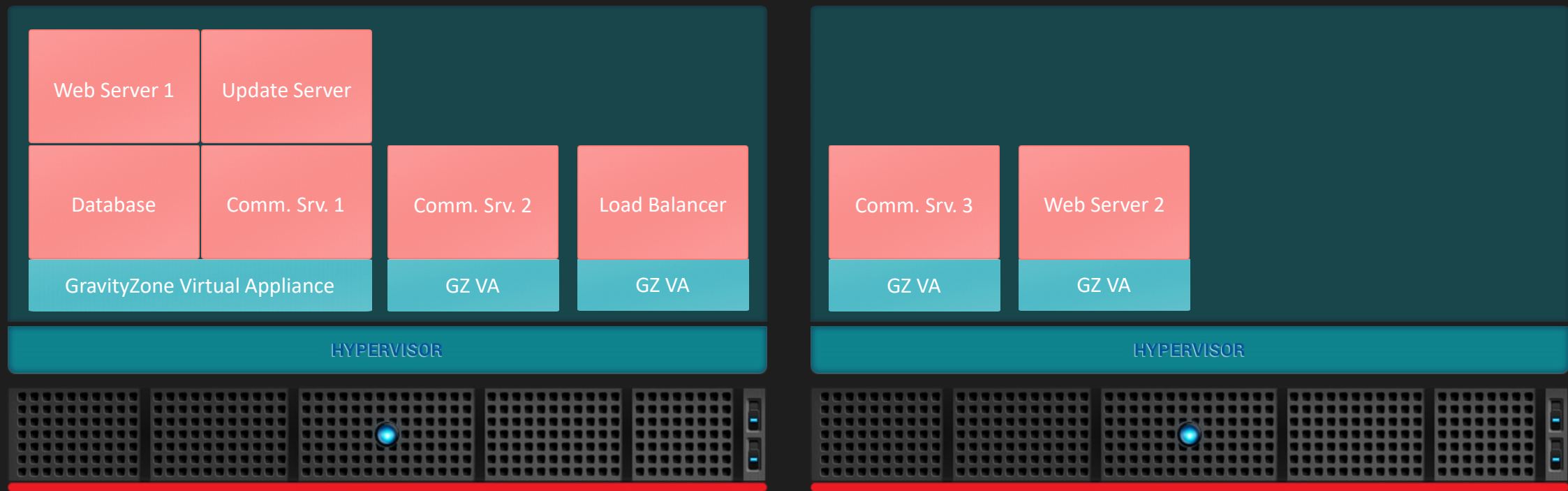
# DEPLOYMENT SCENARIOS

## LOAD BALANCED CLUSTER DEPLOYMENT



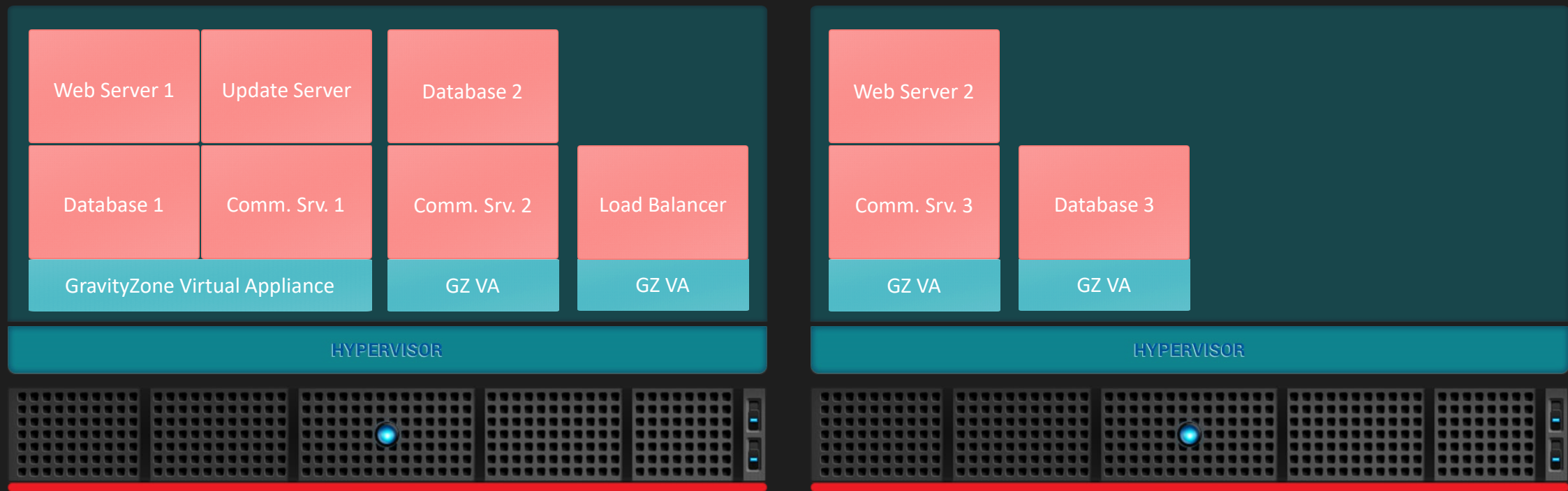
# DEPLOYMENT SCENARIOS

## CONTROL CENTER DEPLOYMENT ACROSS MULTIPLE HOSTS



# DEPLOYMENT SCENARIOS

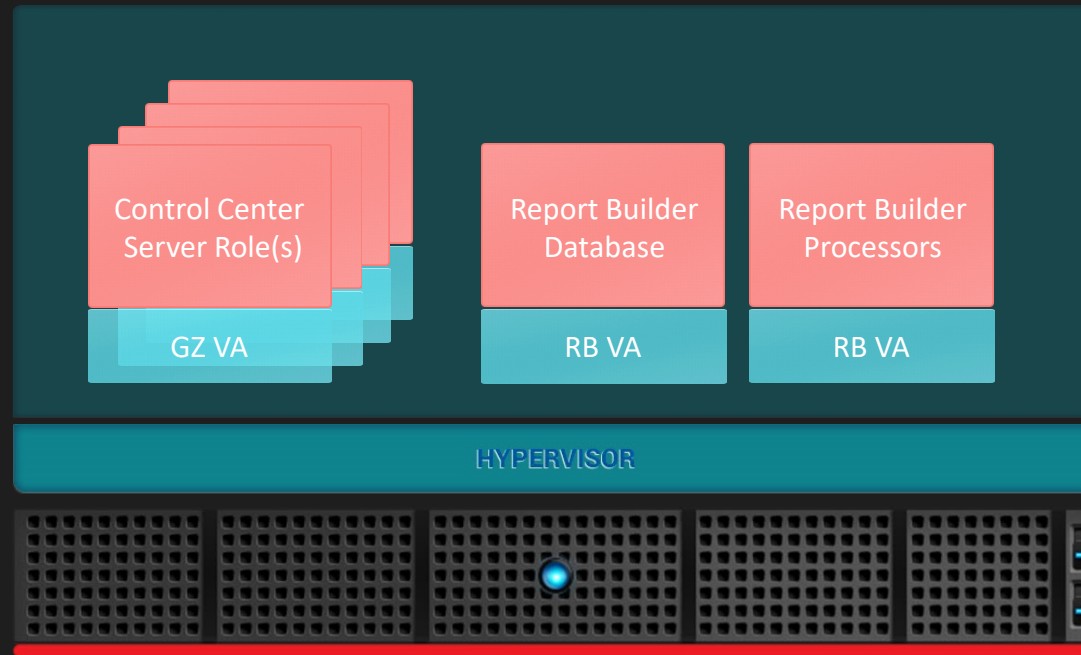
## CONTROL CENTER DEPLOYMENT WITH DATABASE REPLICA SET





# DEPLOYMENT SCENARIOS

## CONTROL CENTER WITH REPORT BUILDER



# LOCAL VS HYBRID VS CENTRAL SCANNING

# SECURITY FOR ENDPOINTS

## BEST SCANNING ENGINES

The scanning engines are automatically set during Bitdefender Endpoint Security Tools packages creation, letting the endpoint agent detect the machine's configuration and adapt the scanning technology accordingly



Local Scan



Hybrid Scan

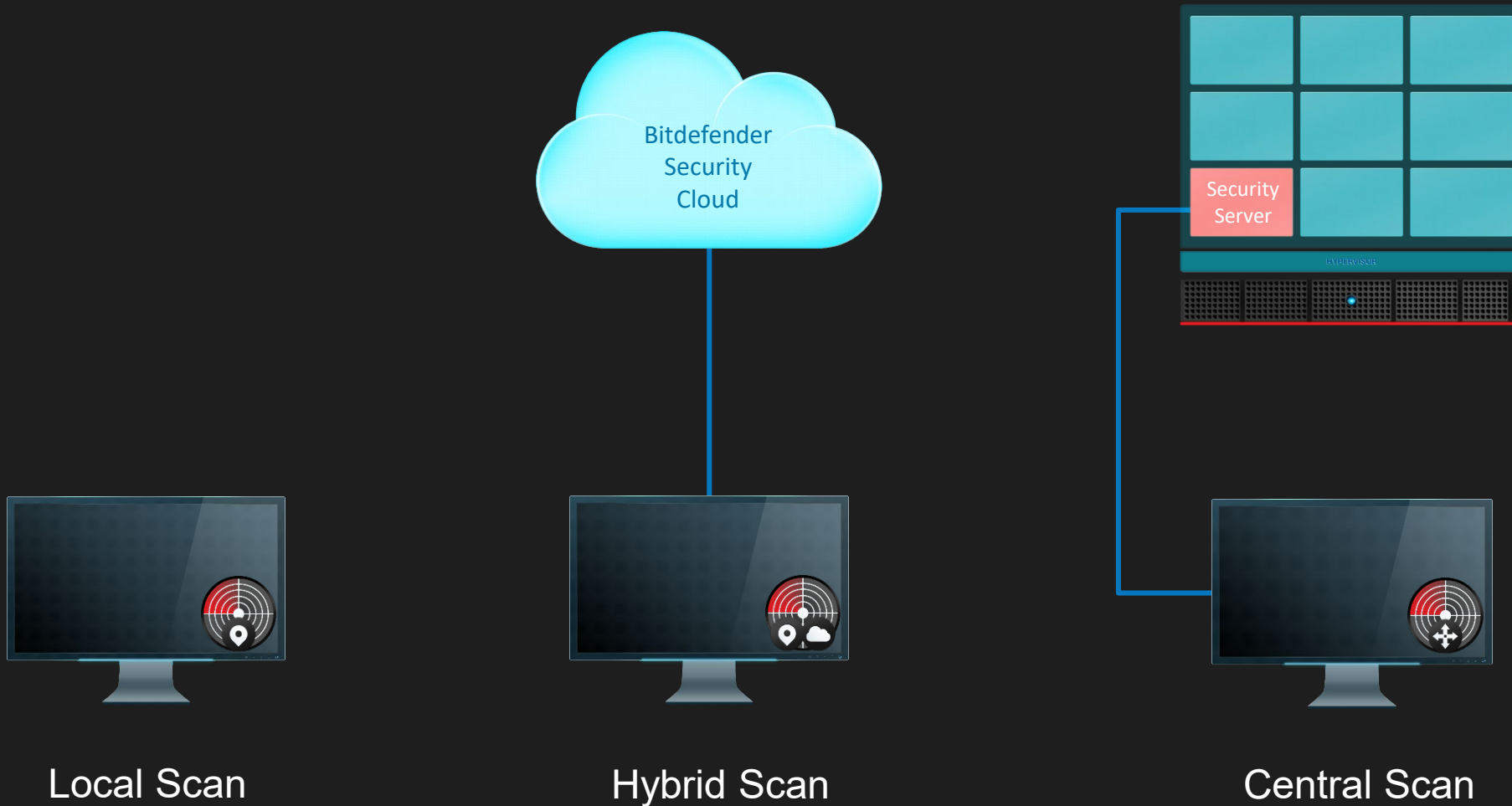


Central Scan



# SECURITY FOR ENDPOINTS

## BEST SCANNING ENGINES



# SECURITY SERVER

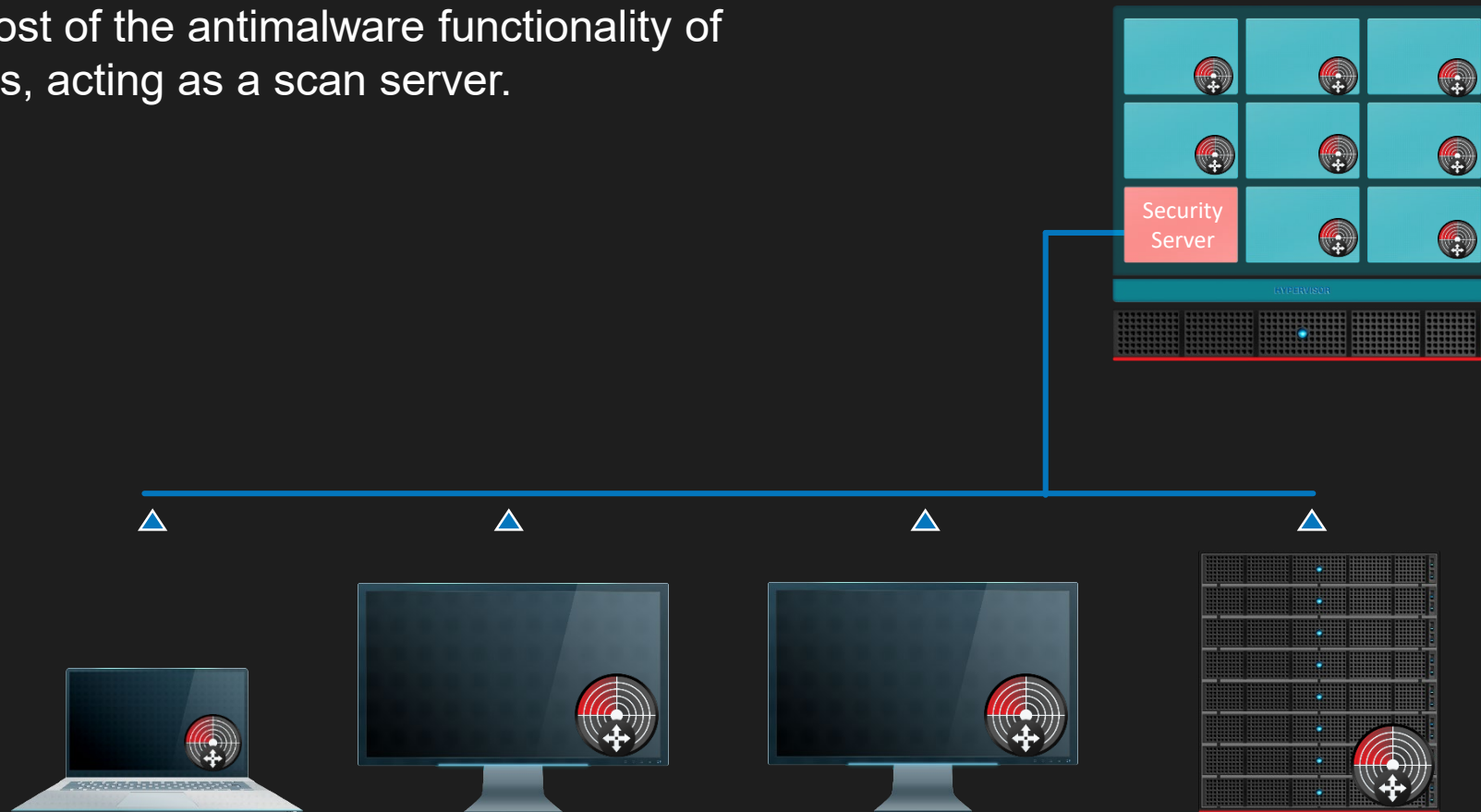




# SECURITY SERVER

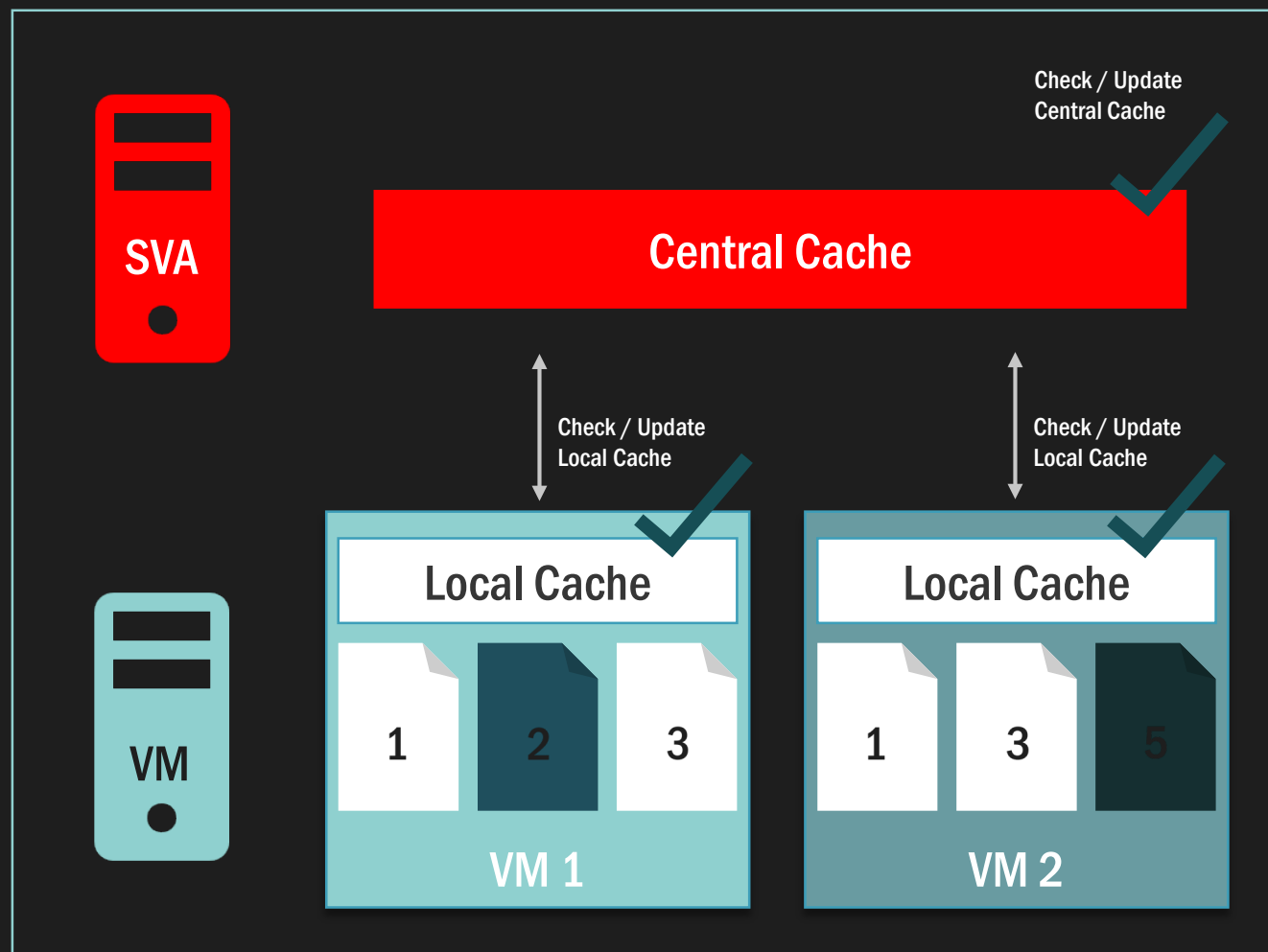
## DEFINITION

Security Server is a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware clients, acting as a scan server.



# SECURITY SERVER

## PATENTED TWO-LEVEL CACHING



Two-level caching on both the virtual machine (VM) and the security virtual appliance (SVA) enables higher antimalware efficiency

The SVA inspects each file only once even if it appears on multiple VMs

This helps avoid redundant scanning, significantly reducing CPU, RAM, IO, and network load

# SECURITY SERVER

## NEW TECHNOLOGIES

### ■ Caching Technology

Local Cache and Central Cache improvements

- All file types are now cached, regardless of file size
- Cache data survives Security Server reboot
- Entries expire after 24h

Shared Central Cache between Security Servers

### ■ New Load Balancing Mechanism

Load Balancing – Redundancy mode

- Provide high-availability for scanning service
- Avoid Security Server overload

Load Balancing – Equal Distribution mode

- Improve scanning performance
- Distribute load “more” evenly across Security Servers

# SECURITY SERVER ARCHITECTURES

## NSX Architecture:

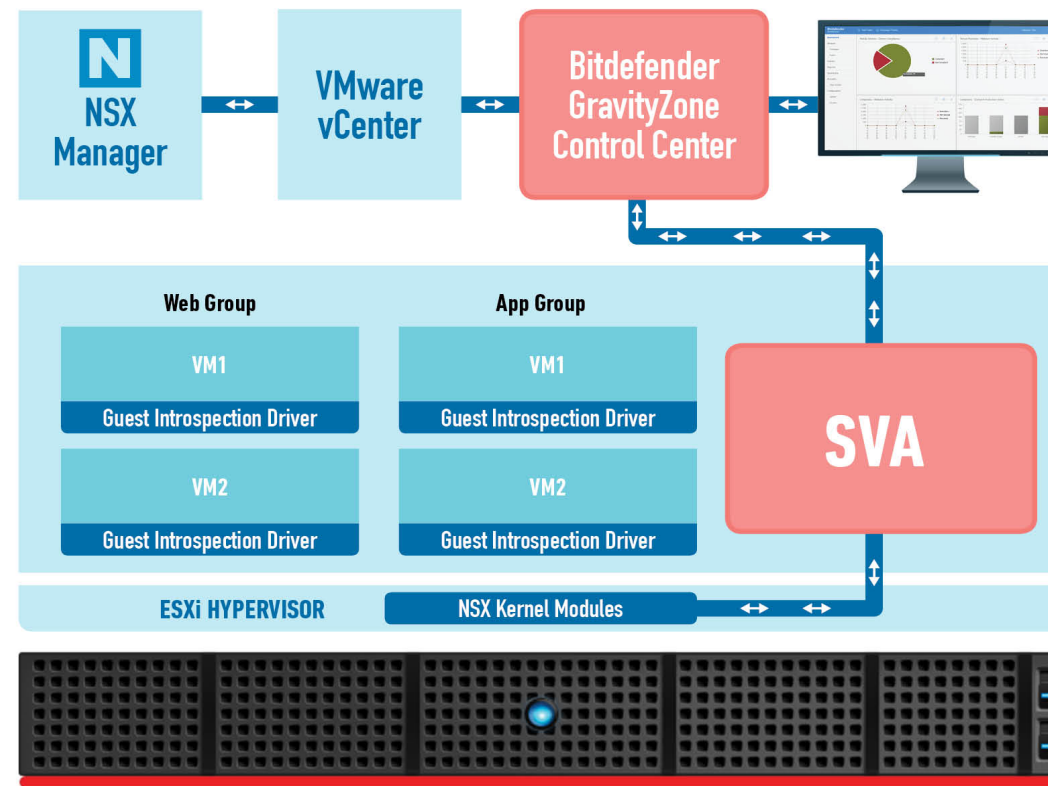
- Security Server is installed on every physical host in the datacenter that contains VMs that needs protection

## Multiplatform Architecture:

- Security Server is installed on one or more hosts so as to accommodate the number of virtual machines and physical clients to be protected
  - ➔ consider the number of protected systems, resources available for Security Server on hosts, as well as network connectivity between Security Server and the protected systems

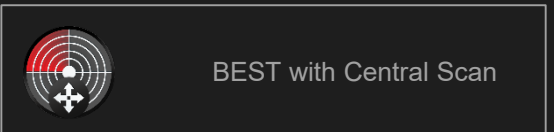
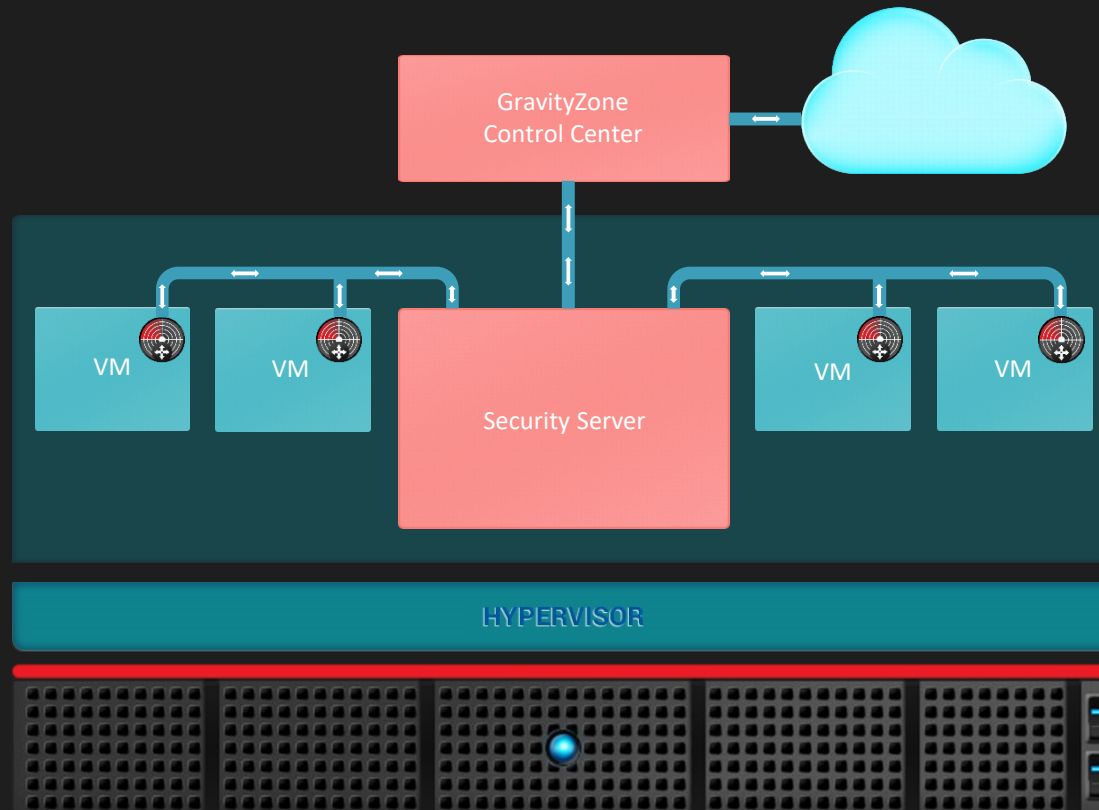
# SECURITY FOR VIRTUALIZED ENVIRONMENTS

## VMWARE ENVIRONMENTS WITH NSX



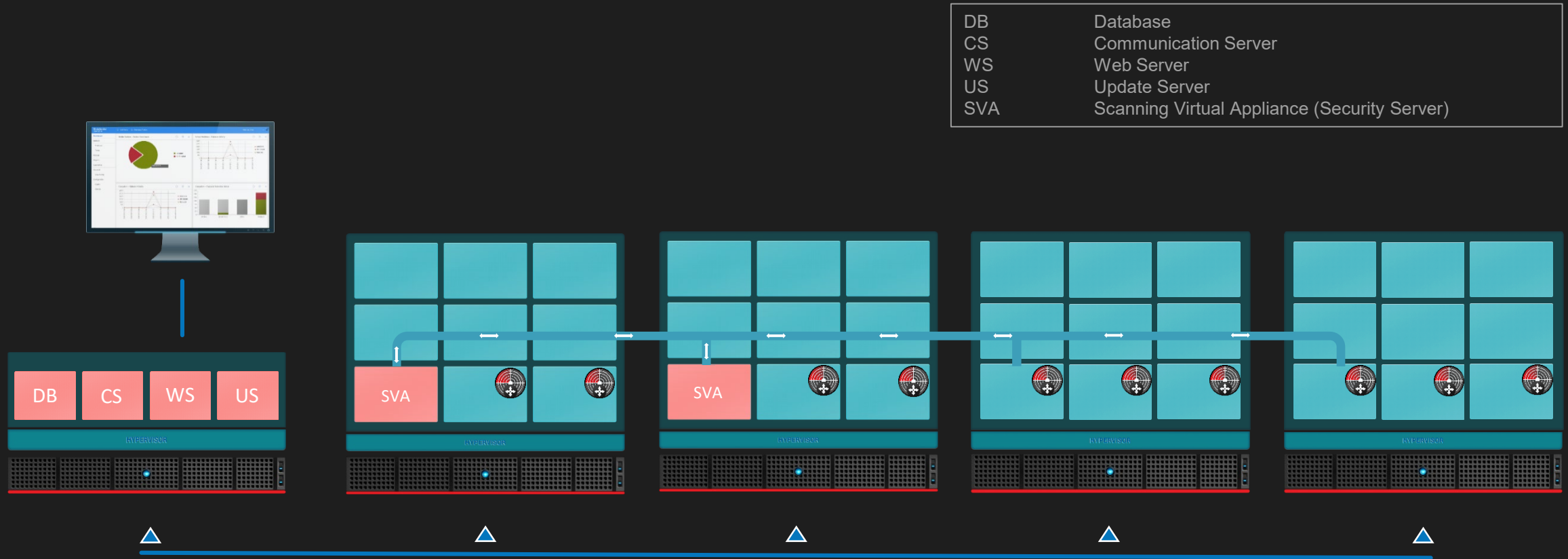
# SECURITY FOR VIRTUALIZED ENVIRONMENTS

## MULTIPLATFORM ARCHITECTURE



# SECURITY FOR VIRTUALIZED ENVIRONMENTS

## MULTIPLATFORM ARCHITECTURE





# MACHINE LEARNING



# MACHINE LEARNING

## WHY IS IT STILL IMPORTANT?

- Early detection of new and advanced threats
- Powered by data-centric mathematical algorithms
- Key ingredient in AI Technology
- Non-resource intensive
- Promotes efficient utilization of resources
- Part of a single, integrated endpoint security agent and management platform

# HYPERDETECT

## TUNABLE MACHINE LEARNING

HyperDetect is an advanced layer of security, which uses specialized local machine models, behavioral analysis techniques trained to spot hacking tools, exploits and malware obfuscation techniques, in the pre-execution stage:

- Targeted attack
- Suspicious file and network traffic
- Exploits
- Ransomware
- Greyware

# HYPERDETECT

## CONTINUED

General

Antimalware

On-Access

On-Demand

HyperDetect

Settings

Security Servers

Sandbox Analyzer

Firewall

Content Control

Device Control

Relay

Exchange Protection

Encryption

☒ HyperDetect

This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.

Protection Level

...to counter relevant threats

☒ Targeted Attack

☒ Suspicious files and network traffic

☒ Exploits

☒ Ransomware

☒ Grayware

Set the detection-aggressiveness level...

☐ Permissive

☐ Normal

☒ Aggressive

☐

☐

☒

☐

☒

☐

☐

☐

☒

☒

☐

☐

Actions

Files:

Deny

Deny

Disinfect

Delete

Move files to quarantine

Report Only

Reset to default

☒ Extend reporting on higher levels

☐ Extend reporting on higher levels

Provides maximum detection accuracy without false positives

Delivers full visibility into suspicious activities

41

# ADVANCED ANTI-EXPLOIT

## NEW PROACTIVE TECHNOLOGY

- Powered by machine learning, Advanced Anti-Exploit is a technology that stops zero-day attacks carried out through evasive exploits
- Catches the latest exploits in real-time and mitigates memory corruption vulnerabilities that can evade other security solutions
- Protects most commonly used applications, such as browsers, Microsoft Office or Adobe Reader, as well as others
- Watches over system processes and protects against security breaches and hijacking existing processes

# ADVANCED ANTI-EXPLOIT

## MONITORING APPLICATIONS

Predefined Applications ^		<a href="#">Reset to Default</a>
Application	Process Name	Status
<a href="#">7-Zip Archiver Console</a>	7z.exe	Default
<a href="#">7-Zip Archiver GUI</a>	7zG.exe	Default
<a href="#">Acrobat Reader</a>	Acrobat.exe;Acroord32.exe	Default
<a href="#">Foxit Reader</a>	FoxitReader.exe	Default
<a href="#">Libre Office, Open Office</a>	Soffice.bin	Default
<a href="#">Microsoft Office, Microsoft Word</a>	Winword.exe	Default
<a href="#">Microsoft Office, Microsoft Excel</a>	Excel.exe	Default
<a href="#">Microsoft Office, Microsoft PowerPoint</a>	Powerpnt.exe;Pptview.exe	Default
<a href="#">Microsoft Office, Microsoft Outlook</a>	Outlook.exe	Default
<a href="#">Microsoft Office, Microsoft Equation Editor</a>	Eqnedt32.exe	Default
<a href="#">Microsoft Office, Conflict Resolution for Access</a>	Acecnflt.exe	Default
<a href="#">Microsoft Office, Filter Loader</a>	Fltldr.exe	Default
<a href="#">Microsoft Internet Explorer</a>	Iexplore.exe	Default
<a href="#">Mozilla Firefox</a>	Firefox.exe	Default
<a href="#">Mozilla Thunderbird</a>	Thunderbird.exe	Default
<a href="#">Opera Browser</a>	Opera*.exe;Launcher*.exe	Default
<a href="#">Apple Safari</a>	Safari.exe;WebKit2WebProcess.exe	Default
<a href="#">Flash Player Container</a>	FlashPlayerPlugin*.exe;Plugin-container.exe	Default
<a href="#">WinRAR Archiver GUI</a>	WinRAR.exe	Default

# ADVANCED ANTI-EXPLOIT

## CUSTOM APPLICATIONS

General

HVI

Antimalware

On-Access

On-Demand

Hyper Detect

Advanced Anti-Exploit

Settings

Security Servers

Sandbox Analyzer

Firewall

Content Control

Application Control

Device Control

Relay

Exchange Protection

< Back

Advanced Anti-Exploit

Add Application

Details

Application Name: \*

Application Name

Processes Names: \*

Processes Names

Use the semicolon (;) to separate processes

Exploit Detection Techniques

Reset to Default

<input checked="" type="checkbox"/>	All	Report Only
<input checked="" type="checkbox"/>	ROP Emulation	Report Only
<input checked="" type="checkbox"/>	ROP Stack Pivot	Report Only
<input checked="" type="checkbox"/>	ROP Illegal Call	Report Only
<input checked="" type="checkbox"/>	ROP Stack Misaligned	Report Only
<input checked="" type="checkbox"/>	ROP Return To Stack	Report Only
<input checked="" type="checkbox"/>	ROP Make Stack Executable	Report Only
<input checked="" type="checkbox"/>	Flash Generic	Report Only
<input checked="" type="checkbox"/>	Shellcode Execution	Report Only
<input checked="" type="checkbox"/>	Shellcode LoadLibrary UNC	Report Only
<input checked="" type="checkbox"/>	Anti-Detour	Report Only
<input checked="" type="checkbox"/>	Flash Payload	Report Only
<input checked="" type="checkbox"/>	ROP Create Thread	Report Only
<input checked="" type="checkbox"/>	Anti-Meterpreter	Report Only
<input checked="" type="checkbox"/>	Obsolete Process Creation	Report Only



# ENDPOINT SECURITY FEATURES

# LAYERED NEXT-GEN EPP WITH EDR IN A SINGLE AGENT

PREVENT

## HARDENING & CONTROL



Patch Management



Full-Disk Encryption



Web-Threat Protection



Application Control



Device Control



Firewall

DETECT

## PRE-EXECUTION DETECTION



Sign. & Cloud Lookup



Local & Cloud ML



HyperDetect Tunable ML



Sandbox Analyzer

## ON- & POST-EXECUTION DETECTION



Anti-Exploit



Process Inspector



Event Recorder



Threat Analytics

INVESTIGATE  
& RESPOND

## AUTOMATIC ACTION



Access Blocking



Quarantine



Disinfection & Removal



Process Termination



Rollback

## INVESTIGATION & RESPONSE



IoC Lookup



Blocklist



Network Isolation



Sandbox Detonation



Visualization

INFORM

## REPORTING & ALERTING



Dashboards & Reports



Notifications



SIEM Integration



API Support

# APPLICATION CONTROL

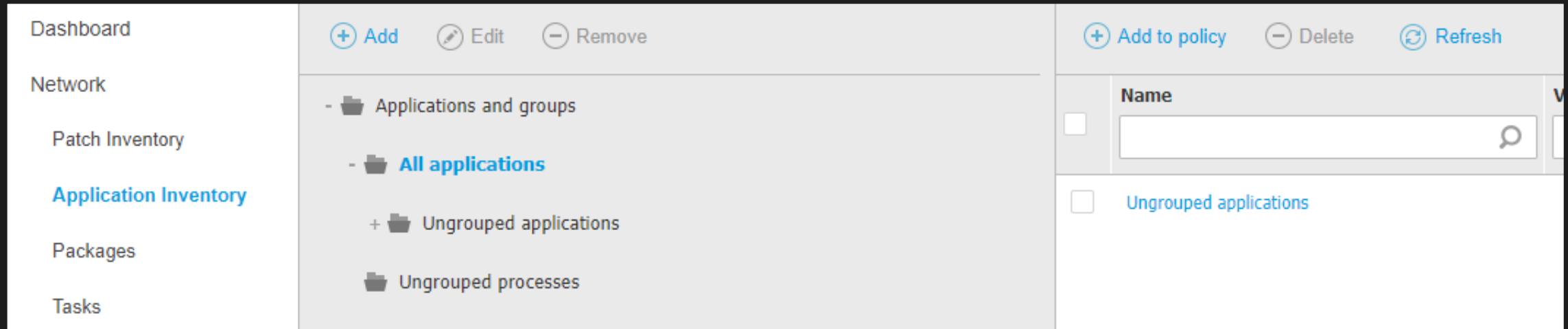
## BENEFITS

- Introduces whitelisting technology
- First layer of defense when it comes to overall system hardening
- Prevents the installation and execution of unwanted, untrusted and malicious applications
- Flexible for organizations to better control the use of installation applications as well as prevent the use of unknown software
- Suitable for organizations that are primary targets for Ransomware and APT

# APPLICATION CONTROL

## APPLICATION INVENTORY








Application Inventory shows all of the applications installed on endpoints that have the Application Control module installed and enabled

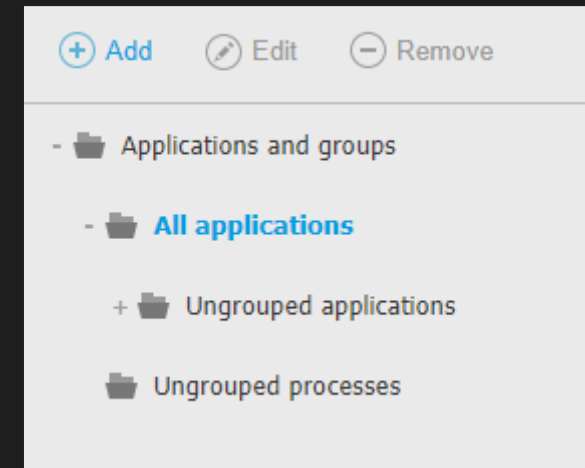


# APPLICATION CONTROL

## APPLICATIONS

- The applications are grouped per categories
- Uncertain applications and processes are stacked in the Ungrouped Applications and Ungrouped Processes folders
- Custom folders can be created

 3D Builder 11	<input type="checkbox"/> 3D Builder 12	12
 3D Builder 12	<input type="checkbox"/> 3D Builder 14	14
 3D Builder 14	<input type="checkbox"/> 64 bit driver installer 1	1
 64 bit driver installer 1	<input type="checkbox"/> 7-Zip 0	0
 7-Zip 0	<input type="checkbox"/> 7-Zip 15	15
 7-Zip 15	<input type="checkbox"/> 7-Zip 15.08 beta (x64) 15	15
 7-Zip 15.08 beta (x64) 15	<input type="checkbox"/> 7-Zip 15.14 (x64) 15	15



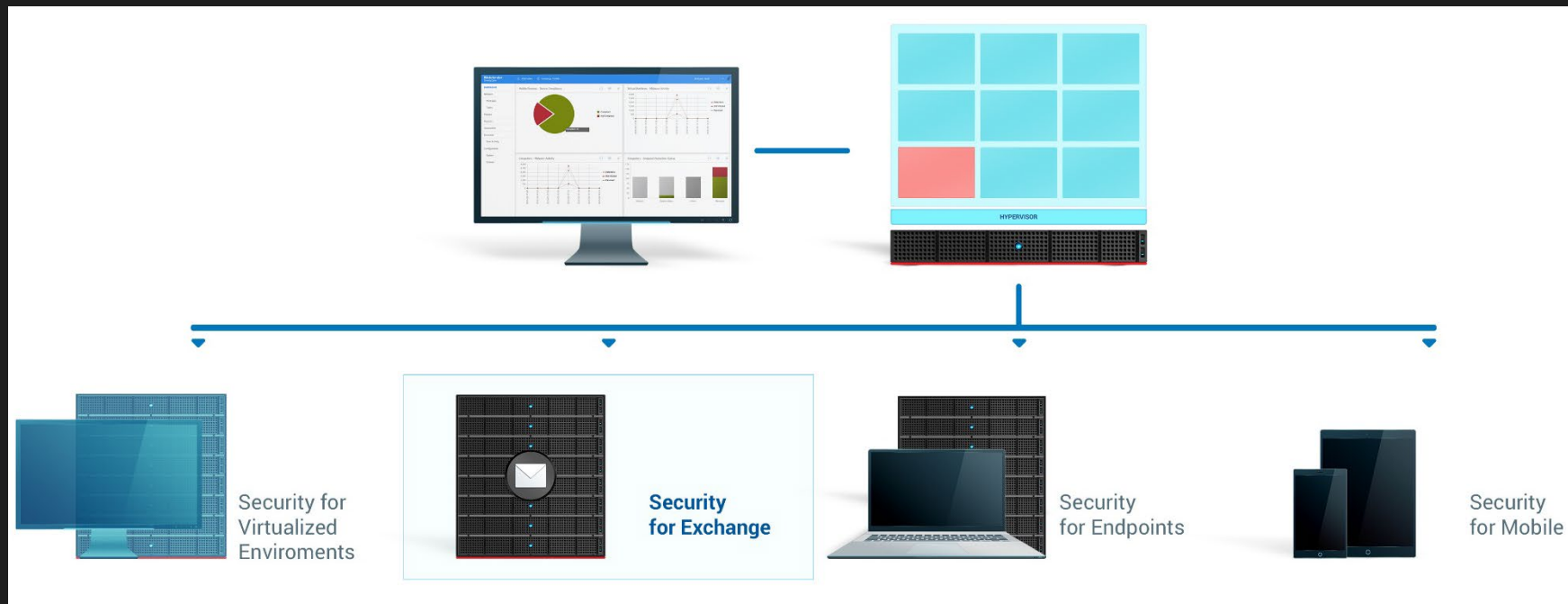
# SECURITY FOR EXCHANGE



# SECURITY FOR EXCHANGE

## DEFINITION

Bitdefender Security for Exchange provides antimalware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the Microsoft Exchange Server.





# SECURITY FOR EXCHANGE

## EXCHANGE INTEGRATION

Bitdefender Endpoint Security Tools with Exchange Protection automatically integrates with the Exchange Servers, depending on the server role. For each role only the compatible features are installed:

Features	MS Exchange 2016/2013		MS Exchange 2007/2010		
	Edge	Mailbox	Edge	Hub	Mailbox
<b>Transport Level</b>					
Antimalware	✓	✓	✓	✓	
Antispam	✓	✓	✓	✓	
Content Filtering	✓	✓	✓	✓	
Attachment Filtering	✓	✓	✓	✓	
<b>Exchange Store</b>					
Antimalware On-demand scanning		✓			✓

# SECURITY FOR EXCHANGE

## HOW PROTECTION WORKS

Filters all Exchange email traffic – incoming, outgoing and internal, regardless of the protocol or mail client used to send emails:

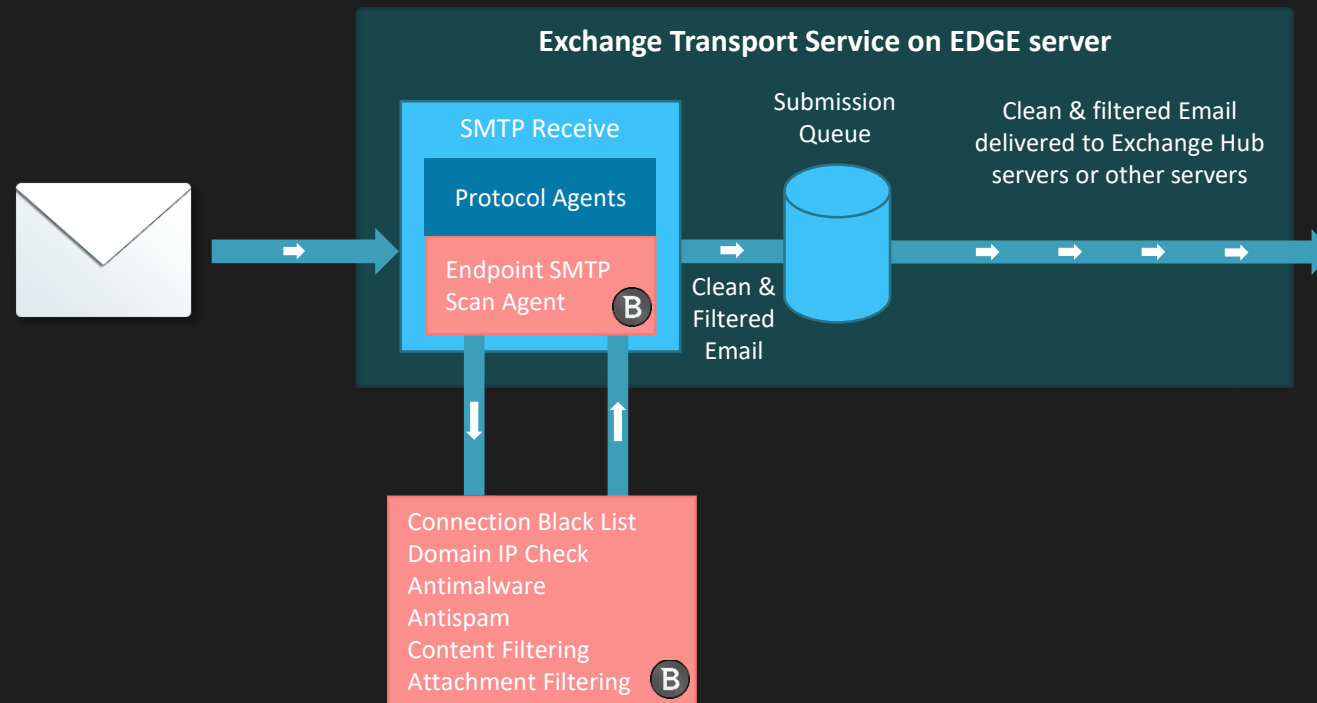
- Desktop clients using MAPI or POP3/SMTP (Microsoft as well as other popular mail client software)
- Mobile clients using Exchange ActiveSync
- Web access via Outlook Web App (OWA)
- Mobile access via Outlook Web App (OWA)

Additionally, allows scanning the Exchange mailbox and public folder databases for malware, by using Exchange Web Services API from Microsoft.

# SECURITY FOR EXCHANGE

## INTEGRATION WITH EXCHANGE TRANSPORT SERVICE

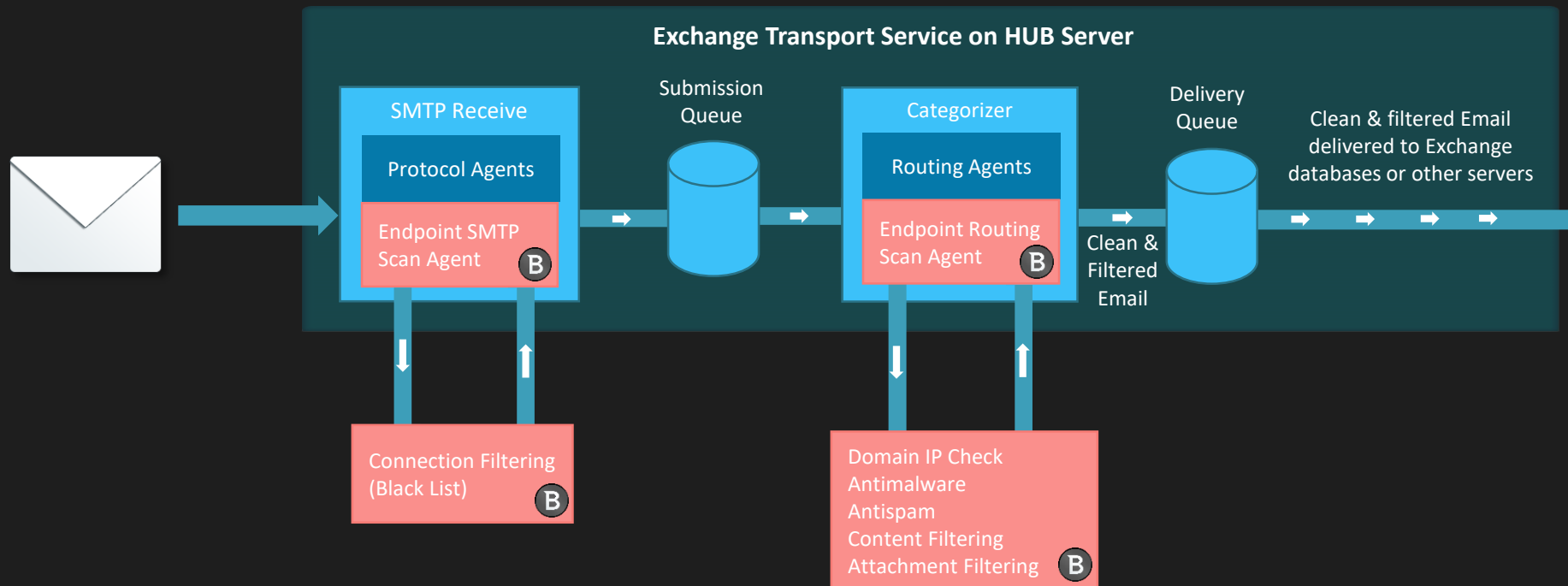
Edge Server:



# SECURITY FOR EXCHANGE

## INTEGRATION WITH EXCHANGE TRANSPORT SERVICE

Hub Server:



# HYPERVISOR INTROSPECTION



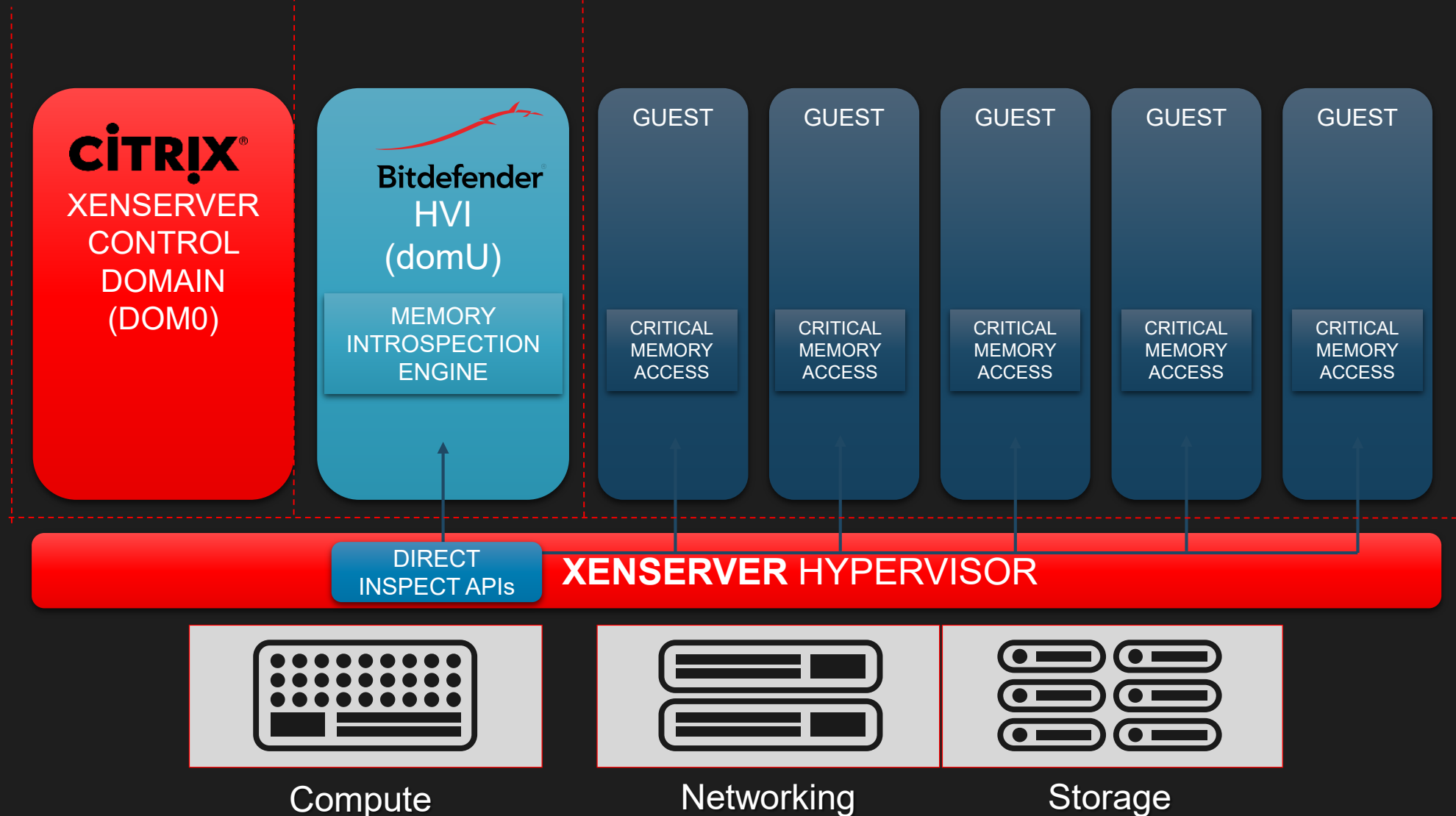
# HYPERVISOR INTROSPECTION (HVI)

## BENEFITS

- New security layer against targeted attacks
- Real-time attack detection at the hypervisor layer
- Truly agentless
- Minimum performance impact
- Already proven against several APTs (APT28, Energetic Bear, Darkhotel, Epic Turla, Regin, Zeus, Dyreza, Gameover)

# A CHANGE IN PARADIGM

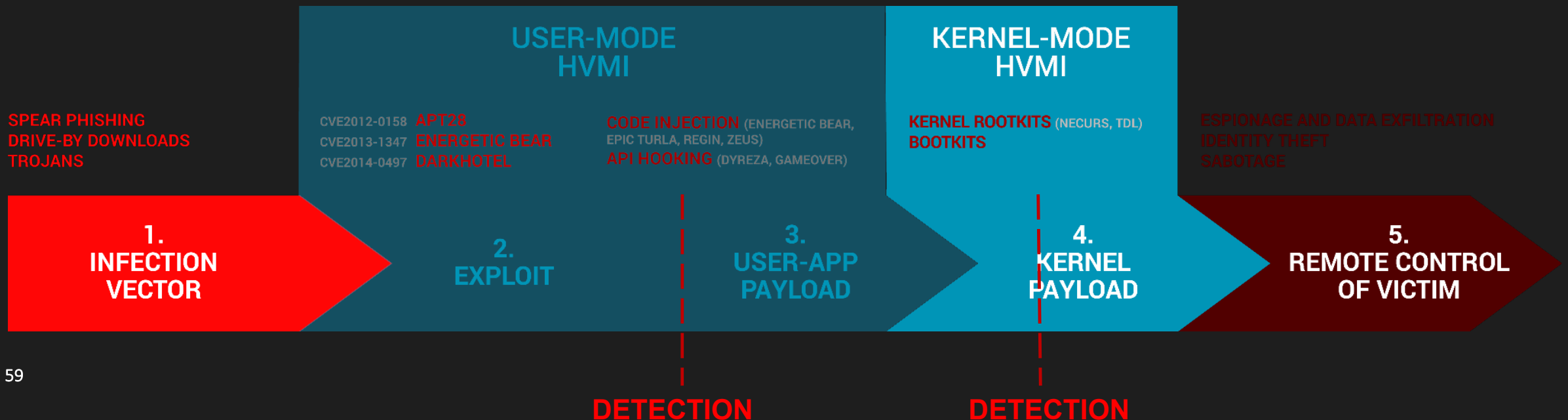
STRONG ISOLATION (HYPERVISOR CONTROLLED, HARDWARE ENFORCED)





# ADVANCED ATTACK KILL CHAIN WITH HYPERVISOR INTROSPECTION

- TARGETS TECHNIQUES
- PROTECTS AGAINST KNOWN AND UNKNOWN ATTACKS
- PREVENTS / DETECTS / REPOTS THESE ATTACKS IN REAL TIME
- BOTH USER MODE AND KERNEL MODE

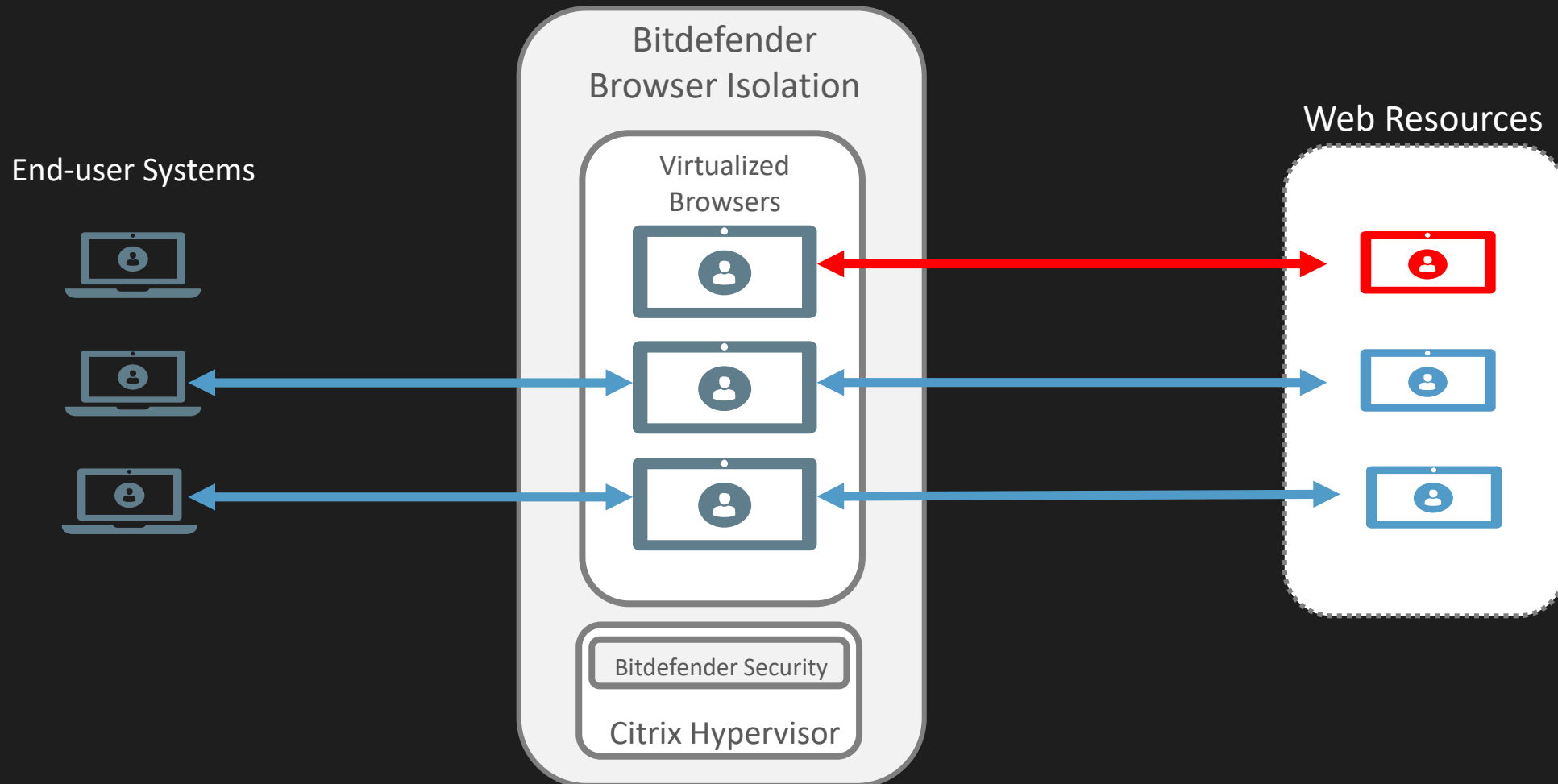


# BROWSER ISOLATION



# BROWSER ISOLATION

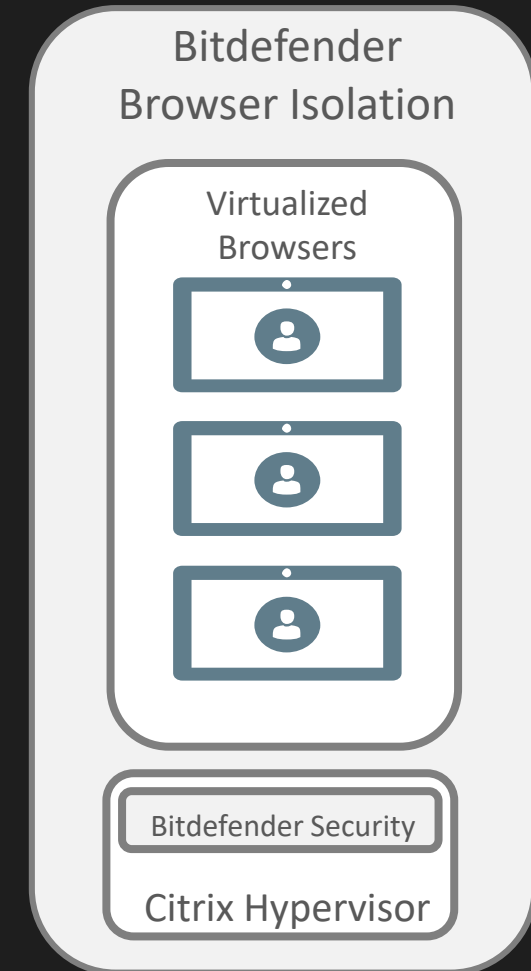
## ISOLATED AND SECURED



# BROWSER ISOLATION

## COMPONENTS

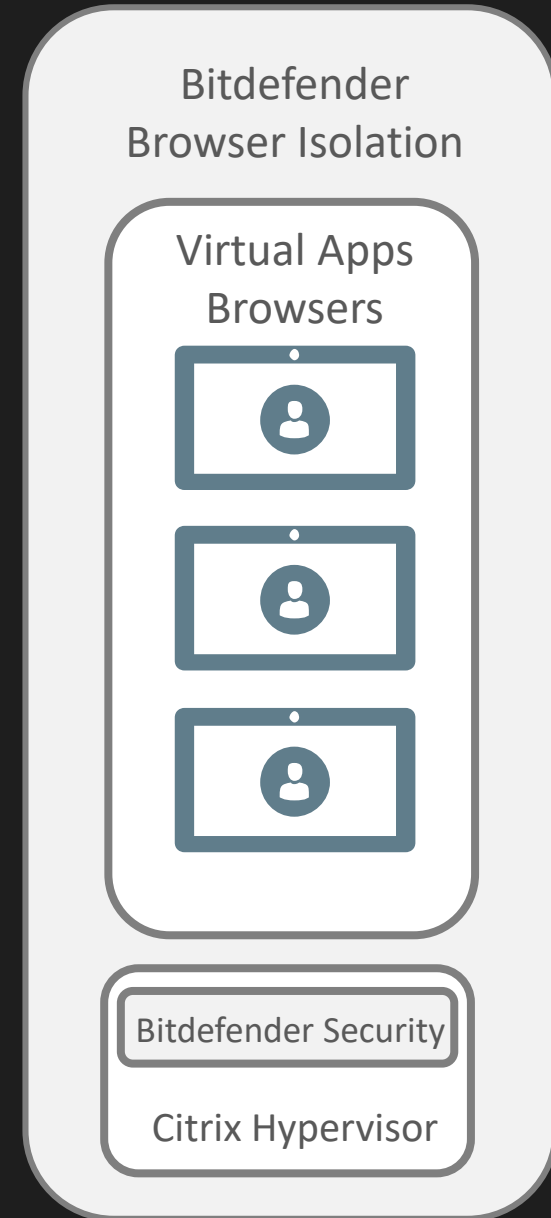
- **Browser virtualization and delivery**
  - Have *already invested* in Citrix Virtual Apps
  - Most frequently virtualized applications are browsers
- **Citrix Hypervisor**
  - Only for targeted scenarios
  - Think of it *as an appliance*
- **Bitdefender Security**
  - Hypervisor Introspection provides *unique* Bitdefender security



# BROWSER ISOLATION

## KEY VALUE POINTS

- **Isolate**  
Move the execution of web content off of high-value systems
- **Secure**  
Prevent attackers from getting a foothold to then attack other assets
- **Unleash**  
Push untapped Citrix Virtual Apps (XenApp) capabilities to a new level



# RISK ANALYTICS



# RISK ANALYTICS

## BENEFITS

- System Misconfiguration is the second biggest cause of mega-scale security disasters
- Majority of threats target well-known application and configuration vulnerabilities.\*\*
- WannaCry could have been blocked with simple configuration changes.\*\*
- “Patch panic” caused by not knowing which systems are truly at risk

# RISK ANALYTICS

## KEY FEATURES

- Risk analytics engine continuously computes a risk score to easily sort and prioritize assets
- Prioritizes security remediation on risk severity and prevalence across 206 indicators
- Automatic fix available for many indicators
- Enables System Hardening with GravityZone Patch, Encryption, Device Control, Application Control and Firewall
- Fully native to all GravityZone products
- Powered by Bitdefender Labs global threat research

### Example Configuration Analytics Rules:

- ASLR Disabled
- Session Manager Protection Mode Disabled
- Insecure Guest Logon Enabled
- No Autorun Disabled
- Telnet Service Enabled



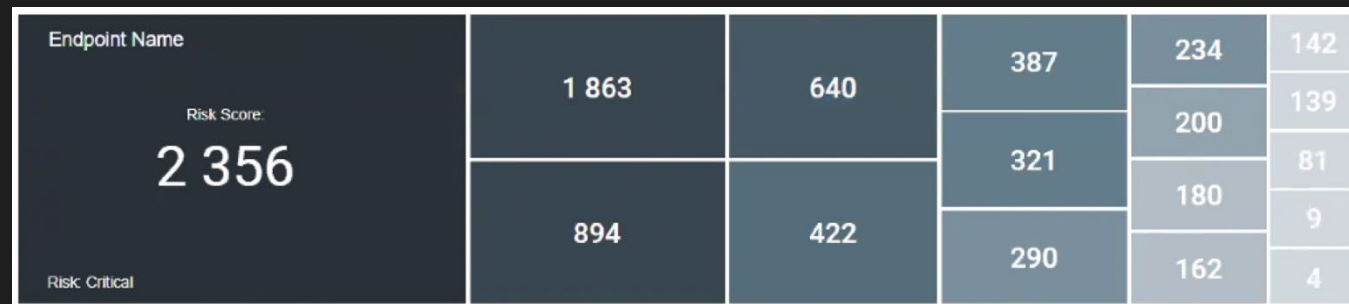
# ENDPOINT RISK ANALYTICS



Enterprise-Wide Risk Dashboard

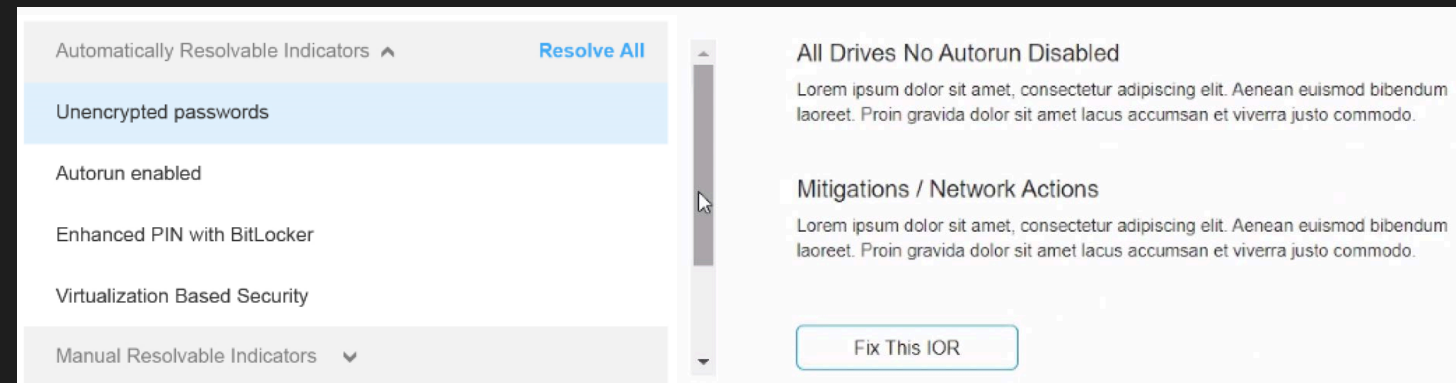


View prioritized risks across the Enterprise (1240 Disabled Firewalls)



See the highest priority endpoints by Risk Score

View Risks by endpoint and automatically fix specific misconfigurations



# EDR

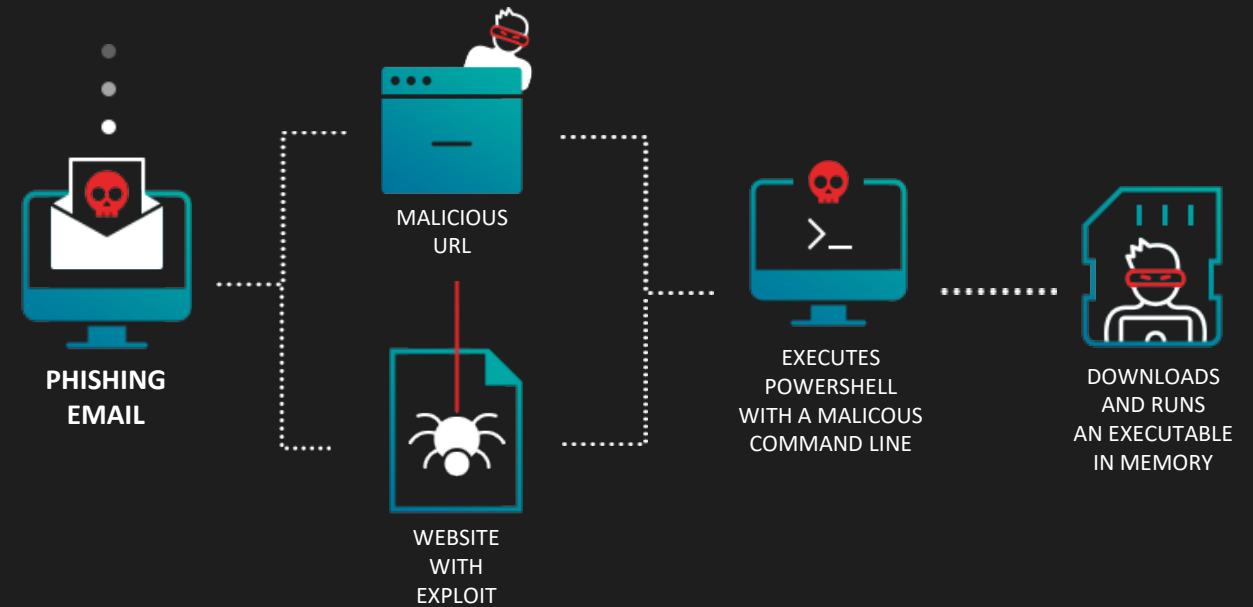


# EDR

## LOW OVERHEAD

Endpoint Detection and Response (EDR) provides 360 degree visibility of threats:

- Provides insights on sophisticated threats that evaded prevention mechanisms
- Unified approach reduces needs for advanced security skills
- Works with Malware Prevention, NTA and ERM to continuously eliminate protection gaps



# INTEGRATED EDR FOR ANY ORGANIZATION

The screenshot shows the Bitdefender GravityZone console. The left sidebar contains navigation links: Dashboard, Incidents, Blocklist, Search, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Accounts, and User Activity. The main content area is titled 'Incidents' and features a filter bar with 'Severity Score' (High, Medium, Low), 'Status' (Open, Investigating, Closed), 'Attack Type' (Exploit, Ransomware, Fileless attacks, Ransomware, Exploit, Fileless attacks), and 'MITRE Tag'. Below the filters, incidents are listed in a table. The incident #1356 is highlighted, showing a severity score of 85, status of 'Blocked', and a 'View' button. The detailed view of incident #1356 shows it was created at 14:24 on 27 Jun, has a severity of 85, and is in a 'Blocked' state. It lists the attack type as 'Ransomware, Adware, Spyware, Worm, Exploit' and the MITRE techniques as 'Execution: Command Line Interface, Exploitation for Client Execution, PowerShell +2'. The incident has impacted 13 endpoints and involved 71 files and processes.

## Case Study

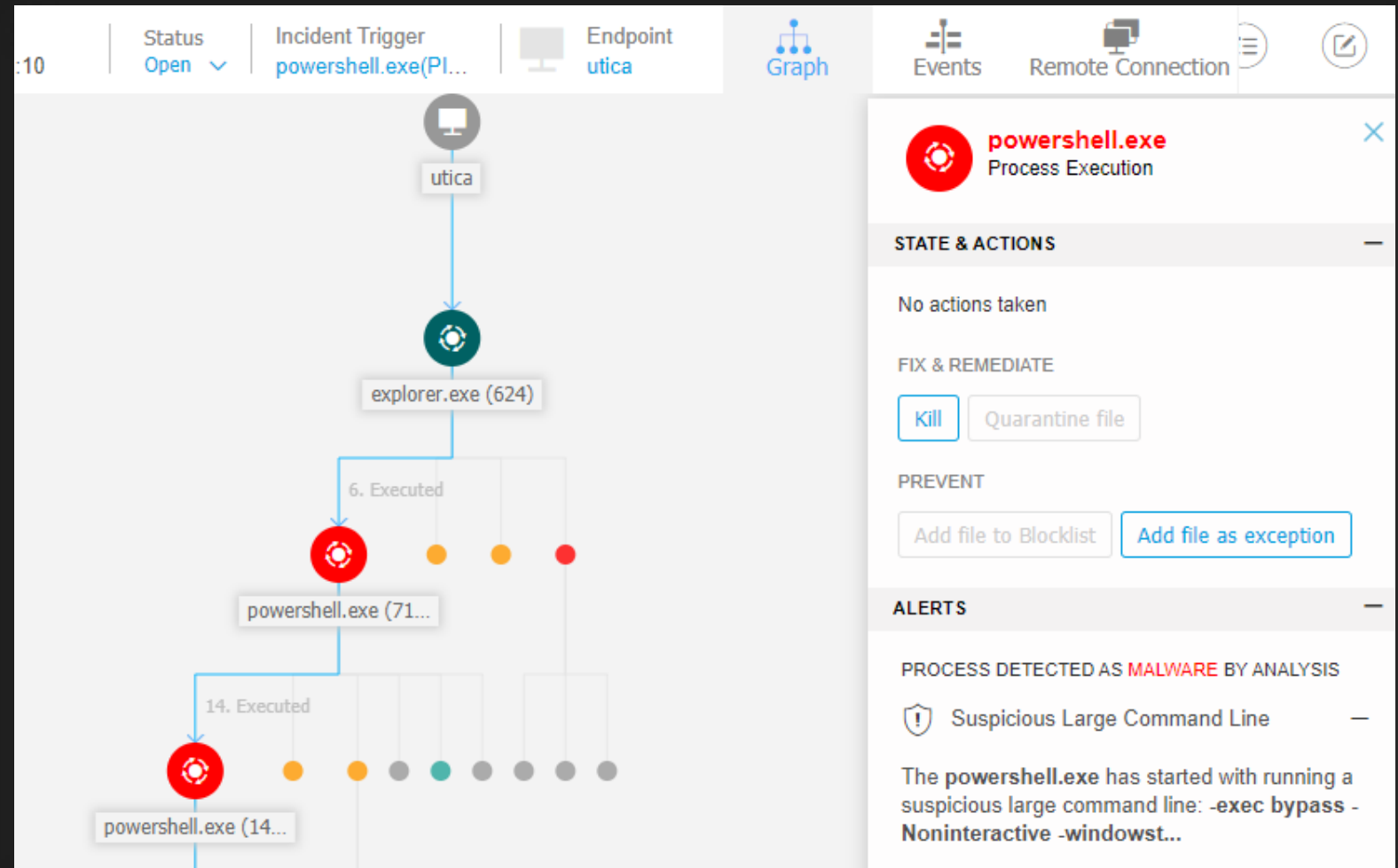
EDR sensor recording raw data from endpoints, data that is correlated with information from the other security layers. It provides visibility on all suspicious activities, automatically creating incidents for security teams to further analyze.

# EDR WORKFLOW AND VISUALIZATION

Advanced detection and response shows precisely how a potential threat works and its context in your environment.

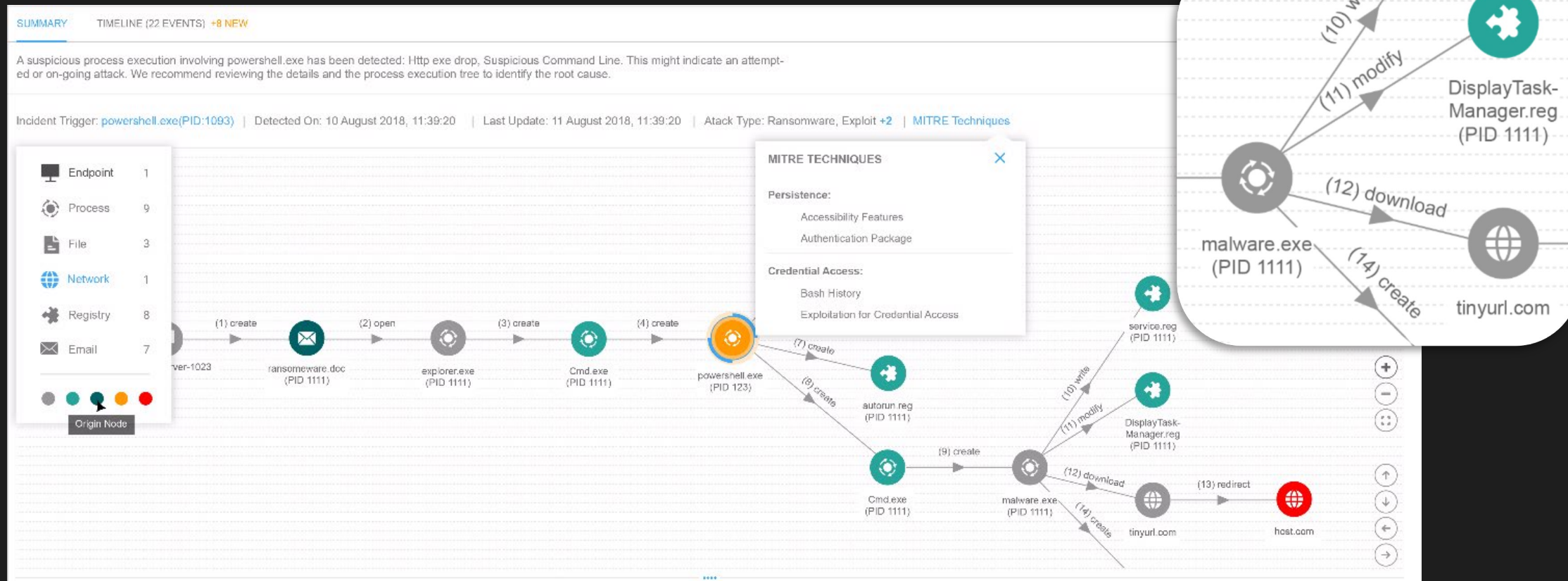
MITRE attack techniques and indicators of compromise provide up to the minute insight into named threats and other malware that may be involved.

Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff.



# PRE AND POST COMPROMISE ATTACK FORENSICS

## Root Cause Analysis



The end-to-end attack forensics provides visibility into past actions covering the lifecycle of an attack (before, during and after). It covers both blocked attacks and suspicious activities.

# EDR SENSOR

## POLICIES

Allows you to enable or disable the EDR Sensor

Bitdefender  
GravityZone

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Accounts

User Activity

General

Antimalware

Sandbox Analyzer

Firewall

Content Control

Device Control

Relay

Exchange Protection

Encryption

EDR Sensor

General

☒ EDR Sensor

Continuously monitors endpoint activity such as running processes, network connections or registry changes. This metadata is collected, reported and processed by Security Analytics servers. At this stage, learning algorithms detect suspicious files and processes running on the system, generating notifications from these incidents.

EDR SENSOR

PROTECTED ENDPOINTS

SECURITY ANALYZER

INCIDENTS

EVENTS

# INCIDENTS

## BLOCKLIST

GravityZone Ultra integrates layered next-gen endpoint protection and easy-to-use EDR platform to protect against even the most elusive cyber threats. It offers:

- Prevention
- Automated detection
- Investigation and response tools

Bitdefender  
GravityZone

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Blocklist

−

Delete

↺

Refresh

	Type	File Hash	Source Type	Source Info
<input type="checkbox"/>	<div></div>	<div></div>	<div></div>	<div></div>



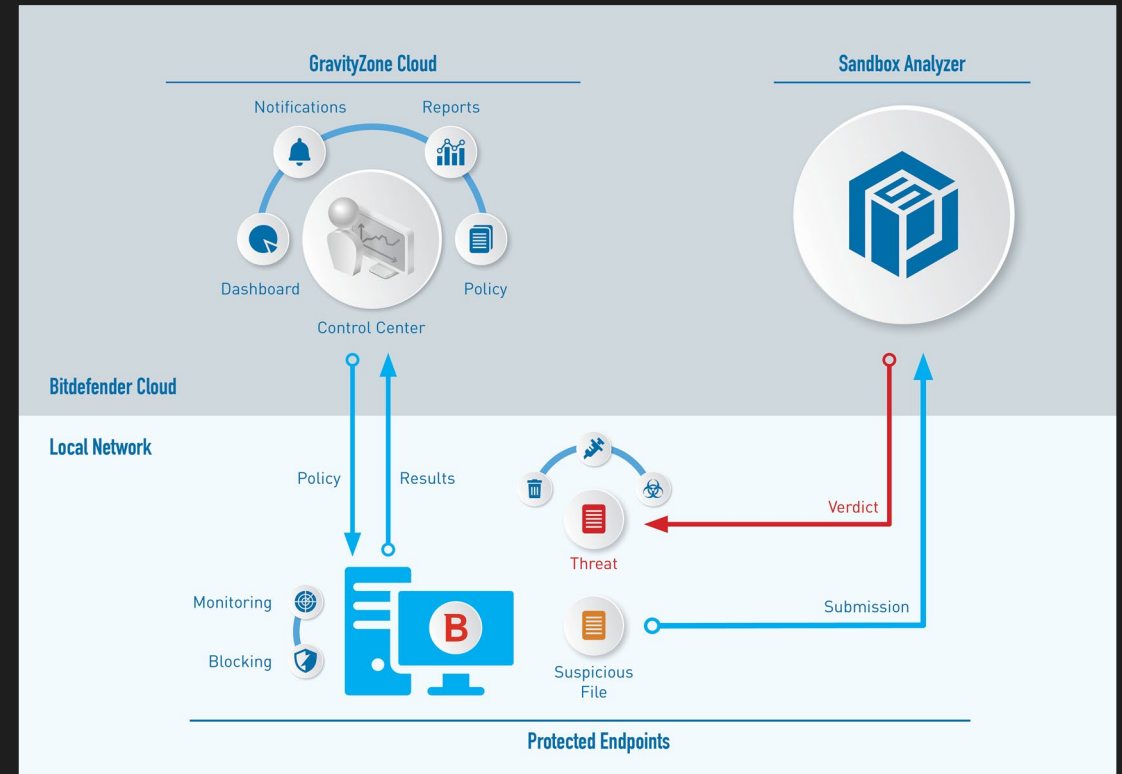
# SANDBOX ANALYZER



# SANDBOX ANALYZER

## CLOUD

- Provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed by Bitdefender antimalware engines.
- Uses machine learning and behavioral analysis to assess suspicious files
- Runs in blocking or monitoring mode
- Provides a verdict in near-real-time and takes policy-based remediation action
- Delivers in-depth reporting on malware behavior

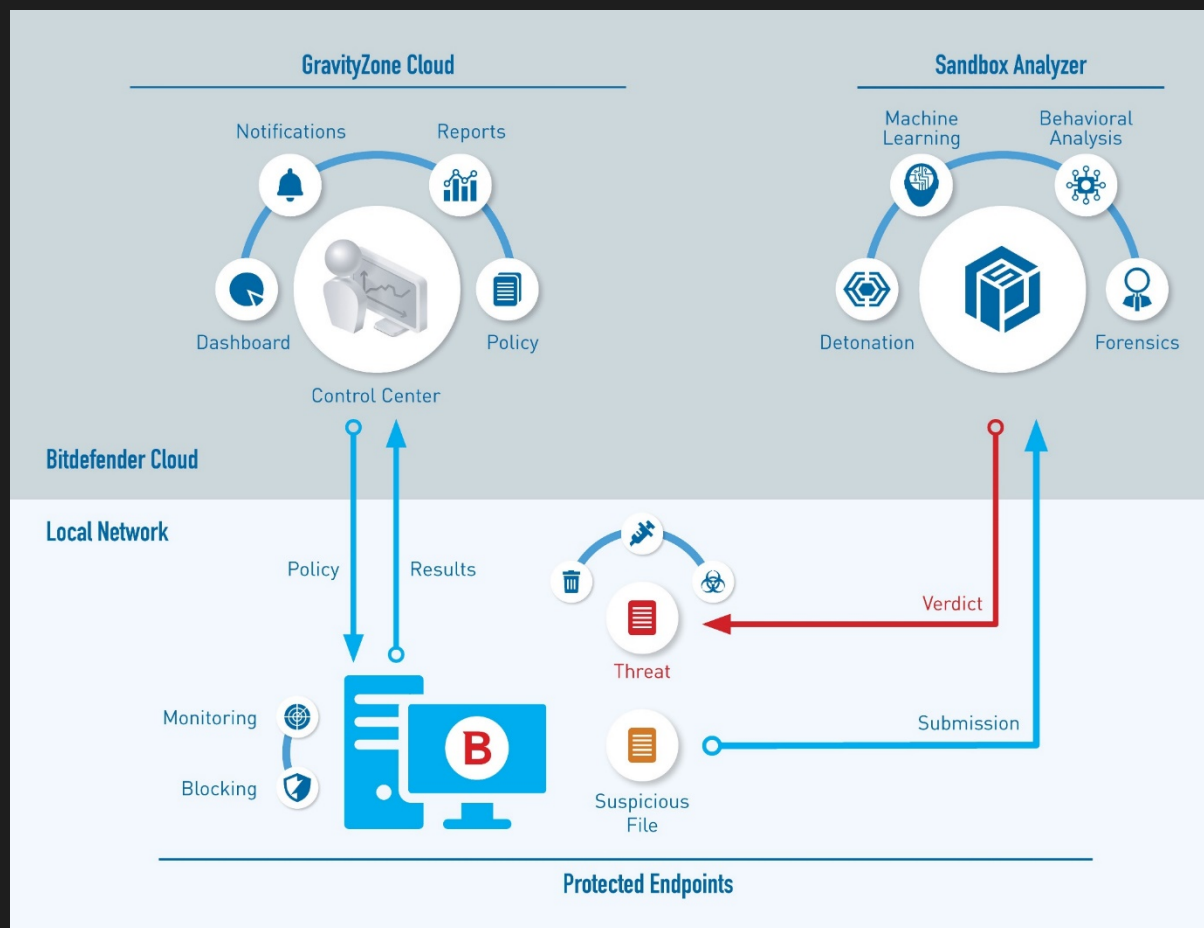


# SANDBOX ANALYZER

## CLOUD

Protects against:

- Advanced targeted attacks
- Custom malware
- Unknown packers



- Uses machine learning and behavioral analysis to assess suspicious files
- Runs in blocking or monitoring mode
- Provides a verdict in near-real-time and takes policy-based remediation action
- Delivers in-depth reporting on malware behavior

# SANDBOX ANALYZER

## ON-PREMISE

- Software virtual appliance designed to provide real-time behavioral analysis of potentially malicious code
- Network Sensor Virtual appliance, which is deployable in a virtualized environment that scans, extracts, and sends content for detonation based on the network traffic
- Automatic submission from Centralized Quarantine
  - Quarantined samples are automatically submitted to Sandbox
- Programmatic interaction with Sandbox
  - Sandbox APIs are now available
  - Methods for: environment discovery, sample submission, report retrieval
  - Documented examples: python, C#, curl requests, NodeJS

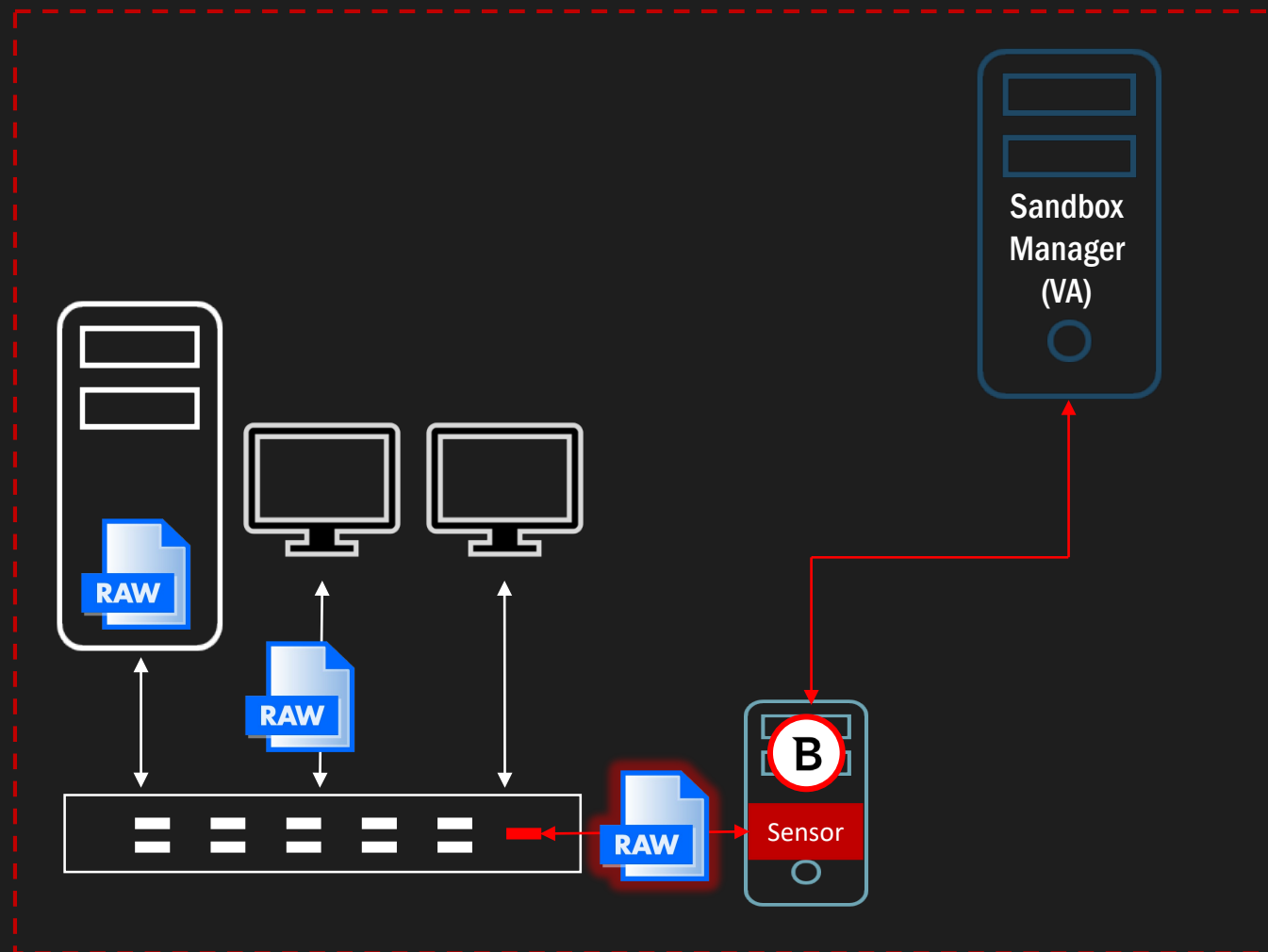


# SANDBOX ANALYZER

## ON-PREMISE (CONTINUED)

### Network Sensor – NSVA

- Virtual appliance deployable in a virtualized environment (ESXi) that scans, extracts and sends content for detonation to a Sandbox Analyzer
- Network capture NIC is connected to switch SPAN port
- Extracts files from network traffic streams and automatically submits to Sandbox Analyzer
- Supports HTTP, FTP, SMTP, SMB



# NETWORK ATTACK DEFENSE



# NETWORK ATTACK DEFENSE

## BENEFITS

New level of protection against attackers seeking access to the system by exploiting network vulnerabilities. It contributes to extend protected areas, now with network based security that blocks threats such as:

- Brute Force attacks
- Password Stealers
- Network Exploits
- Lateral movements before they can execute

# NETWORK ATTACK DEFENSE INSTALLATION

Bitdefender  
GravityZone

Dashboard

Incidents

Blocklist

Search

Network

Patch Inventory

Packages

Tasks

Risk Management

Policies

Assignment Rules

Reports

Quarantine

Companies

Accounts

User Activity

Sandbox Analyzer

Manual Submission

Back

Reconfigure Client

Choose the protection modules and roles you want on the target endpoints. You can add new modules besides the existing ones, remove certain modules, or match the existing configuration.

Modules

Add

Remove

Match List

Modules:

☒ Antimalware

☐ Advanced Threat Control

☐ Advanced Anti-Exploit

☐ Firewall

☒ Network Protection

☐ Content Control

☒ Network Attack Defense

☐ Device Control

☐ Power User

☐ Patch Management

☐ EDR Sensor

Roles:

☐ Exchange Protection

☐ Relay

Save

Cancel

All targeted clients will be reconfigured according to the selected settings.

New Endpoint Package

General

Name: \*

Description:

Language: English

Company: Choose company

Modules:

☒ Antimalware

☒ Advanced Threat Control

☒ Advanced Anti-Exploit

☒ Firewall

☒ Network Protection

☒ Content Control

☒ Network Attack Defense

☒ Device Control

☐ Power User

☐ Patch Management

☒ EDR Sensor

☐ Exchange Protection

Roles:

☐ Exchange Protection

Save

Cancel



# NETWORK ATTACK DEFENSE

## CONFIGURATION

☰

Bitdefender  
GravityZone

Welcome, Partner

?

Dashboard

Incidents

Blocklist

Search

Network

Patch Inventory

Packages

Tasks

Risk Management

Policies

Assignment Rules

Reports

⚙️ General +

🛡️ Antimalware +

🏠 Sandbox Analyzer +

🔒 Firewall +

🌐 Network Protection -

General

Content Control

Web Protection

Network Attacks

🔧 Patch Management

🖥️ Device Control +

☒ Network Attack Defense

This feature is a security layer designed to detect network attack techniques that try to gain access on specific endpoints. It can be customized to suit your organization's security requirements.

Attack Techniques

<input checked="" type="checkbox"/>	Initial Access	Block ▾
<input checked="" type="checkbox"/>	Credential Access	Block ▾
<input checked="" type="checkbox"/>	Discovery	Block ▾
<input checked="" type="checkbox"/>	Lateral Movement	Block ▾
<input checked="" type="checkbox"/>	Crimeware	Block ▾

Reset to Default

# ADD-ON FEATURES



# INTEGRATED PATCH MANAGEMENT ADD-ON

- Helps improve security posture by expediently discovering and eliminating vulnerabilities
- Provides the widest range of security- and non-security patches for operating systems, third-party applications and golden images
- Covers Windows-based physical, virtual on-prem and cloud-based endpoints and servers
- Is deployed and managed from the GravityZone console and integrated into its agent

The screenshot shows the Bitdefender GravityZone web console interface. The left sidebar contains navigation links: Dashboard, Network, Patch Inventory, Packages, Tasks, Policies (highlighted), Assignment Rules, Reports, Quarantine, Accounts, and User Activity. Under Policies, a sub-menu lists General, Antimalware, Firewall, Content Control, Patch Management (selected), Device Control, Relay, and Exchange Protection. The main content area is titled 'Patch Download Settings' and includes a dropdown for 'Enter a Relay with Patch Caching Server' with a '+' icon. Below this is a table with columns 'Priority', 'Relay', and 'Action'. Further down, there are three checked checkboxes: 'Use vendor websites as fallback location to download patches', 'Automatic patch scan', and 'Install patches automatically after scan'. The 'Automatic patch scan' section shows a recurrence of 'Daily' at '21:00'. A warning message states: 'Warning: A patch installed for one product may also affect others'. Below the warning, 'Update status' is set to 'Security' with a dropdown set to 'Immediately'. 'Non-security' is set to 'Weekly' on 'Thu' at '21:00'. There is an unchecked checkbox for 'Specific vendor and product'. At the bottom, there are 'Save' and 'Cancel' buttons.

Bitdefender GravityZone

Dashboard

Network

Patch Inventory

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Accounts

User Activity

General

Antimalware

Firewall

Content Control

Patch Management

Device Control

Relay

Exchange Protection

Patch Download Settings

Enter a Relay with Patch Caching Server

Priority	Relay	Action
----------	-------	--------

☒ Use vendor websites as fallback location to download patches

☒ Automatic patch scan

Recurrence:

Daily at 21:00

☒ Install patches automatically after scan

**Warning**

A patch installed for one product may also affect others

Update status:

☒ Security Immediately

☒ Non-security Weekly on Thu at 21:00

☐ Specific vendor and product

Vendor Products

Vendor Products

Save Cancel



# FULL-DISK ENCRYPTION ADD-ON

- Leverages native Windows BitLocker and Mac OS FileVault encryption to ensure compatibility and performance
- Is fully integrated into the GravityZone Control Center for centralized deployment, management and key recovery
- Requires no additional agent to deploy or key management server to install
- Delivers encryption-specific reports to help prove compliance
- Supports pre-boot authentication enforcement

# GRAVITYZONE SECURITY FOR STORAGE

- Unmatched real-time protection
  - On-access scanning with configurable automatic actions and exclusions
  - Customizable reporting and real-time notifications
- Efficient management via GravityZone on-premises or cloud console
- Broad compatibility
  - Citrix ® ShareFile, Nutanix ® Files™ (AFS), and ICAP-compliant NAS (Dell ® Compellent™, EMC® Isilon, Hitachi® HNAS, HPE® 3PAR StoreServ, IBM® Storwize, etc.
- Unlimited scalability
- High availability and resilience



# EMAIL SECURITY

## BENEFITS

- Unique multi-engine technology platform

Highly accurate message categorization and threat protection

- Combination of email security and full mail routing engine

Easy to manage, allows for custom email delivery based on:

30 conditions (including direction, sender/recipient, AD attributes, subject, body, headers, attachment size, etc)

25 actions (including accept, reject, re-route, add content to subject/body/headers, quarantine, modify spam score)

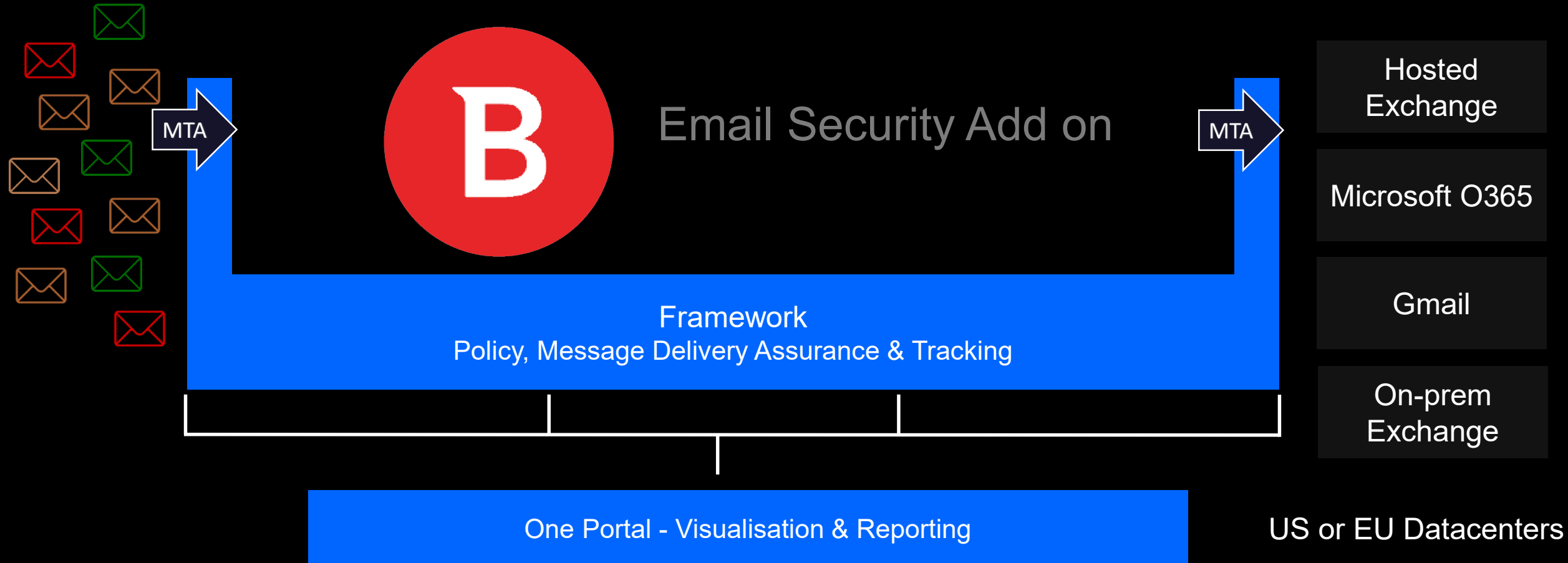
- Flexible deployment, cloud scalable

Accommodates virtually any deployment scenarios

Adapts to any amount of mail due to elastic cloud architecture



# EMAIL SECURITY ARCHITECTURE



# NETWORK TRAFFIC SECURITY ANALYTICS (NTSA)





# NTSA

## OVERVIEW

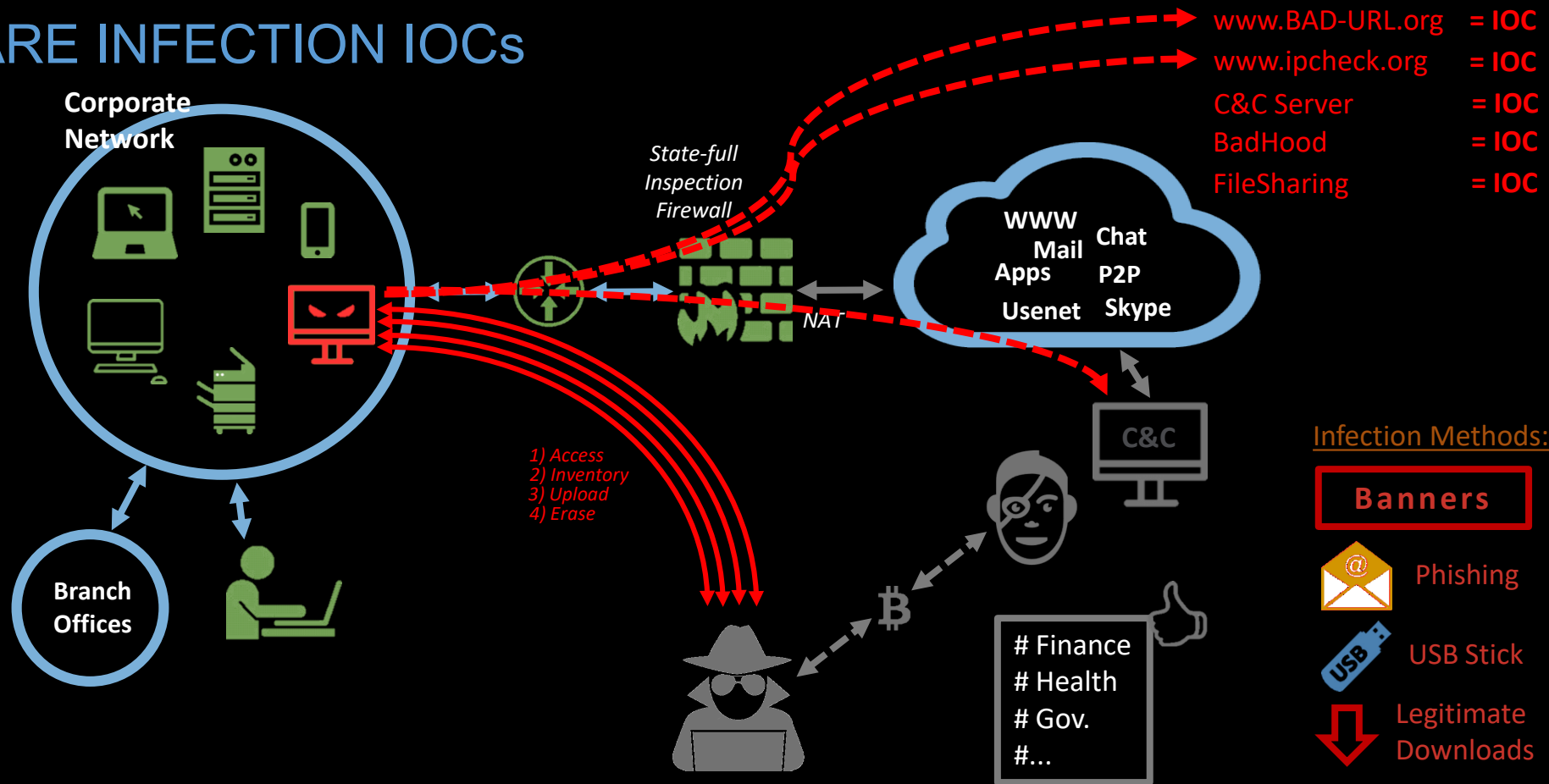


Unique concept for detecting and reporting malware:

- agentless that monitors the behavior of all IoT devices on your network
- essential network traffic security analyzer and breach detector
- focuses solely on monitoring outbound traffic to detect malicious behavior
  - ➔ focuses on the outbound communication characteristics of malware that has installed itself on your devices and networks
  - ➔ instantly detects advanced persistent threats
- provides accurate visibility into advanced or targeted attacks and malware that has slipped through your security defense
- detects what traditional security technologies (Firewalls, Sandbox, IPS/IDS etc.) miss
- Plug-and-Play non intrusive solution

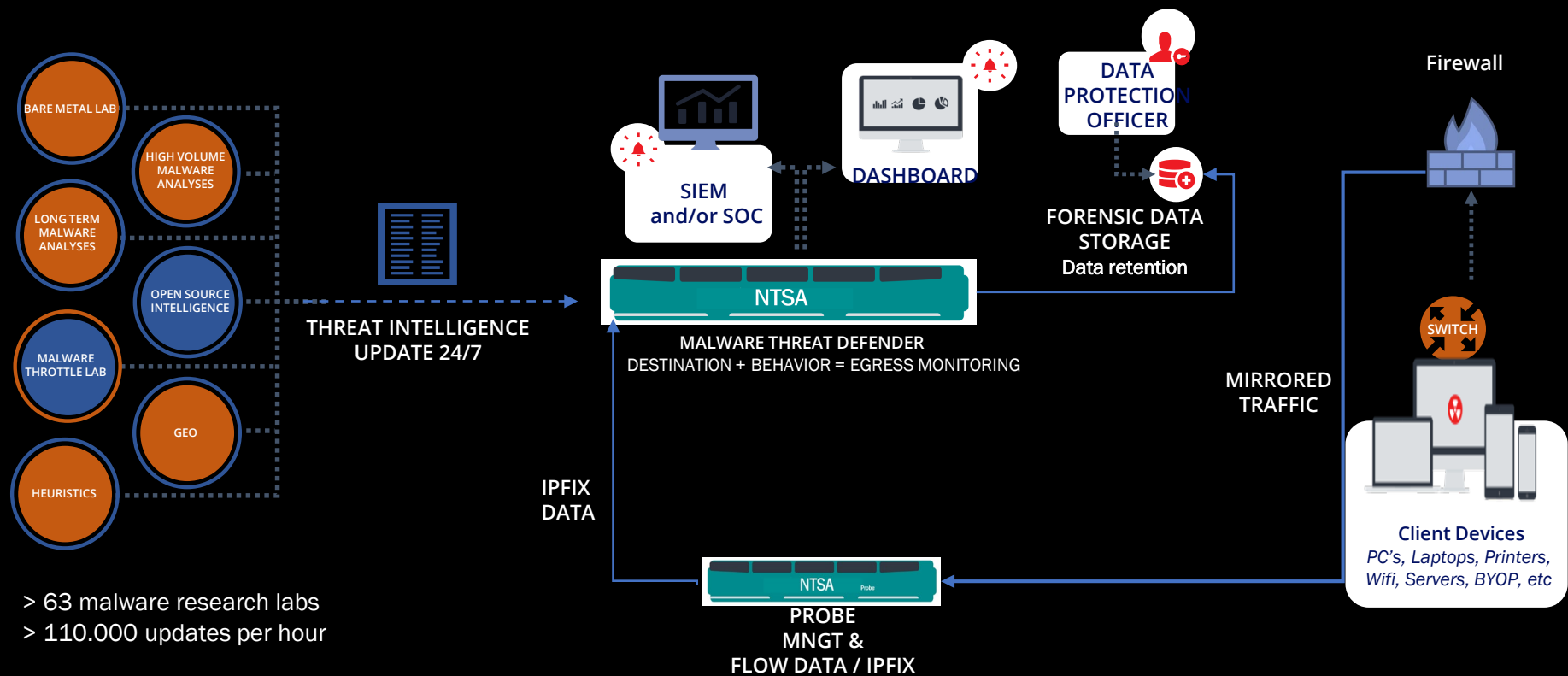
# NTSA

## MALWARE INFECTION IOCs



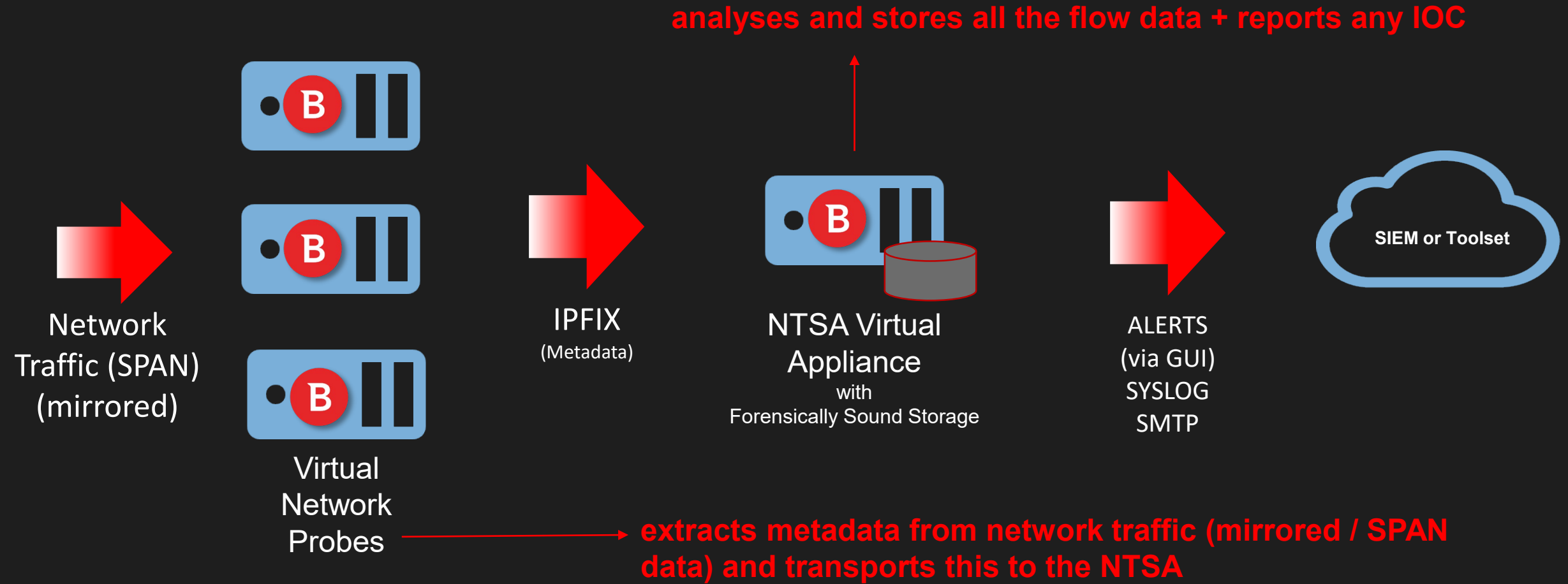
# NTSA

## ARCHITECTURE

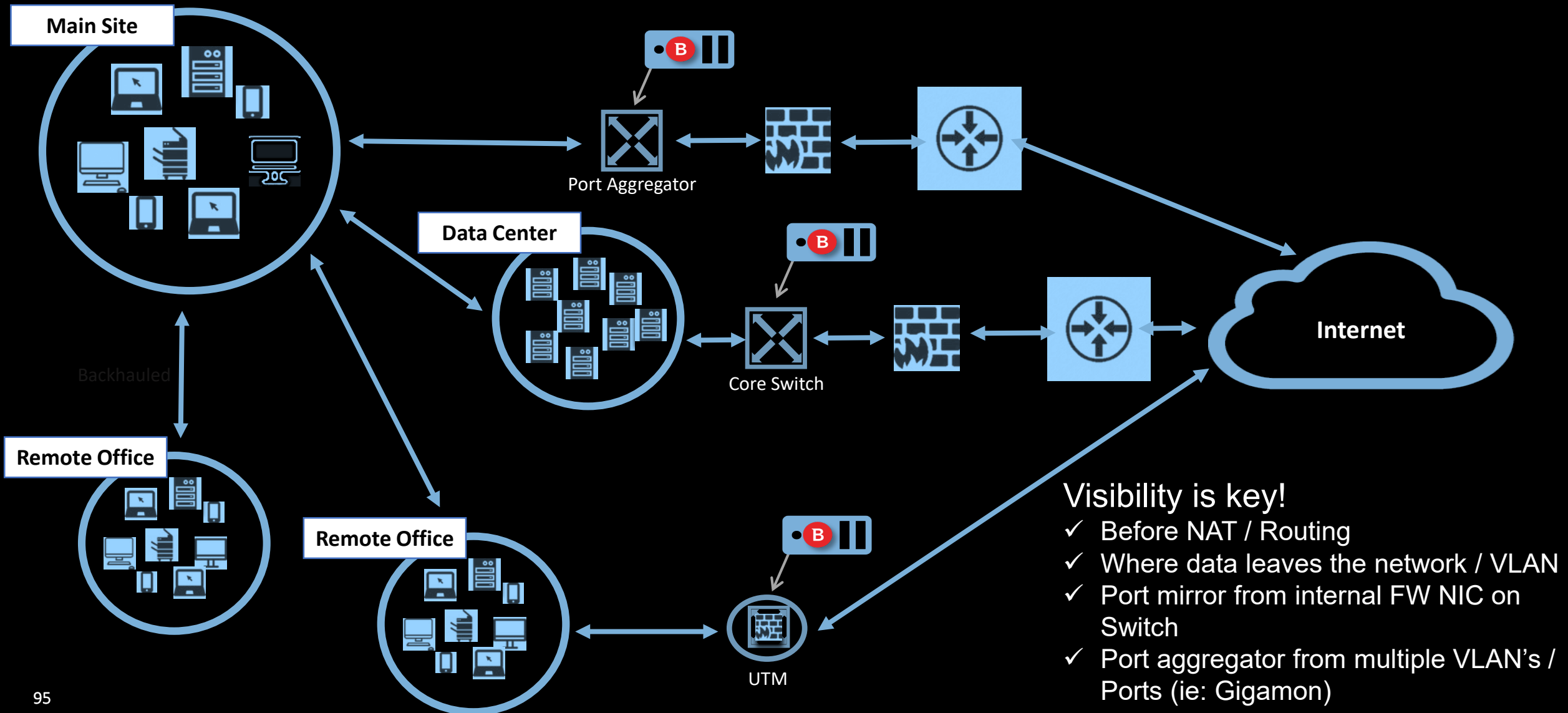


# NTSA

## COMPONENTS



# Strategic Probe Placement



# SECURITY FOR MOBILE DEVICES (MDM)

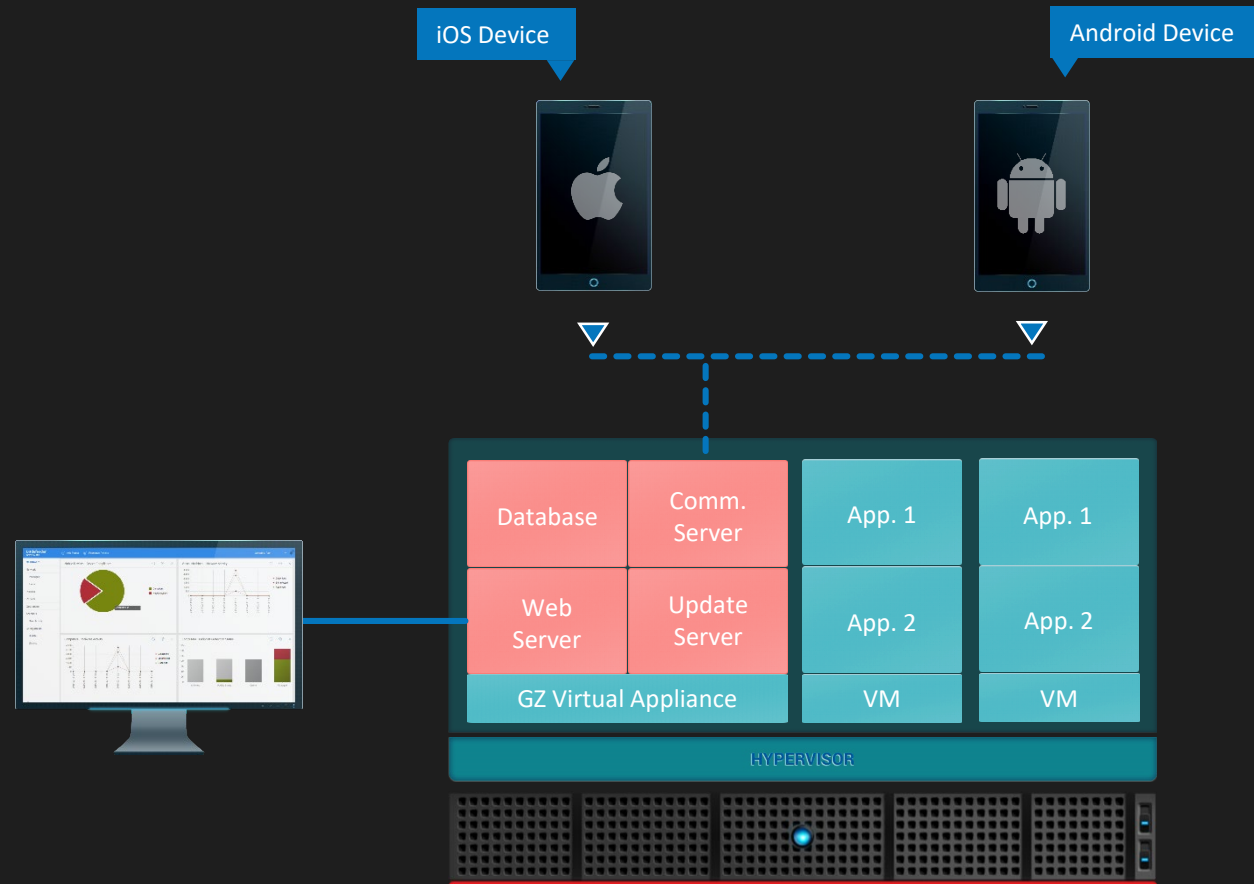


# SECURITY FOR MOBILE DEVICES

## COMPONENTS

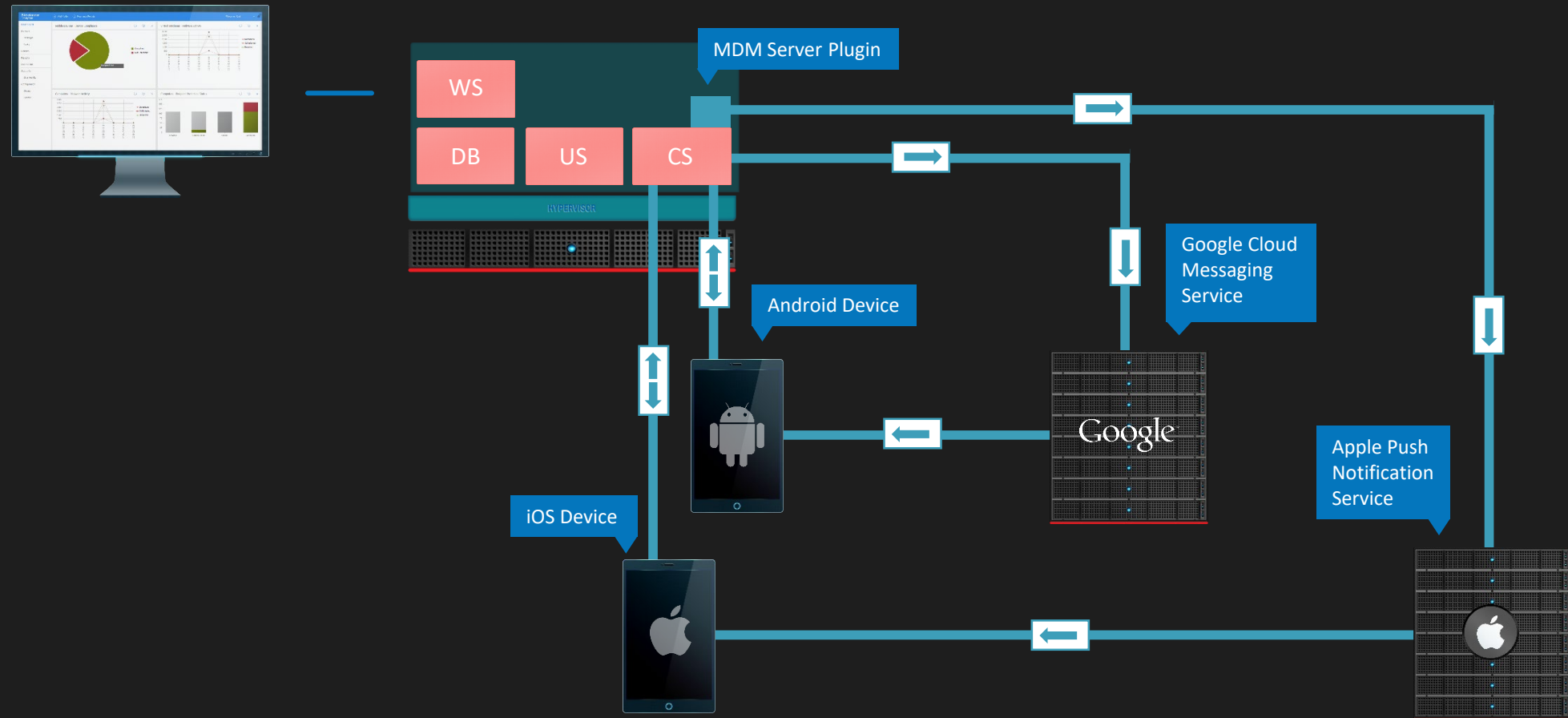
**GravityZone Mobile Client for Android**

**GravityZone Mobile Client for iOS**



# SECURITY FOR MOBILE DEVICES

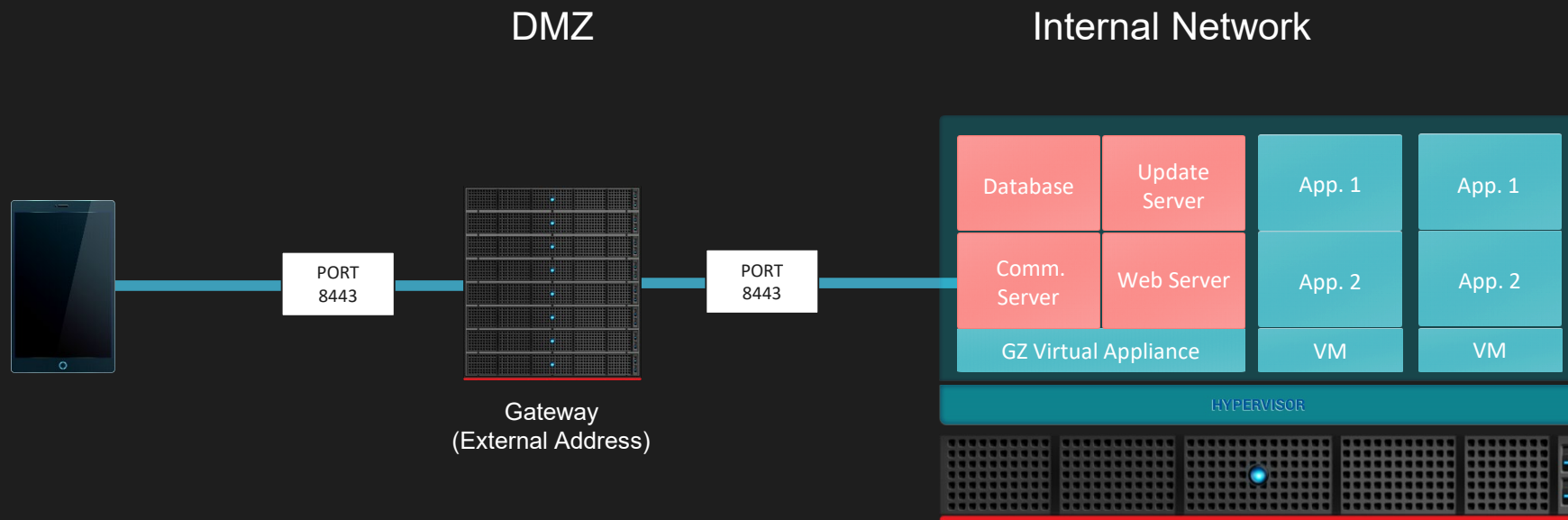
## COMMUNICATION WORKFLOW





# SECURITY FOR MOBILE DEVICES

## MDM COMMUNICATION SERVER



# SECURITY FOR MOBILE DEVICES

## MOBILE DEVICE MANAGEMENT

Unifies enterprise-wide security with management and compliance control of iPhone, iPad and Android.

Security features include:

- screen lock
- authentication control
- device location
- remote wipe
- detection of rooted or jailbroken devices
- security profiles.

On Android devices the security level is enhanced with **real-time scanning** and **removable media encryption**.



# GRAVITYZONE PRODUCT BUNDLES AND OPTIONS

Components	Business Security	Advanced Business Security	Elite	Ultra	Enterprise
Console-Delivery Options	On-Premises / Cloud	On-Premises / Cloud	On-Premises / Cloud	Cloud	On-Premises
Coverage					
Endpoint Security	Yes	Yes	Endpoint Security HD	Endpoint Security XDR	Yes
Mobile Security		On-Premises	On-Premises		Yes
Security for Virtualized Environments	Yes	Yes	Yes	Yes	Per-CPU / VS / VDI Licensing
Security for Exchange		Yes	Yes	Yes	Yes
Hypervisor Introspection (HVI)			Per-CPU Licensing (On-Prem)		Per-CPU Licensing
Security Technologies					
Machine Learning	Yes	Yes	Yes	Yes	Yes
Advanced Anti-Exploit	Yes	Yes	Yes	Yes	Yes
Sandbox Analyzer			Yes	Yes	
HyperDetect (Tunable ML)			Yes	Yes	
Process Inspector (ATC)	Yes	Yes	Yes	Yes	Yes
Network Attack Defense	Yes	Yes	Yes	Yes	Yes
Central Scanning (Offloaded to an SVA)		Yes	Yes	Yes	Yes
Visibility into Suspicious Activities			Yes	Yes	Report Builder
Application Control	Blacklisting	Blacklisting	Blacklisting Whitelisting (On-Prem)	Blacklisting	Blacklisting Whitelisting
EDR				Yes	
Add-Ons					
Full-Disk Encryption (Add-on)	Yes	Yes	Yes	Yes	Yes
Patch Management (Add-on)	Yes	Yes	Yes	Yes	Yes
Licensing					
License Type and Term Restrictions	Bundle, Yearly License Up to 30% of Devices Can Be Servers	Bundle, Yearly License Up to 35% of Devices Can Be Servers	Bundle, Yearly License Up to 35% of Devices Can Be Servers	Bundle, Yearly License Up to 35% of Devices Can Be Servers	A la Carte, Annual Licensing

# Q&A





# THANK YOU

