

# Bitdefender Certification Day

## 18 giugno 2021

**Roberto Novasconi - Avangate Italia**  
*Senior Support and Training Specialist*

**Stefano Maranzana - Bitdefender**  
*Sales Engineer*

**Giovanni D'Amato - Bitdefender**  
*Sales Engineer*

### Agenda

- 10:00 - 10:15 Benvenuto
- 10:15 - 12:00 GravityZone Corso
- 12:00 - 12:15 Pausa
- 12:15 - 13:00 DEMO interattiva
- 14:00 - 14:30 DEMO interattiva
- 14:30 Test Certificazione

# Bitdefender eLearning

[\*https://elearning.bitdefender.com/\*](https://elearning.bitdefender.com/)

Effettuare login con il proprio account personale.

Se non ne disponete fatecelo sapere subito,  
indicandoci Nome e cognome, email, azienda



ENDPOINT • NETWORK • CLOUD

# BITDEFENDER GRAVITYZONE

Bitdefender®

[WWW.BITDEFENDER.COM](http://WWW.BITDEFENDER.COM)



# COURSE CONTENTS

1. Overview
2. GravityZone Control Center
3. Unified Next-Gen Endpoint Security Client
4. Security for Virtualized Environments
5. Hypervisor Introspection
6. Security for Mobile Devices
7. Security for Storage
8. Sandbox Analyzer On-Premise
9. Security for Exchange
10. Email Security Cloud
11. Summary

GRAVITYZONE™  
THE SECURITY PLATFORM FOR  
END-TO-END BREACH AVOIDANCE

# BITDEFENDER GRAVITYZONE®

**THE ENTERPRISE SECURITY PLATFORM  
FOR THE BEST BREACH AVOIDANCE**

Unified Prevention, Detection, Response and  
Hardening Across Endpoint, Network and  
Cloud

5 Bitdefender®

LAPTOPS AND  
WORKSTATIONS



MOBILE  
DEVICES



VIRTUAL  
DESKTOPS  
VDI / DAAS



SERVERS



SOFTWARE-DEFINED &  
HYPERCONVERGED  
INFRASTRUCTURE



PUBLIC, PRIVATE &  
HYBRID CLOUD



STORAGE  
ICAP Compatible



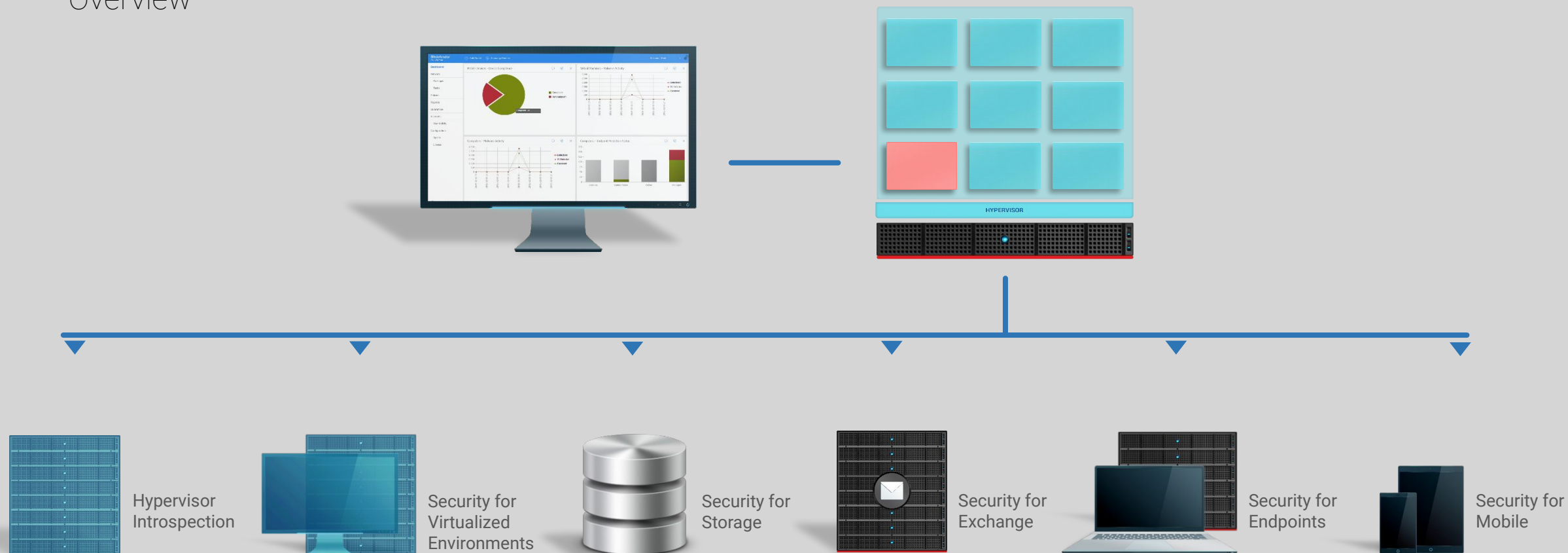
EMAIL  
Hosted or On-prem



Bitdefender®  
GRAVITYZONE

# GRAVITYZONE ON-PREMISE

## Overview



# GRAVITYZONE CLOUD

## Overview



# GRAVITYZONE

## ON-PREMISE vs CLOUD

FEATURE / SECURITY TECHNOLOGY	GravityZone	
	ON-PREMISE	CLOUD
<b>MANAGEMENT &amp; INTEGRATION</b>		
▼ Multi Tenancy		✓
▼ Active Directory Integration	✓	✓
▼ vCenter Server Integration	✓	
▼ Xen Server Integration	✓	
▼ Nutanix Prism Integration	✓	
▼ AWS Integration	✓	✓
▼ Azure Integration	✓	
<b>DETECTION AND RESPONSE MODULES</b>		
▼ Search Queries		✓
▼ Ransomware Mitigation	✓	✓
<b>HARDENING AND RISK ANALYTICS MODULES</b>		
▼ Endpoint Risk Analytics (ERA)		✓
▼ Application Control (Blacklisting)	✓	✓
▼ Application Control (Whitelisting)	✓	
<b>SECURITY SERVICES / ADD-ONS</b>		
▼ Security for Mobile Devices	✓	
▼ Hypervisor Introspection	✓	
▼ Email Security		✓
<b>SERVICES</b>		
▼ MDR		✓





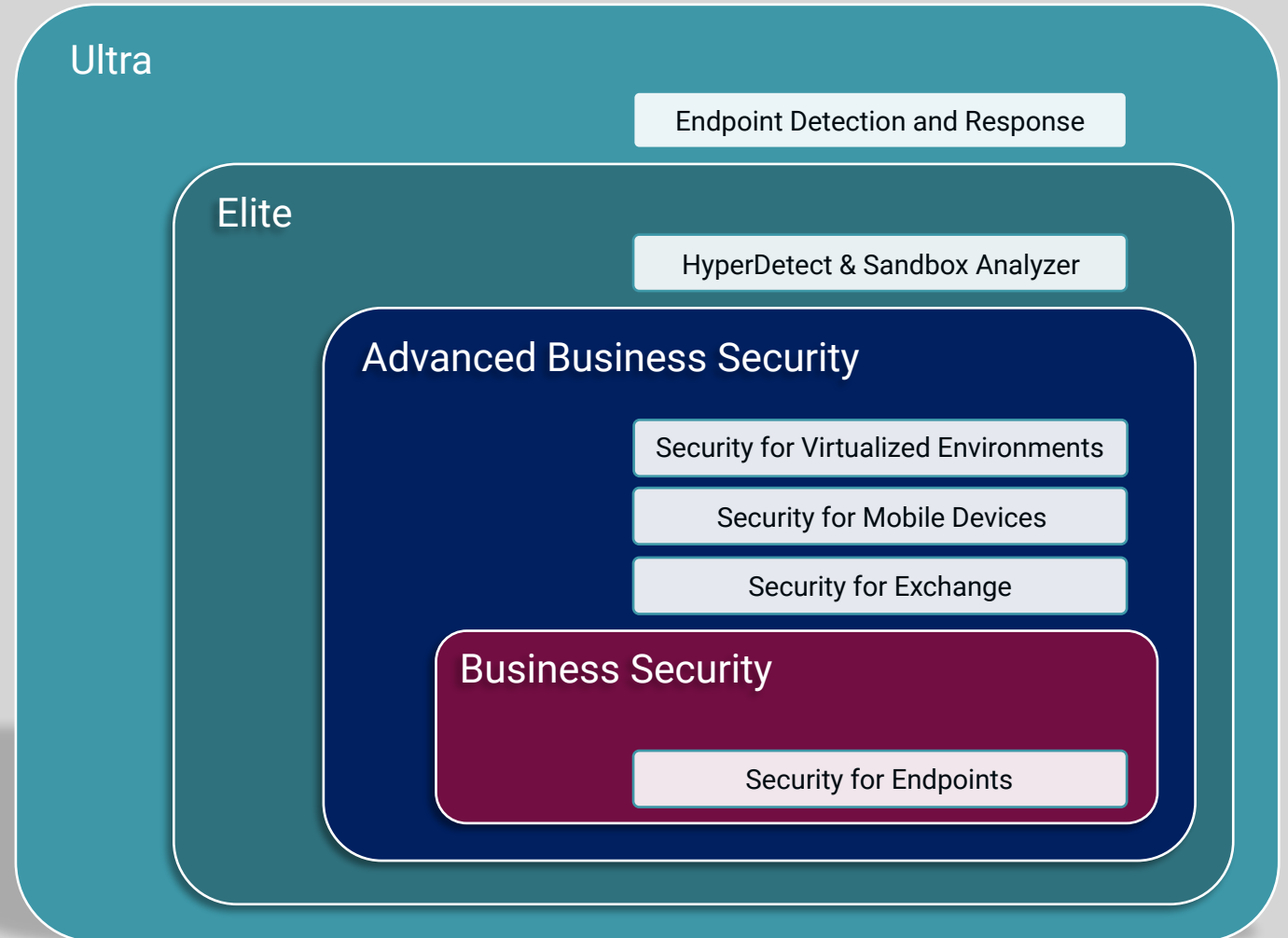
#### Add-ons for Bundles:

- Patch Management
- Full Disk Encryption
- Security for Storage
- Email Security (cloud)

#### Add-ons for Enterprise licensing:

- Patch Management
- Sandbox Analyzer (on-premise)
- Full Disk Encryption
- Security for Storage
- HVI (on-premise)
- Enterprise Elite Add-on for à-la-carte licensing
- Ultra Add-on for à-la-carte licensing

# AVAILABLE BUNDLES

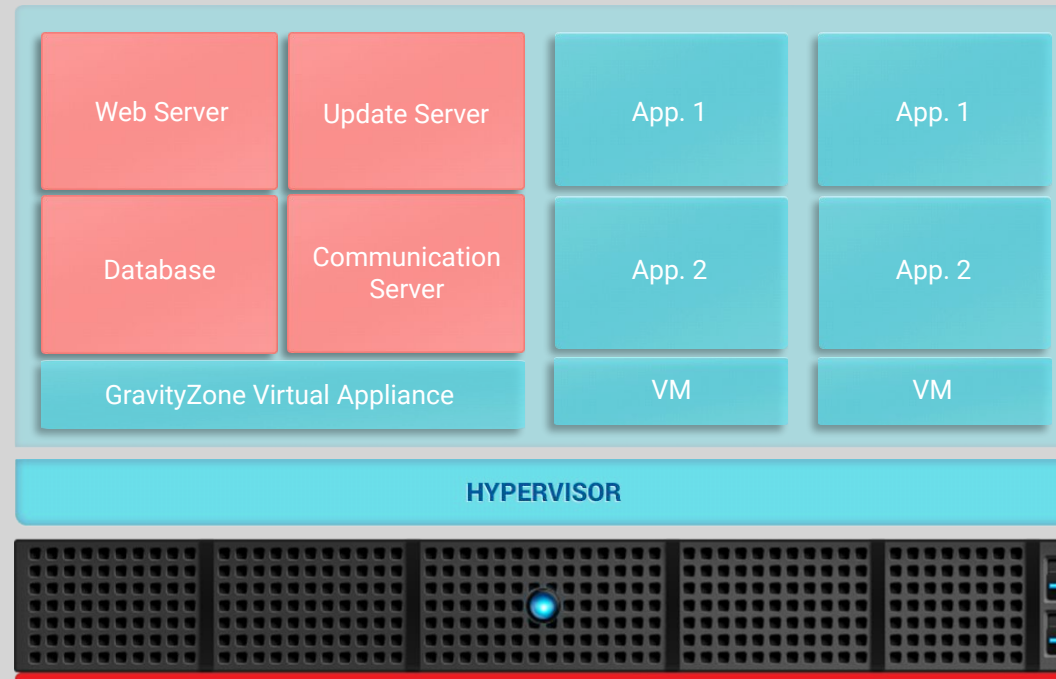


# GRAVITYZONE CONTROL CENTER

The Management Component

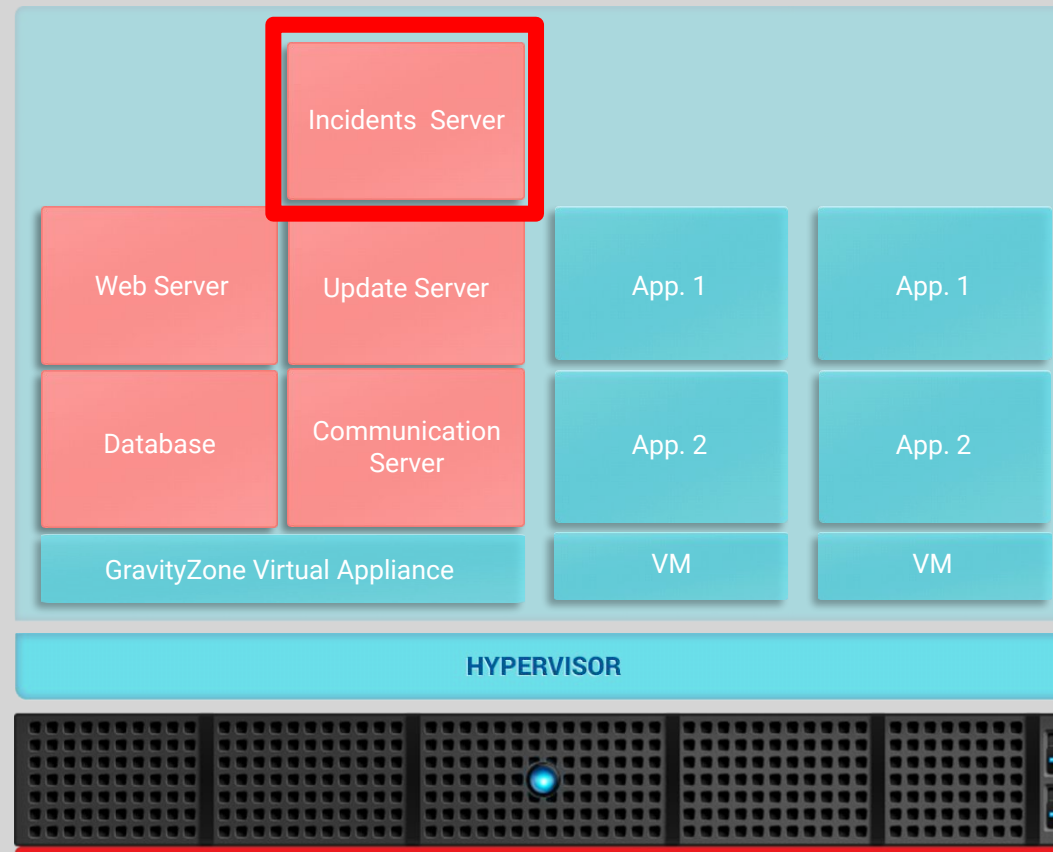
# Control Center

**All-in-One** Deployment - **up to 4000 endpoints**



# Control Center

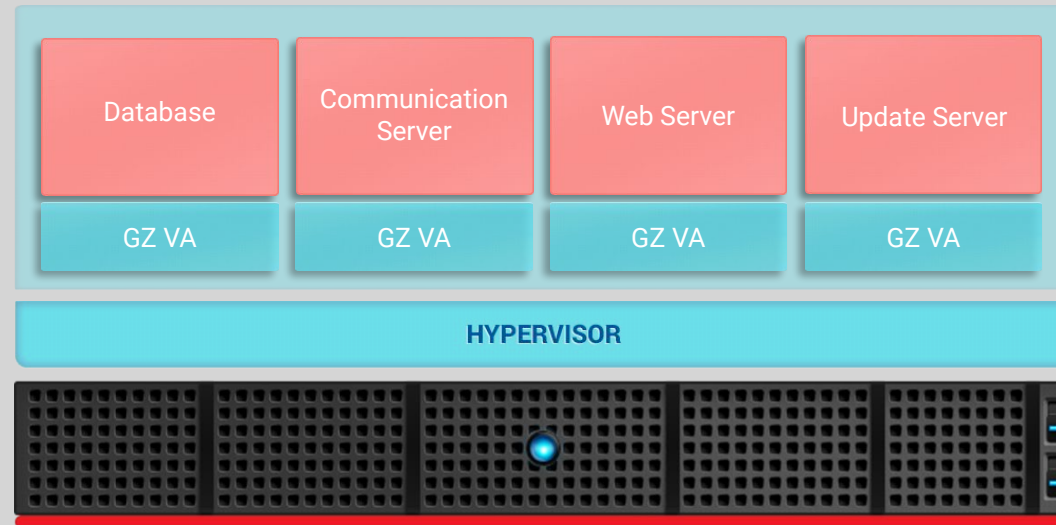
**All-in-One** Deployment **with** Incidents Server (**EDR**)





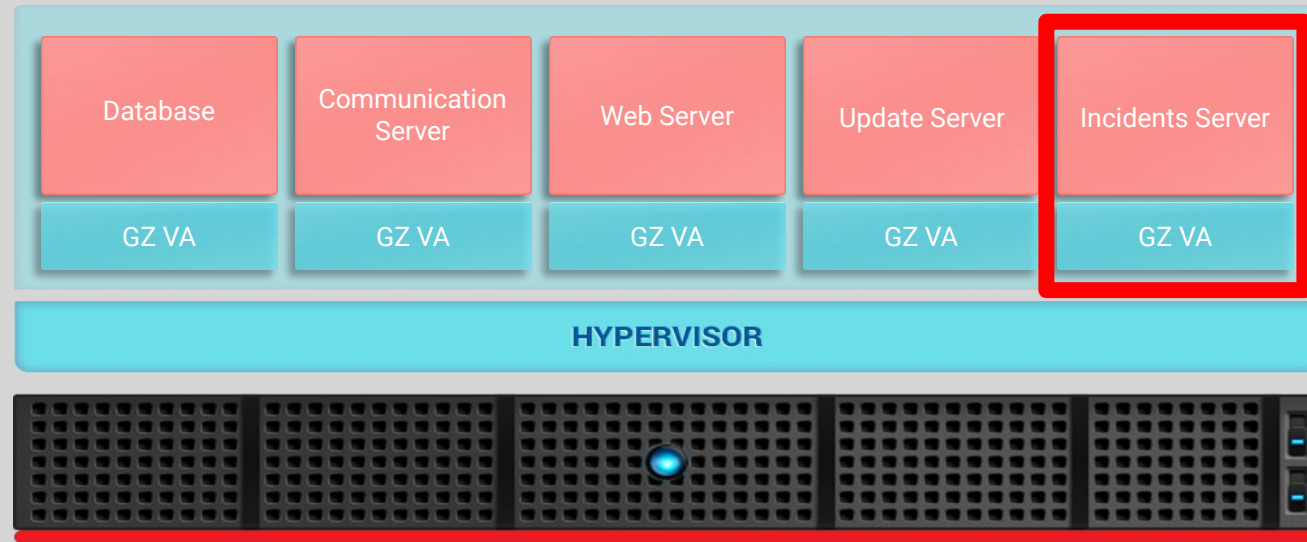
# Control Center

**Cluster** Deployment - **up to 10000 endpoints**



# Control Center

**Cluster Deployment with** Incidents Server (**EDR**)



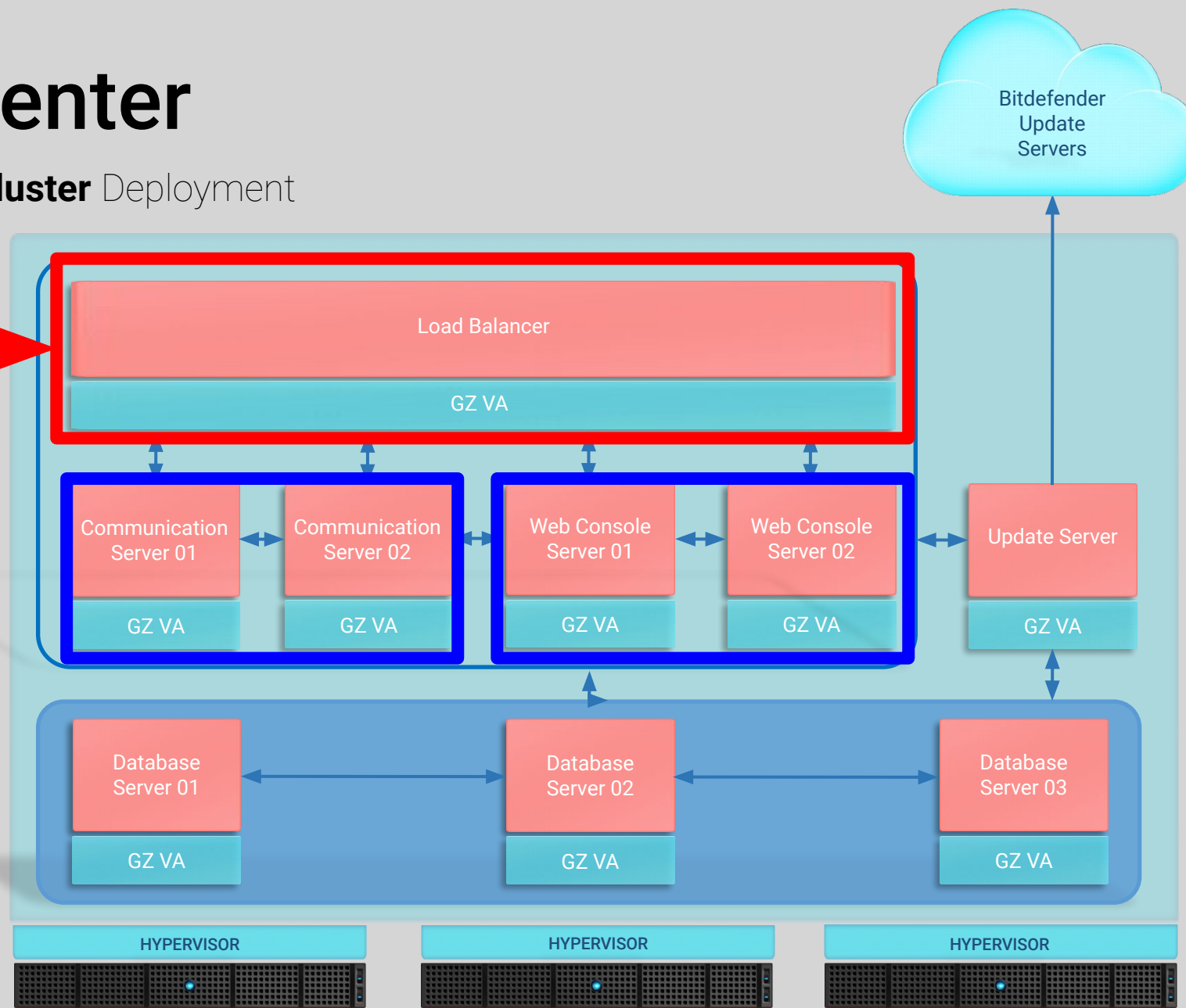
# Control Center

## Load Balanced HA Cluster Deployment

VA dedicata  
LoadBalancer

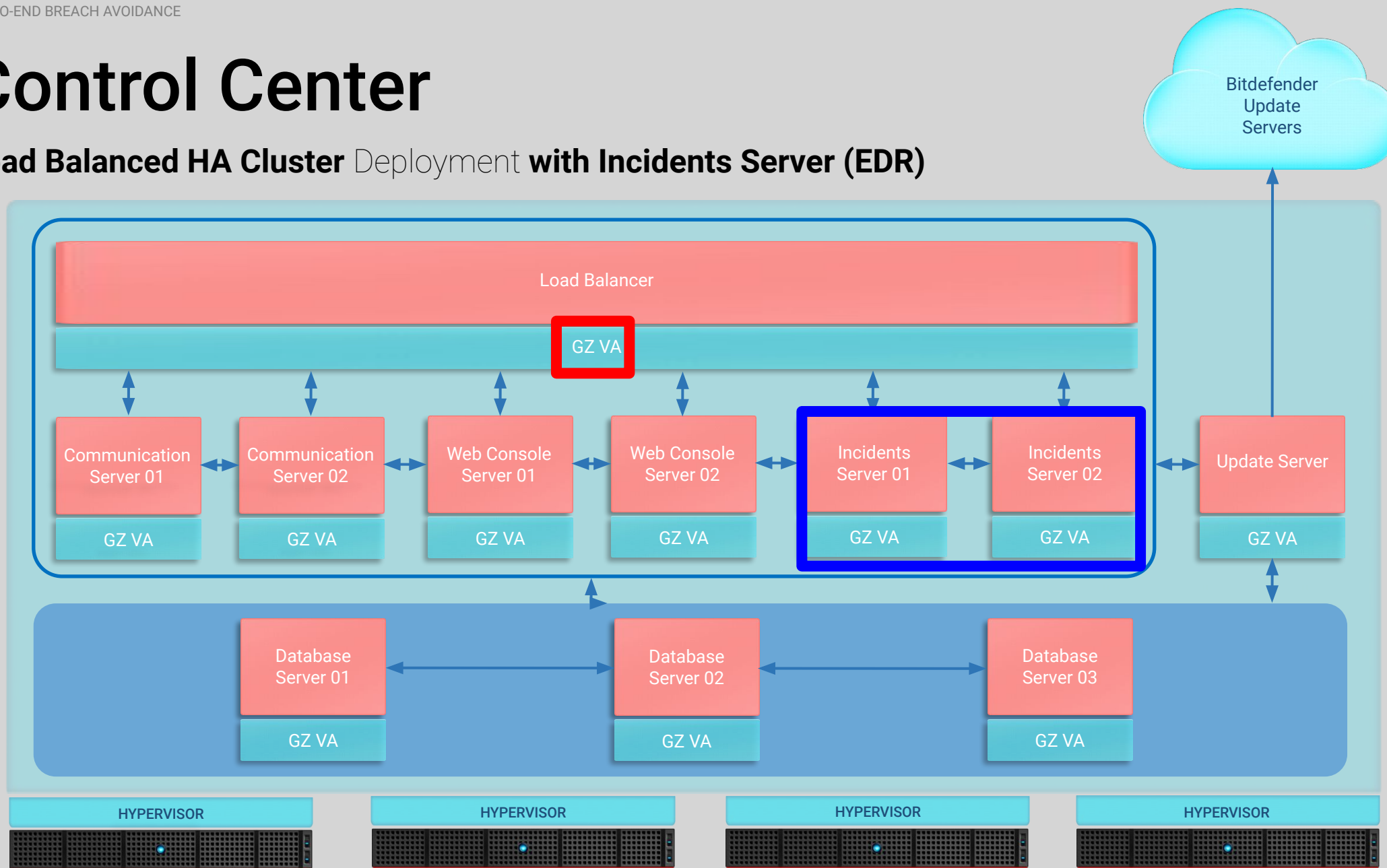
Mongo DB - Replica Set  
Min 3 copie - Max 7 copie

15 Bitdefender®



# Control Center

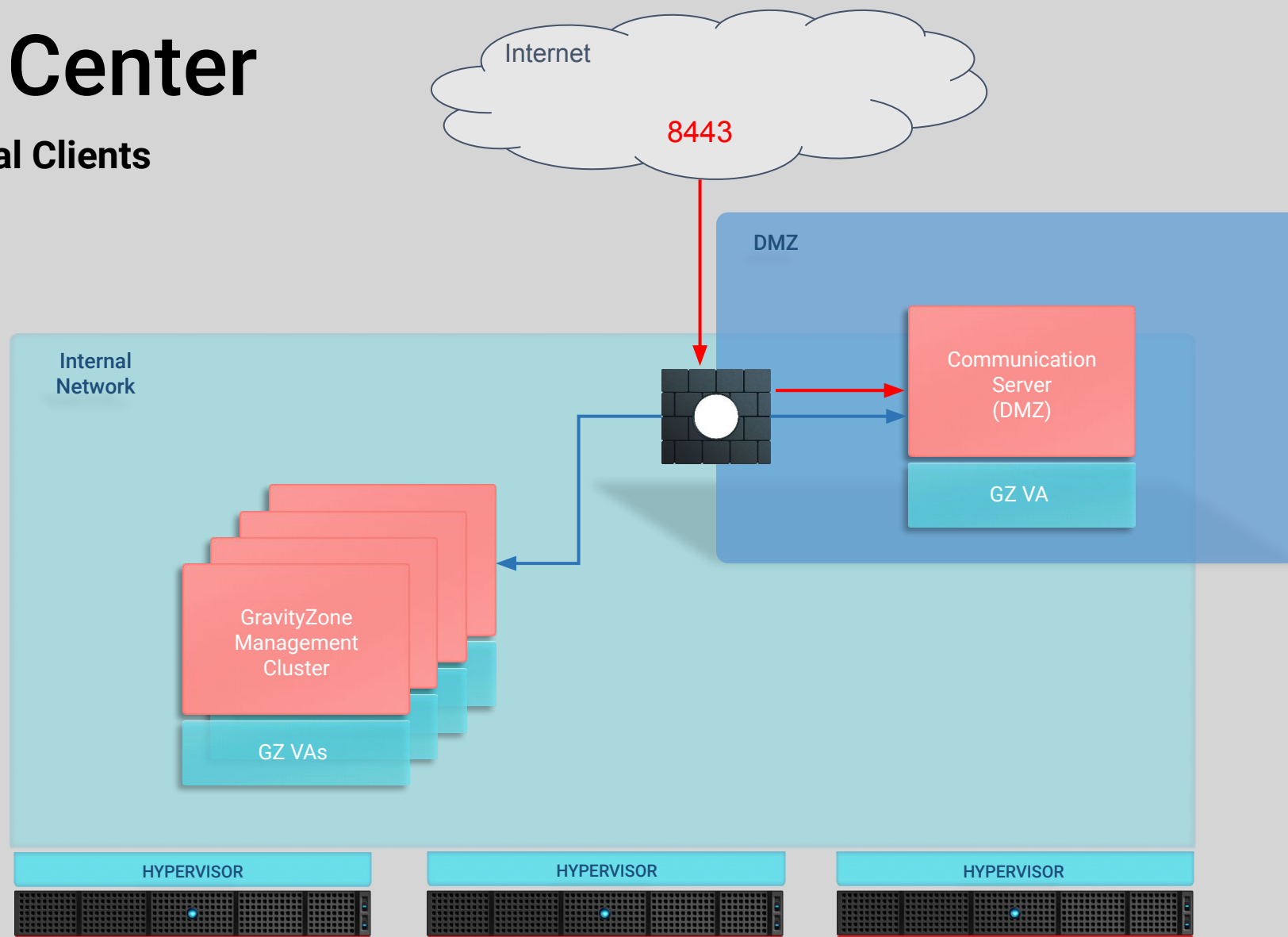
## Load Balanced HA Cluster Deployment with Incidents Server (EDR)





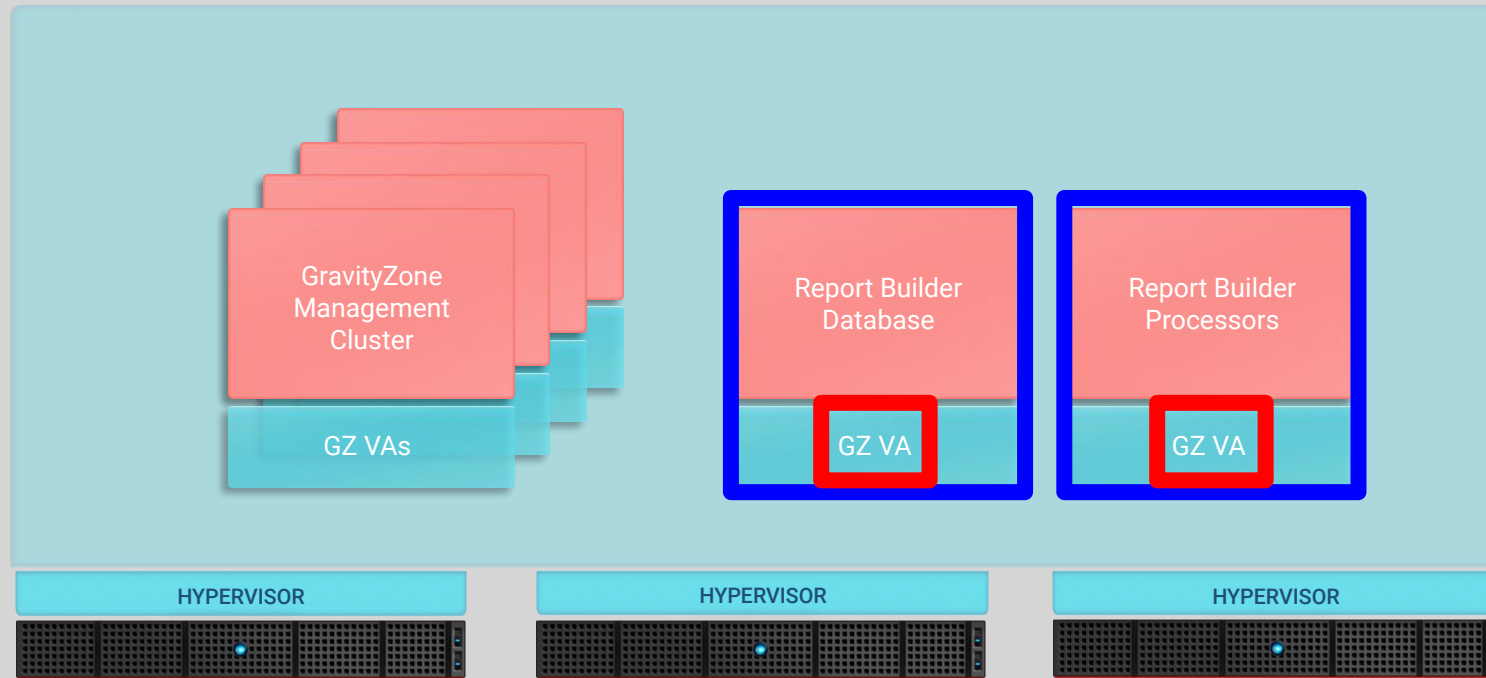
# Control Center

Managing **External Clients**



# Control Center

optional **Report Builder**



# BITDEFENDER ENDPOINT SECURITY TOOLS

Unified Next-Gen Endpoint Security Client

Windows

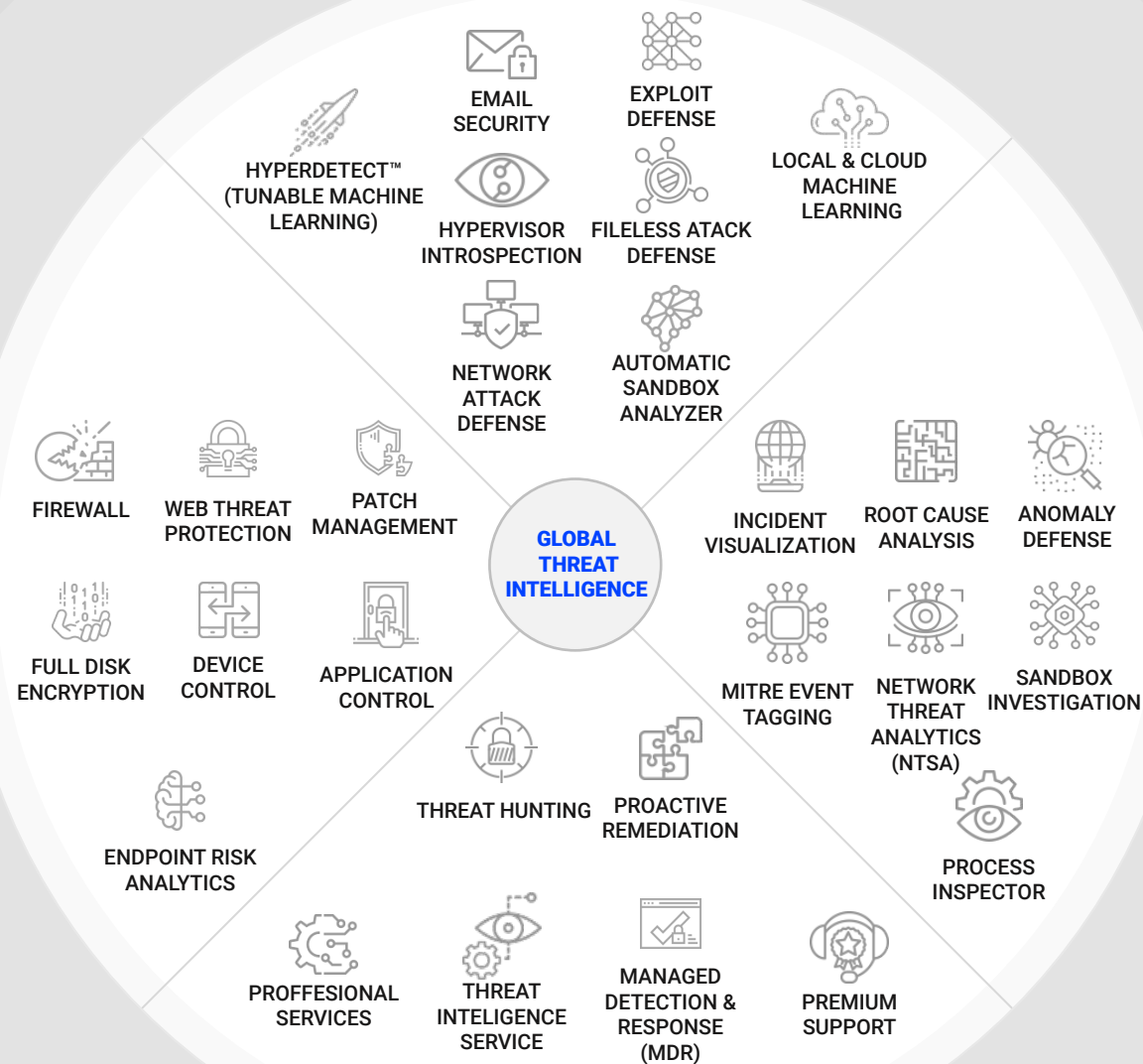
Linux

Mac OS

# INTEGRATED TECHNOLOGIES & SERVICES FOR THE BEST BREACH AVOIDANCE

Bitdefender GravityZone is a next-generation security platform that lets you protect all the endpoints in the enterprise, including client devices and both virtual and physical datacenter infrastructure.

RISK  
ANALYTICS &  
HARDENING



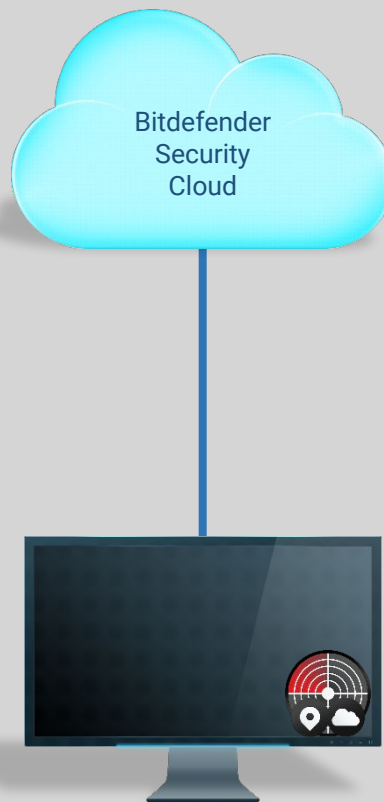


# BEST

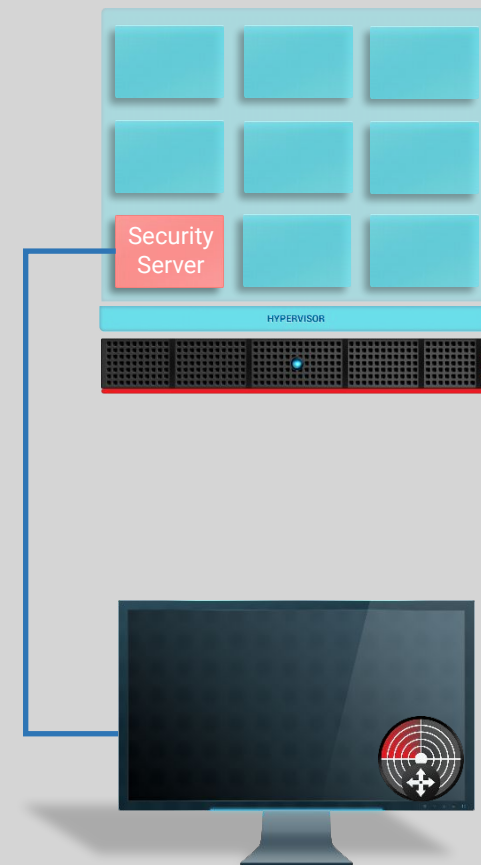
## Scan Engines



Local Scan



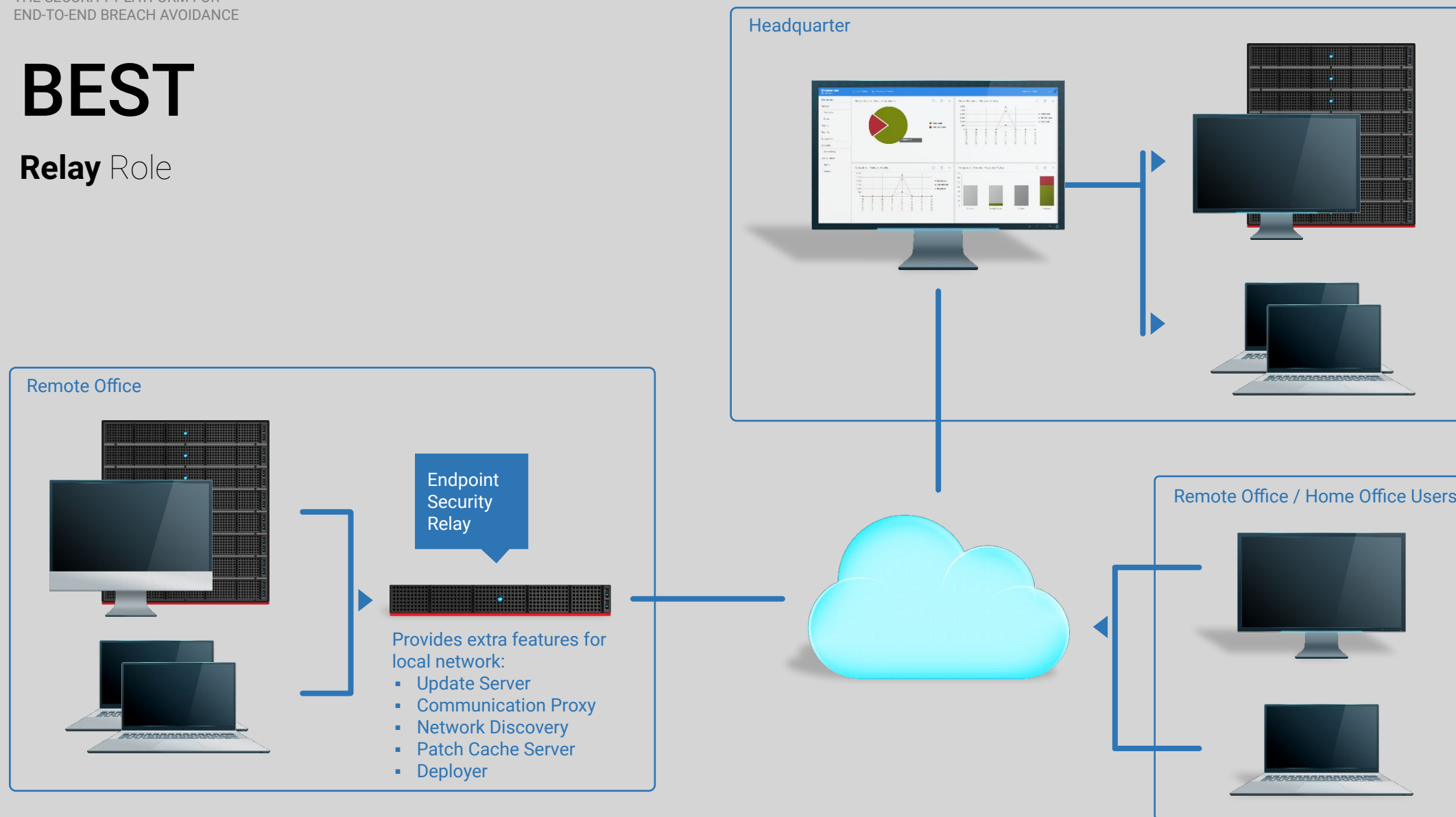
Hybrid Scan



Central Scan

# BEST

## Relay Role



# BITDEFENDER ENDPOINT SECURITY TOOLS

Protection Layers  
Availability

	WINDOWS		LINUX	macOS
Layer	Workstations	Servers	Servers	Workstations
▼ Antimalware	✓	✓	✓	✓
Local Scan	✓	✓	✓	✓
Central Scan	✓	✓	✓	
Hybrid Scan	✓	✓	✓	
▼ Advanced Threat Control	✓	✓		✓
▼ Fileless Attack Protection	✓	✓		
▼ HyperDetect	✓	✓	✓	
▼ Advanced Anti-Exploit	✓			
▼ Firewall	✓			
▼ Content Control	✓			✓
▼ Network Attack Defense	✓			
▼ Device Control	✓	✓		✓
▼ Application Control (Whitelisting)	✓	✓		
▼ Full Disk Encryption	✓	✓		✓
▼ Patch Management	✓	✓		
▼ Endpoint Detection and Response (EDR)	✓	✓	✓	✓
▼ Endpoint Risk Analytics (ERA)	✓	✓		
▼ Sandbox Analyzer	✓	✓		
Automatic Submission	✓	✓		
Manual Submission	✓	✓		
▼ Tamper Protection	✓	✓		✓
▼ Relay Role	✓	✓	✓	

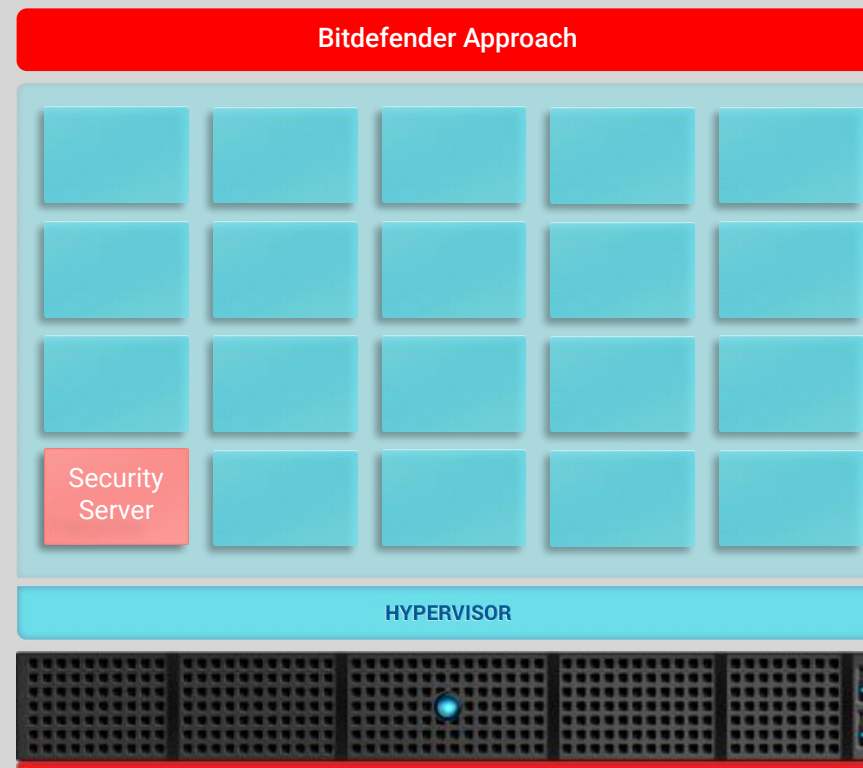
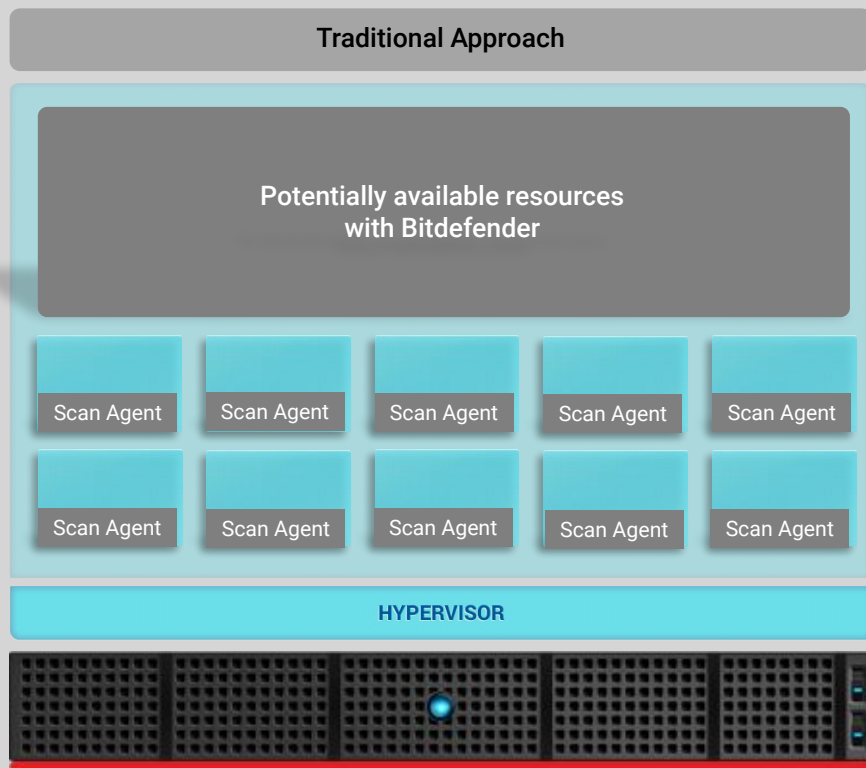
# SECURITY FOR VIRTUALIZED ENVIRONMENTS

Hypervisor Agnostic Security



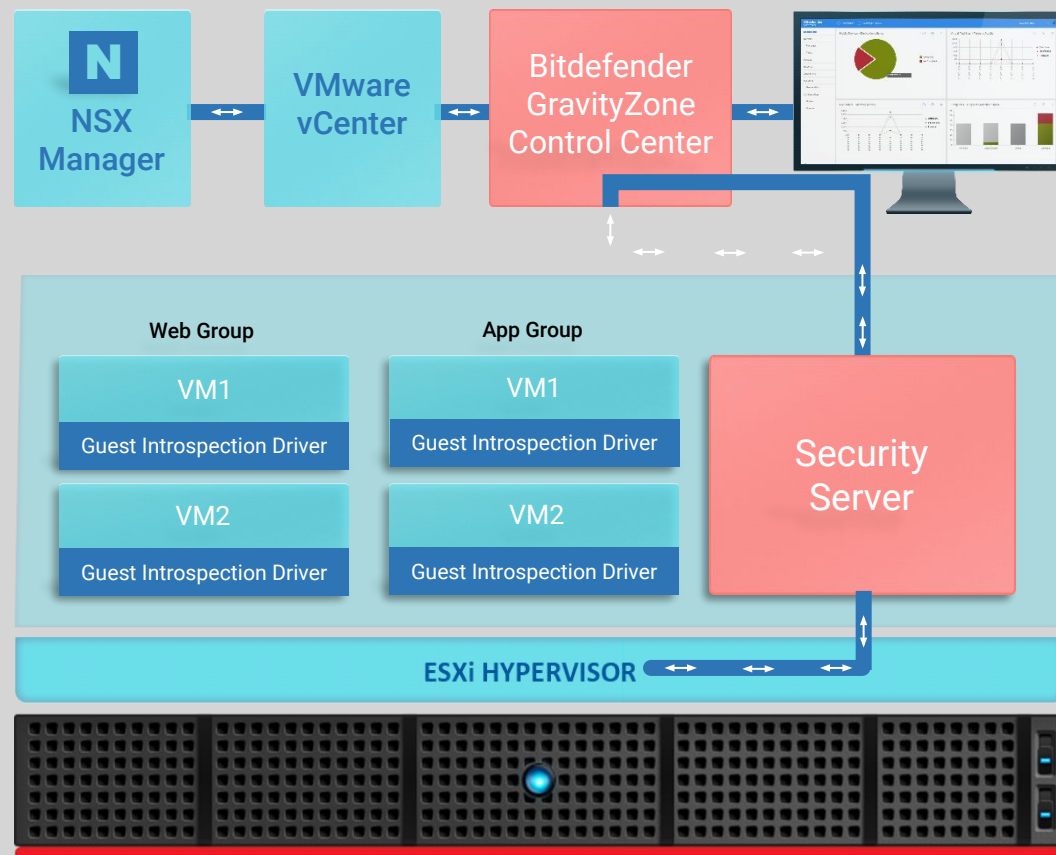
# SVE

## Traditional vs. Bitdefender Approach



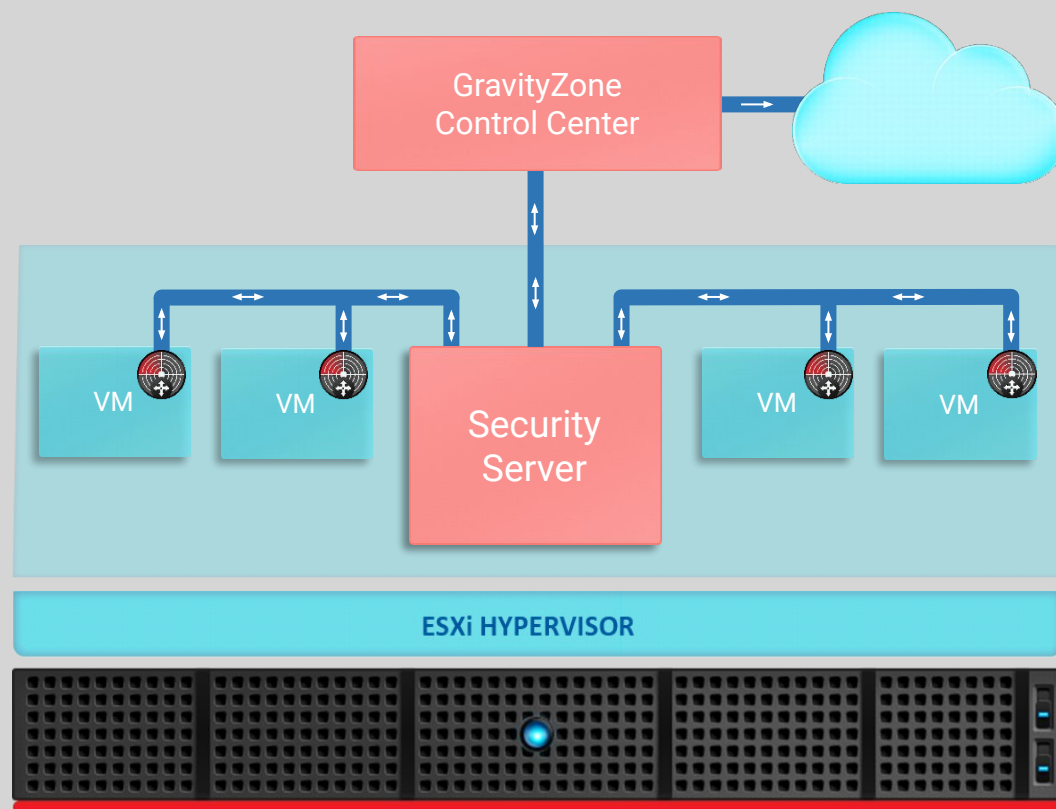
# SVE

VMware Environments with NSX-V / NSX-T



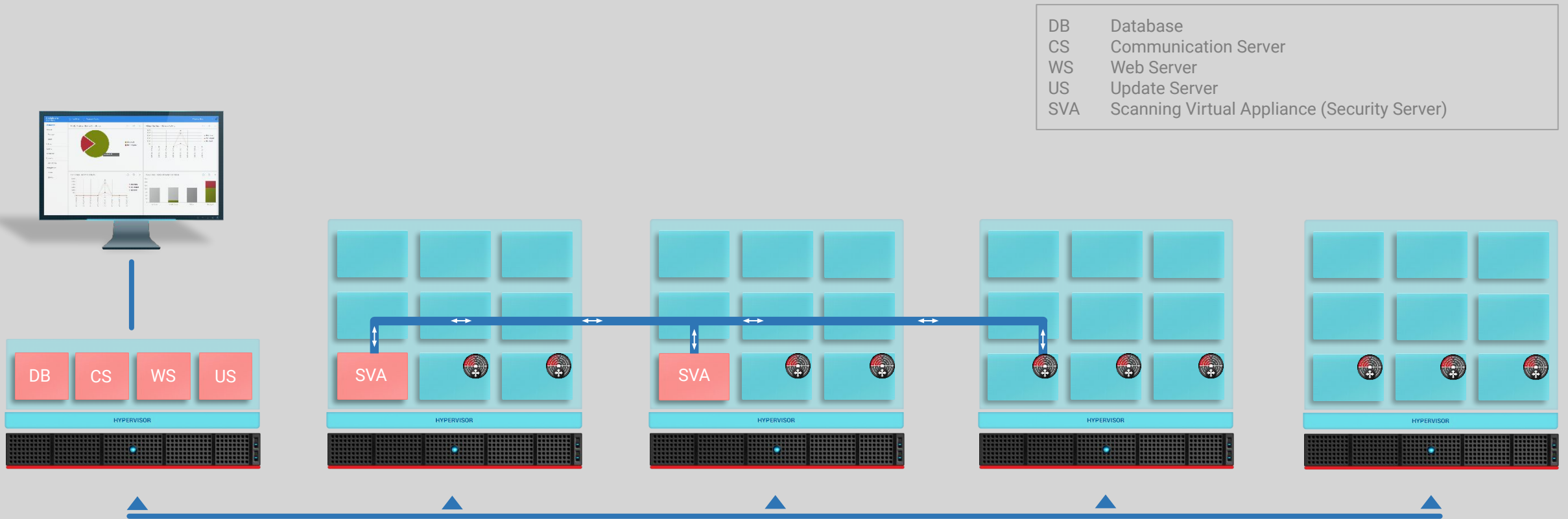
# SVE

## Multiplatform Architecture



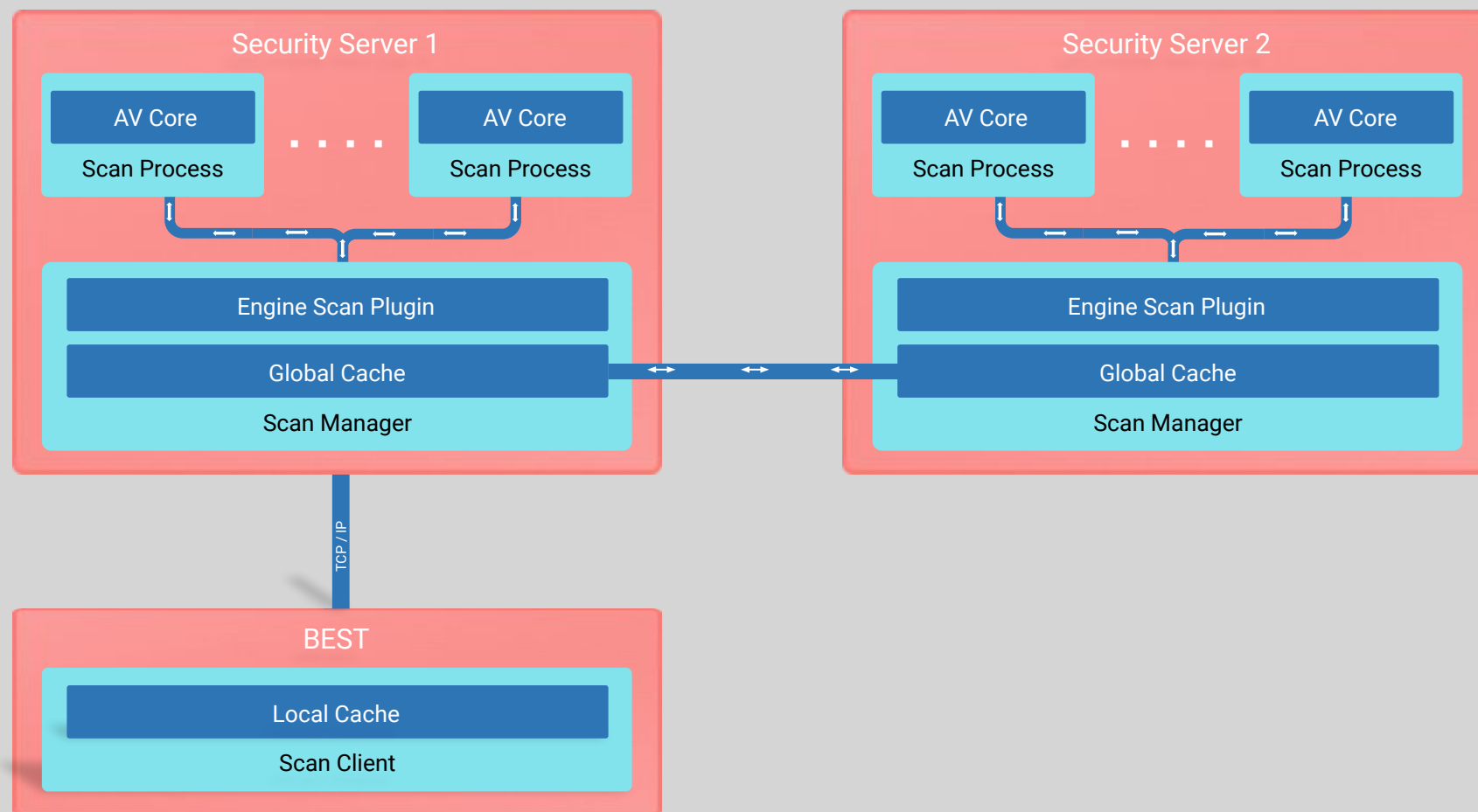
# SVE

## Multiplatform Architecture



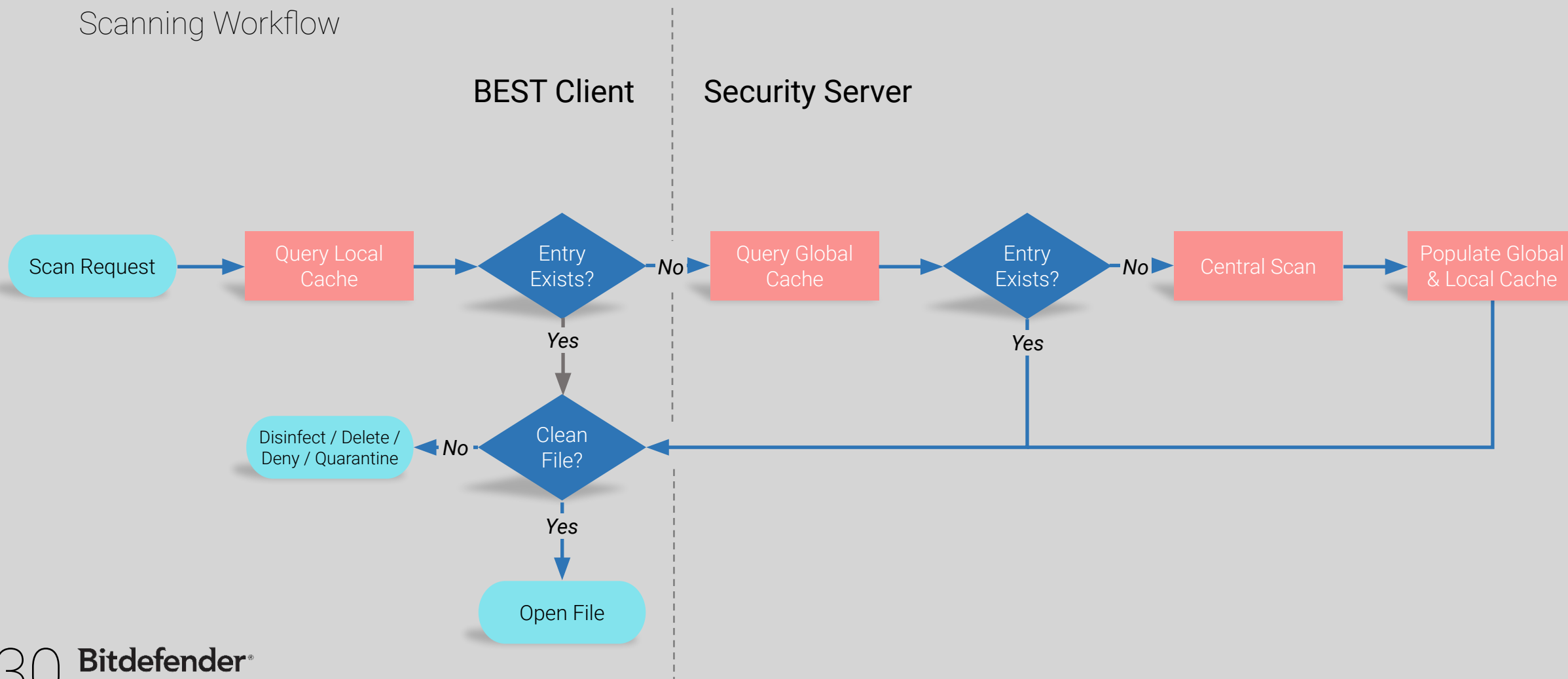
# SVE

## Scanning Components



# SVE

## Scanning Workflow



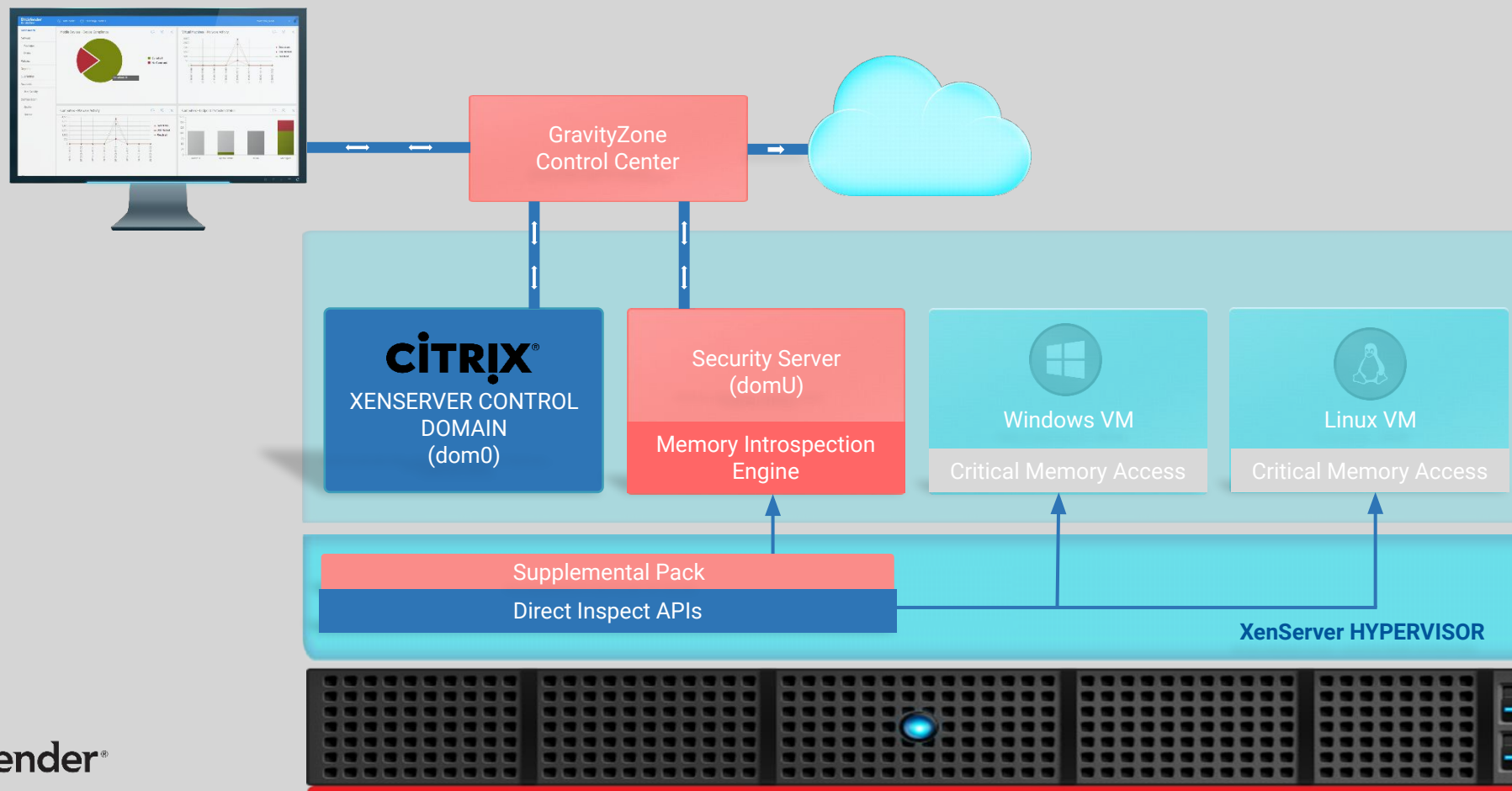
# HYPERVISOR INTROSPECTION

Security at Hypervisor Level



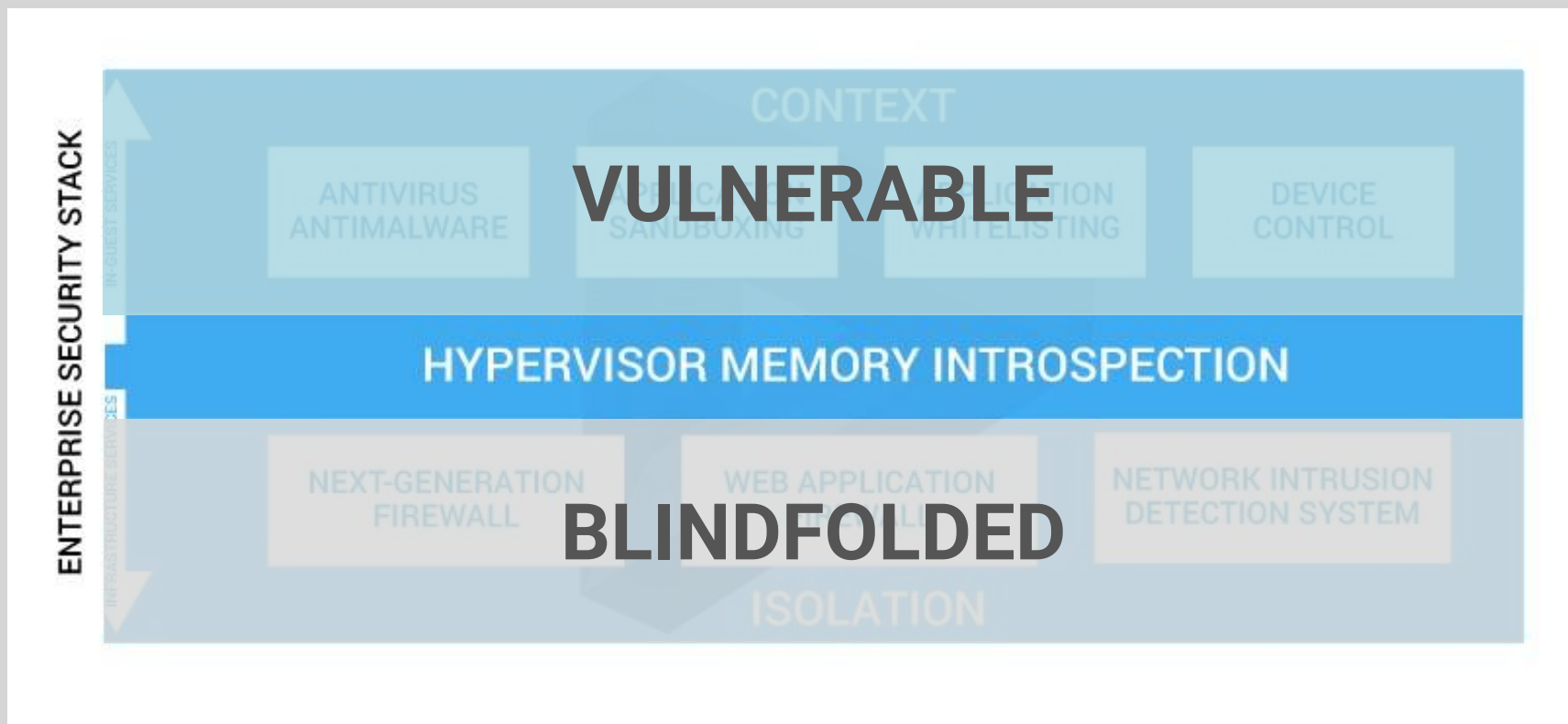
# HYPERVISOR INTROSPECTION

True Agentless Memory Protection



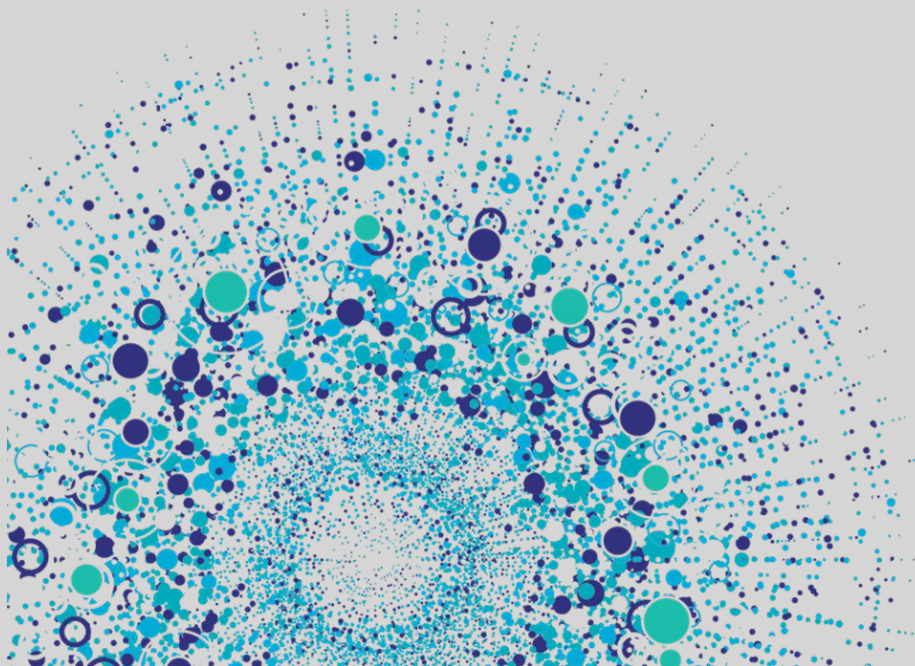
# HYPERVISOR INTROSPECTION

True Agentless Protection



## ENDPOINT SECURITY PERSPECTIVE

OPERATING SYSTEM LEVEL



HUNDREDS OF MILLION  
KNOWN & UNKNOWN **MALWARE**

## BITDEFENDER HVI PERSPECTIVE

HYPERVERSOR LEVEL



HEAP SPRAY  
CODE INJECTION  
FUNCTION DETOURING  
API HOOKING ETC.

# SECURITY FOR MOBILE DEVICES

Detects advanced attacks in real-time and automates alert triage

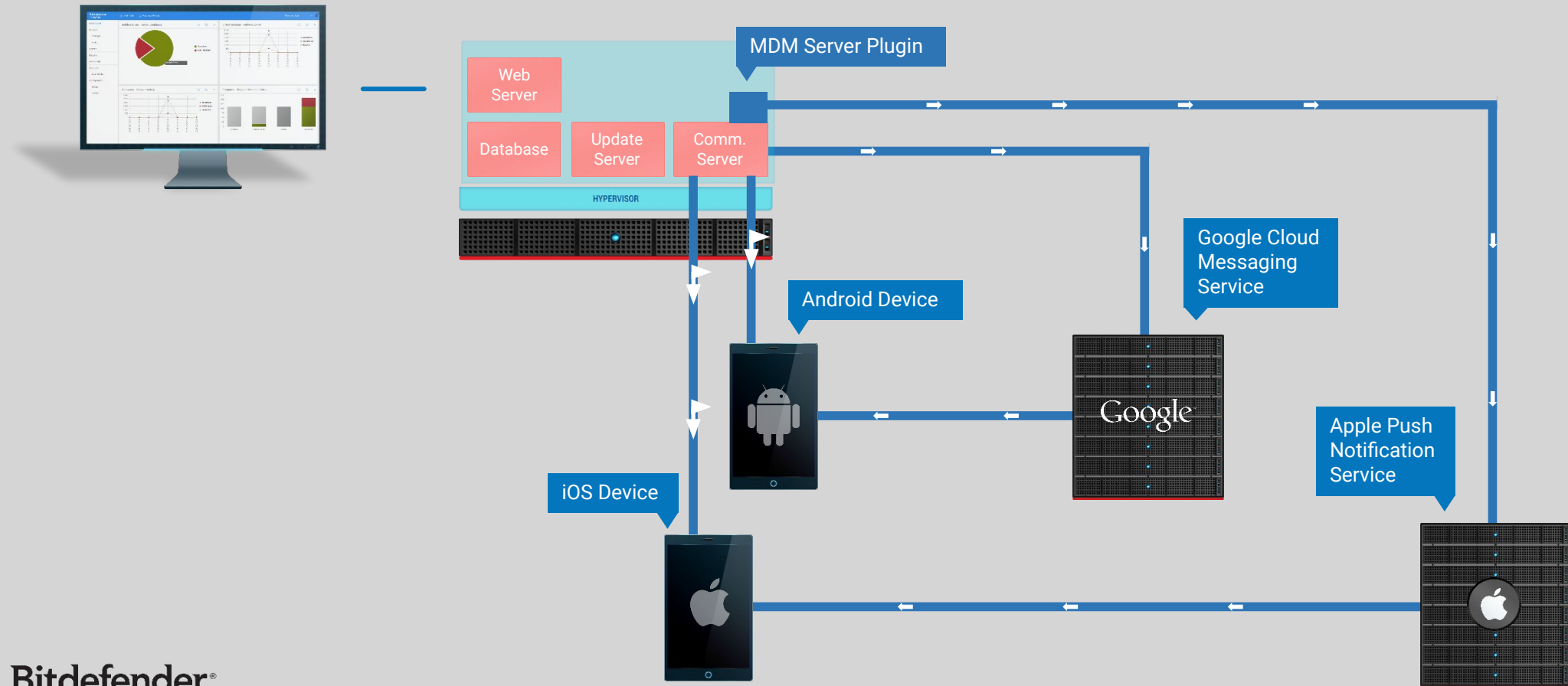
## SECURITY FOR MOBILE DEVICES

Provides basic MDM  
functionalities and  
security features

FEATURES	Android	iOS
<b>Mobile Device Management</b>		
▼ Screen Lock	✓	✓
▼ Authentication Control	✓	✓
▼ Device Location	✓	✓
▼ Remote Wipe	✓	✓
▼ Detection of Rooted or Jailbroken Devices	✓	✓
▼ Security Profiles	✓	✓
<b>Security</b>		
▼ Antimalware	✓	
▼ Removable Media Encryption	✓	

# SECURITY FOR MOBILE DEVICES

## Communication Workflow



# SECURITY FOR STORAGE

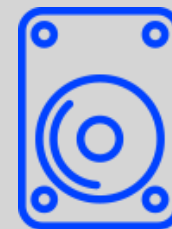
Protects ICAP-compliant NAS and file-sharing solutions



# SECURITY FOR STORAGE

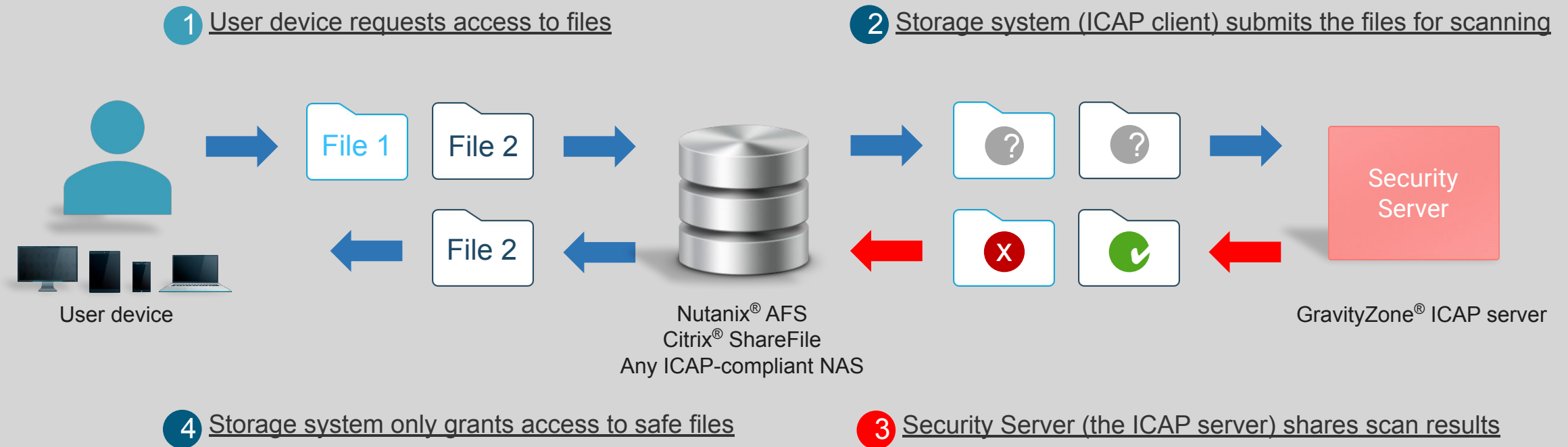
Managed by GravityZone Control Center

- Real-time protection for Citrix ShareFile, Nutanix AFS, and **ICAP-compliant** NAS (e.g., Dell® Compellent™, Dell EMC® Isilon, Hitachi® HNAS, HPE® 3PAR StoreServ, IBM® Storwize, etc.)
  - **On-access scanning** with configurable **automatic actions and exclusions**
  - **Customizable reporting** and **real-time notifications**



# SECURITY FOR STORAGE

How It Works



# SECURITY FOR STORAGE

Compatibility

GravityZone Security for Storage add-on works with:

- GravityZone Advanced Business Security
- GravityZone Elite
- GravityZone Ultra
- GravityZone Enterprise Security

**NON** suitable for **GravityZone Business Security**

# SANDBOX ANALYZER ON-PREMISE

Automated, AI-powered, Integrated

# SANDBOX ANALYZER

What It Does

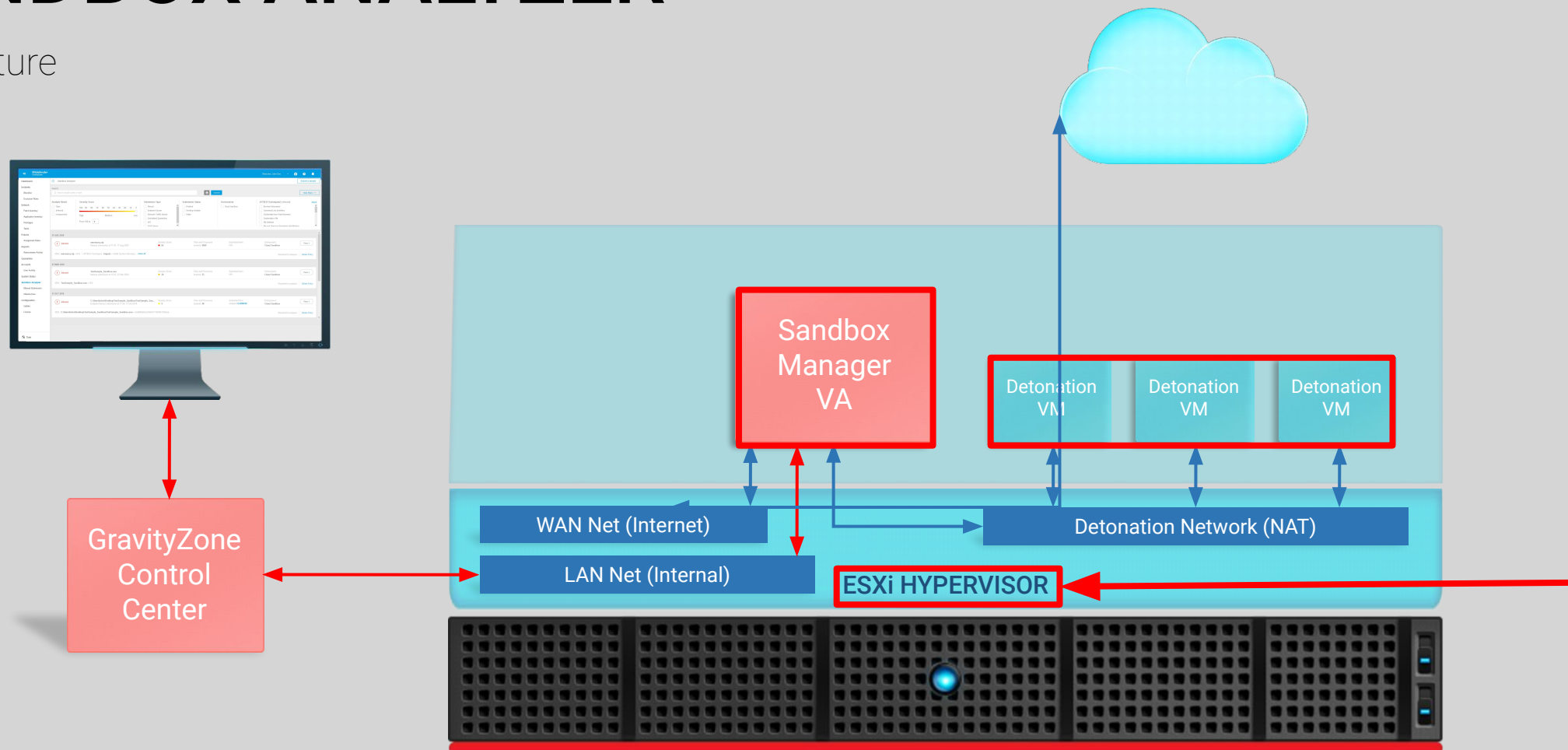
- Records and analyzes all system changes during file execution:
  - File system changes: create, modify, delete, change
  - Registry key changes
  - Process operations: create, terminate, inject
  - API instructions execution
  - Network connections

\*You can also manually submit files/URL for analysis form console



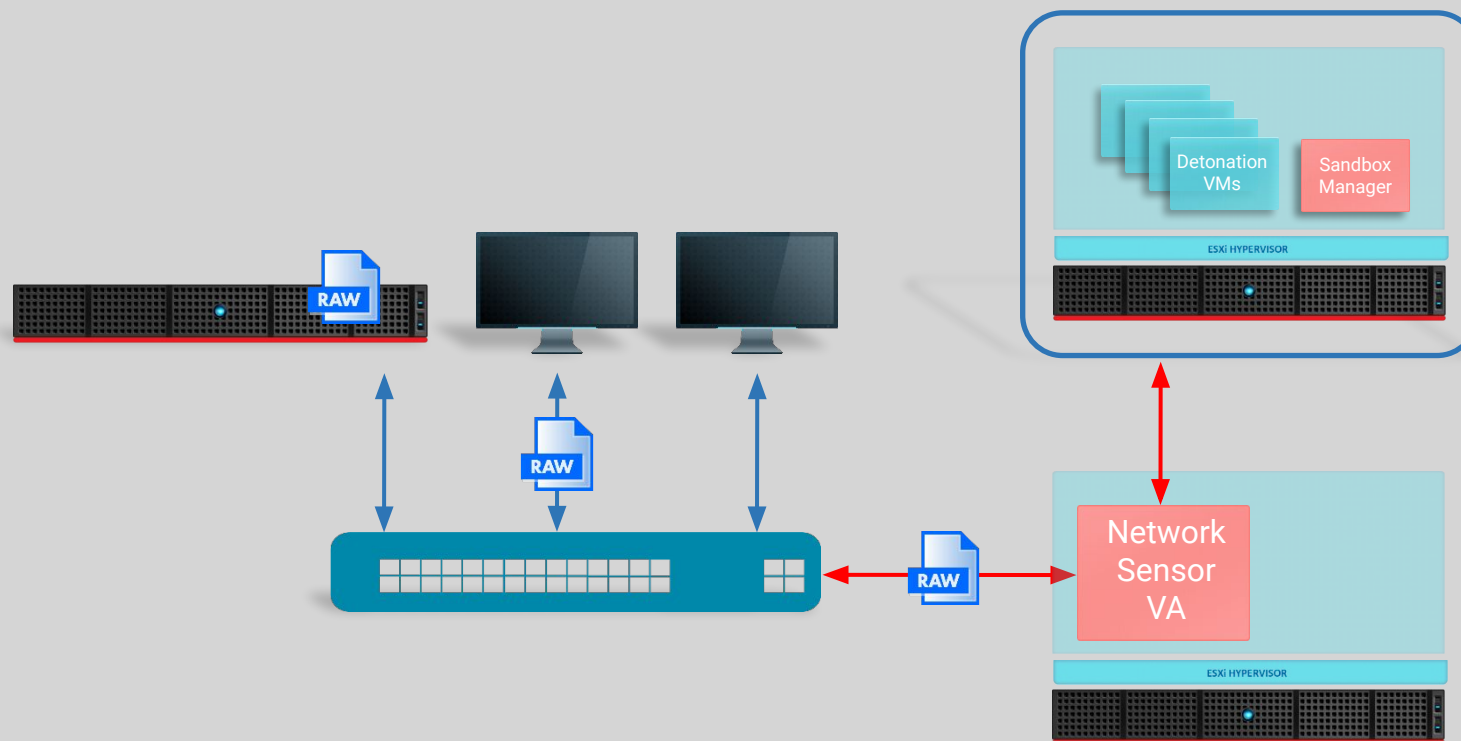
# SANDBOX ANALYZER

## Architecture



# SANDBOX ANALYZER

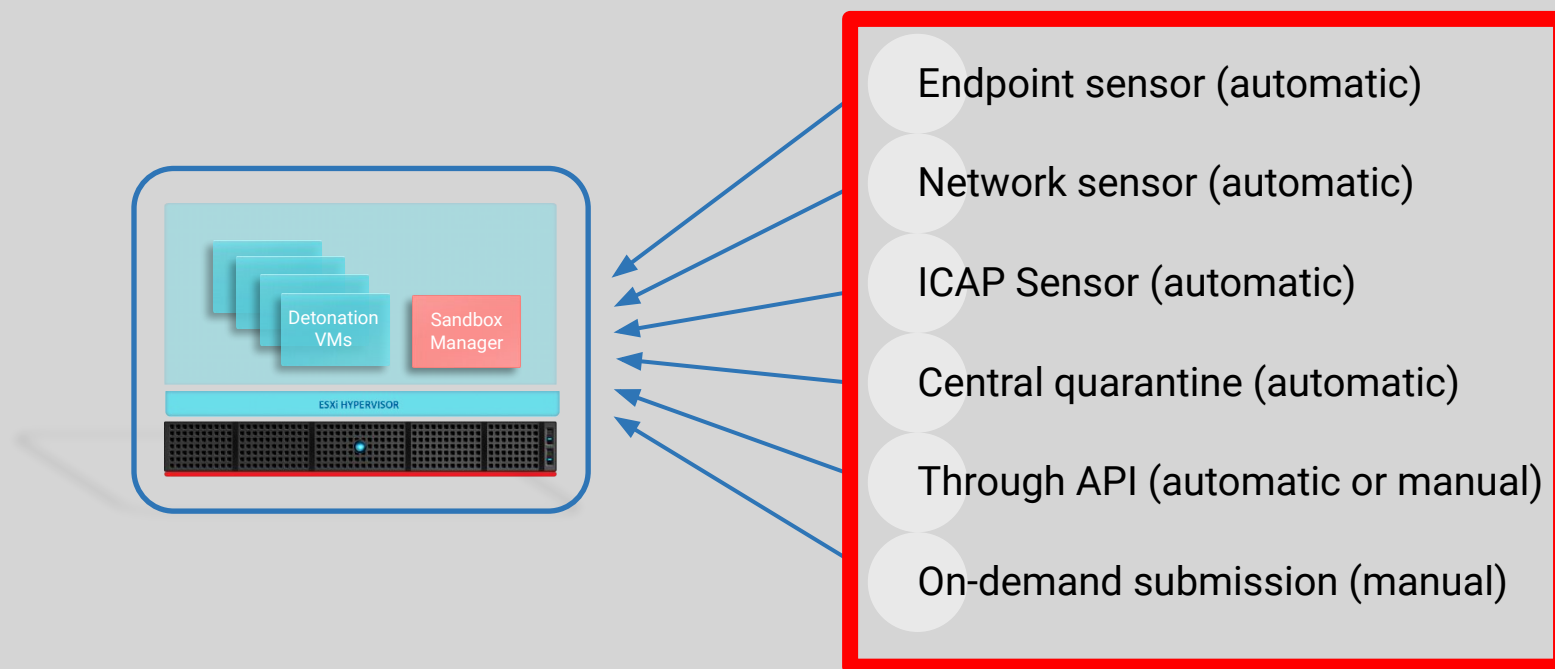
Network Sensor (NSVA)





# SANDBOX ANALYZER

## Submission Options



# SANDBOX ANALYZER

## Supported File Types



PE files, 32 bit, 64 bit



Archives: zip, rar, tar, gz, 7-zip etc.



Support for URL detonation using pre-installed browsers



MS Office file-types: doc, docx, pptx, xps, rtf etc. ; Adobe Reader pdf etc.



Scripts with support for command line switches

# SECURITY FOR EXCHANGE

Top-rated antispam and antimalware for mail servers,  
ensuring a secure messaging and collaboration  
environment

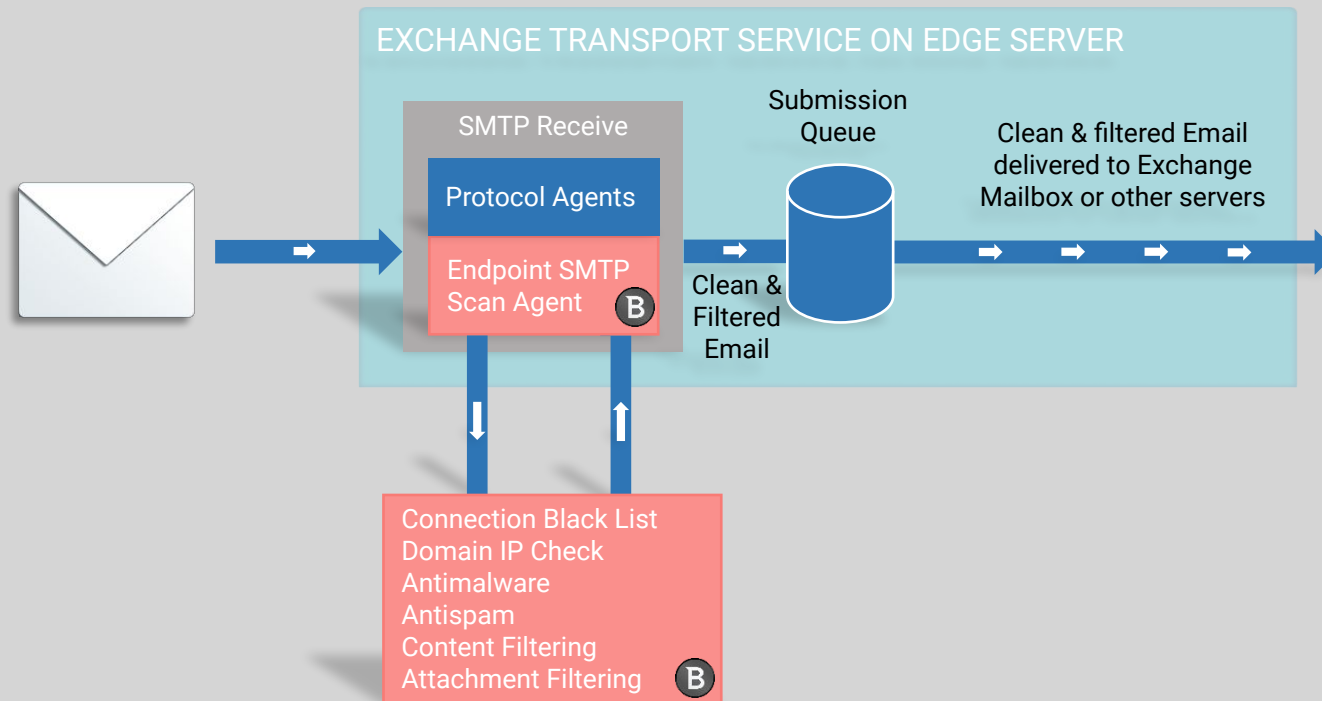
# SECURITY FOR EXCHANGE

## Features Availability

	Microsoft Exchange 2019 / 2016 / 2013		Microsoft Exchange 2010 / 2017		
FEATURES	Edge	Mailbox	Edge	Hub	Mailbox
<b>TRANSPORT LEVEL</b>					
▼ Antimalware Filtering	✓	✓	✓	✓	
▼ Antispam Filtering	✓	✓	✓	✓	
▼ Content Filtering	✓	✓	✓	✓	
▼ Attachment Filtering	✓	✓	✓	✓	
<b>EXCHANGE STORE</b>					
▼ On-demand Antimalware Scanning		✓			✓

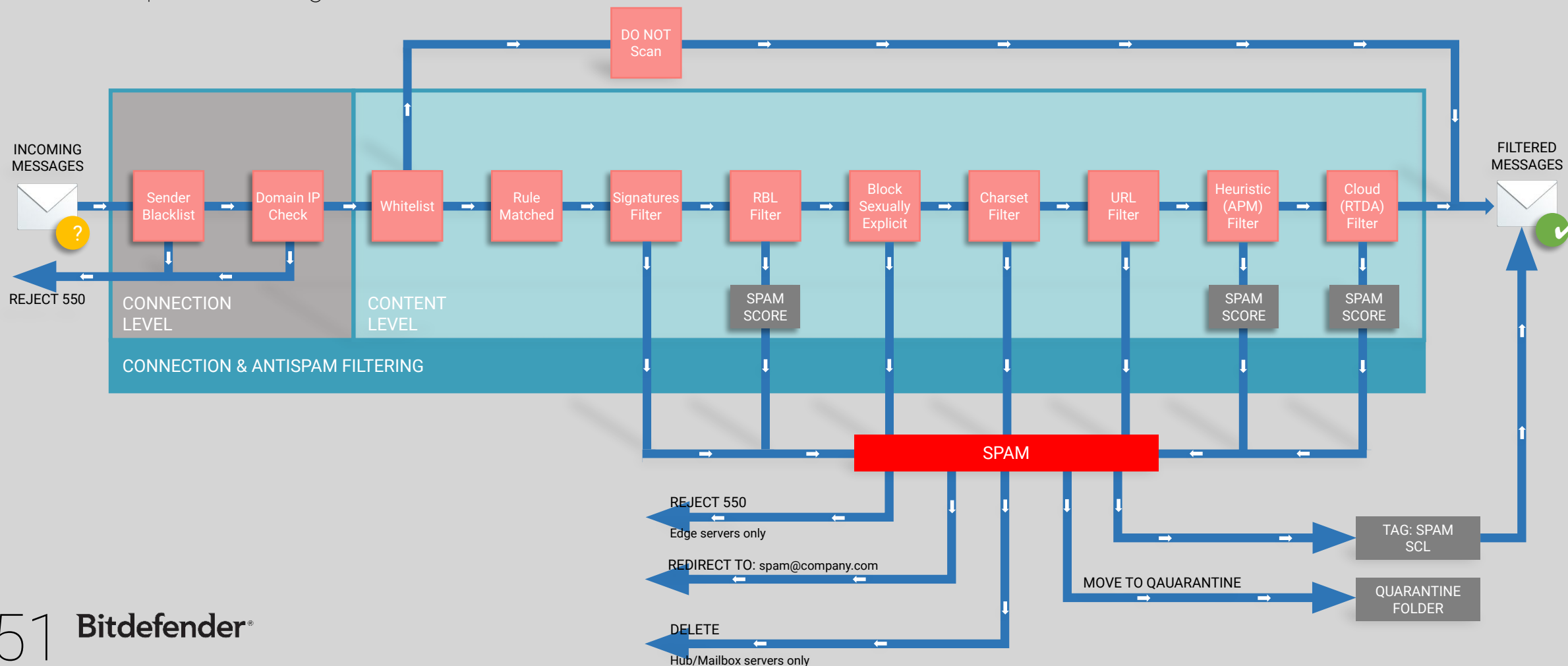
# SECURITY FOR EXCHANGE

Integration With Exchange Transport Service



# SECURITY FOR EXCHANGE

## Antispam Filtering



# EMAIL SECURITY CLOUD

Uses multiple industry-leading engines to provide an outstanding level of protection against known, unknown and emerging email threats



# EMAIL SECURITY

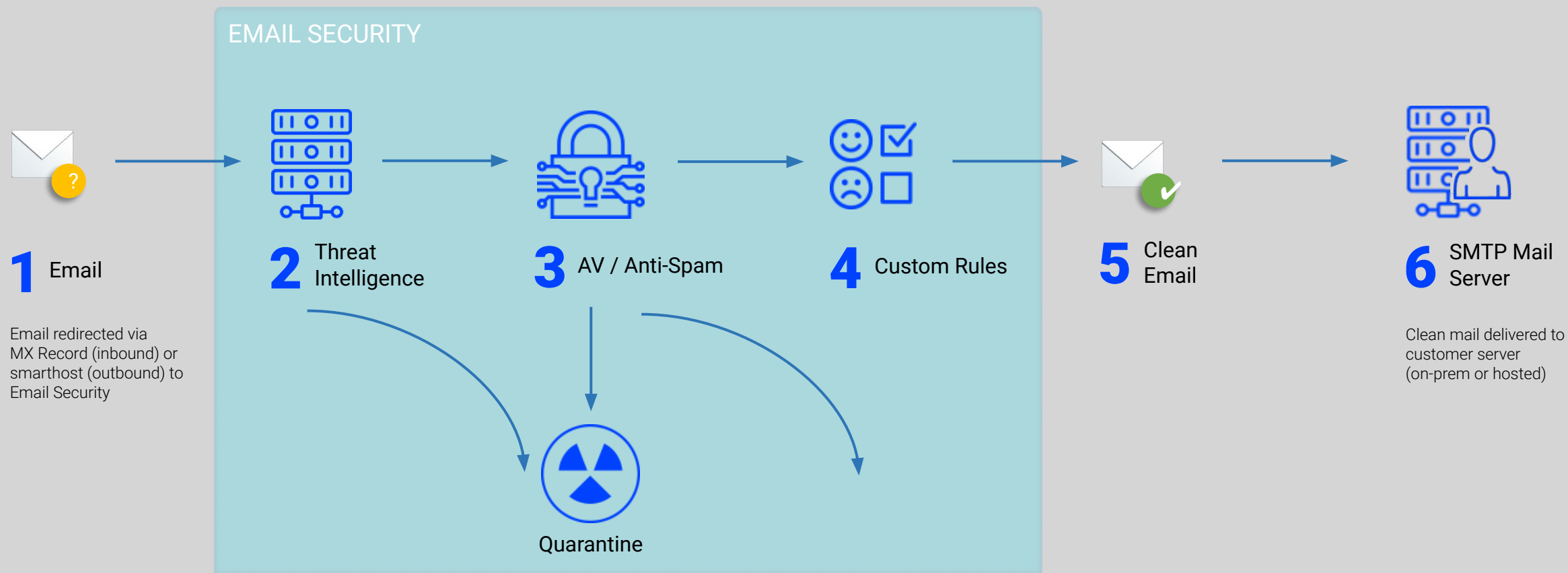
## What It Does

- Security combined with a full cloud mail routing engine
- Apply rules based on connection level characteristics
- Over 30 conditions available including [direction](#), [sender/recipient](#), [AD attributes](#), [subject](#), [body](#), [headers](#), [attachment size](#) etc.
- Over 25 actions including [accept](#), [reject](#), [re-route](#), [add content to subject/body/headers](#), [\(quarantine, modify spam score\)](#)
- Customisable dictionaries based on patterns and regular expressions



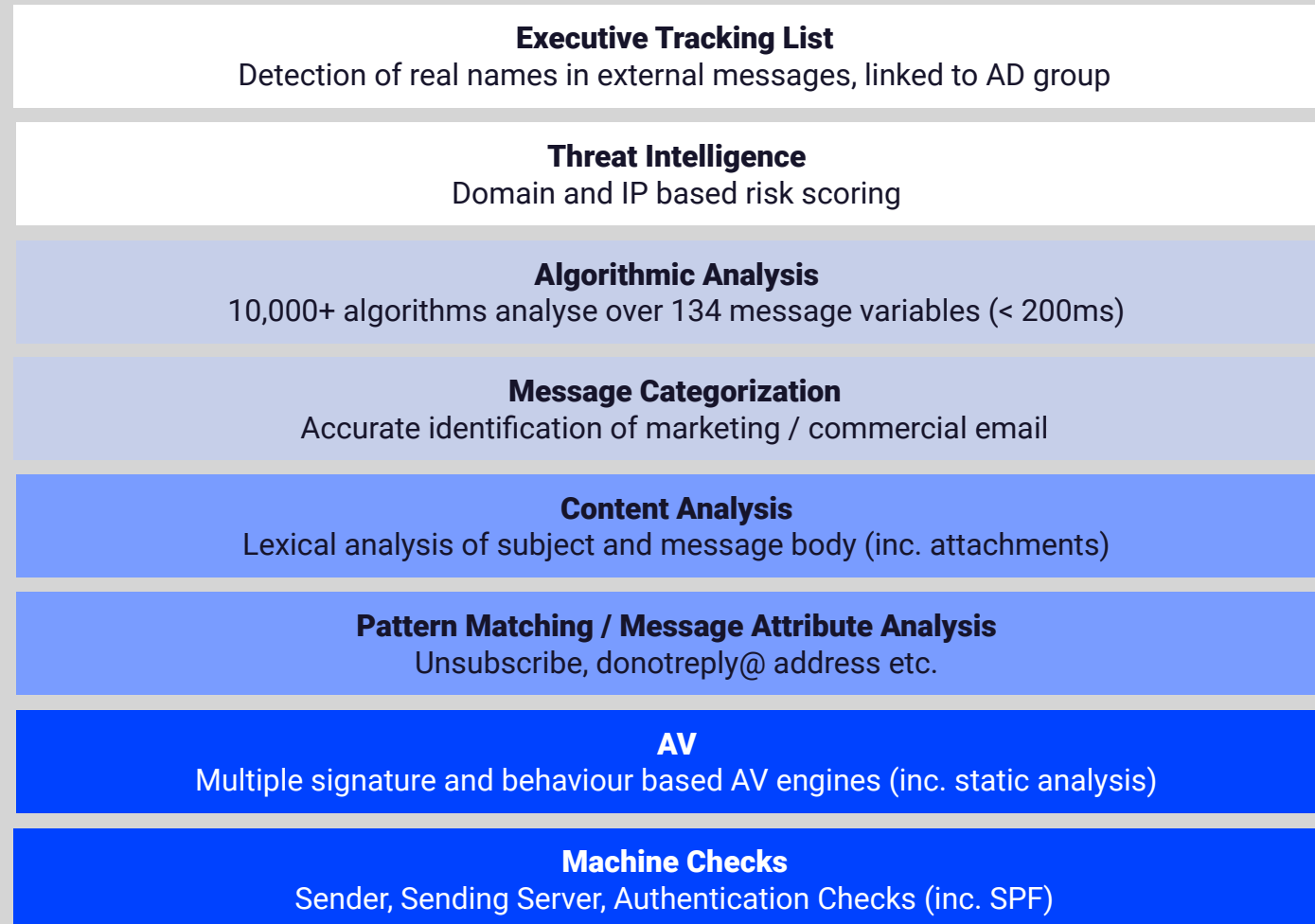
# EMAIL SECURITY

How It Works



# EMAIL SECURITY

## Multi-layered Approach

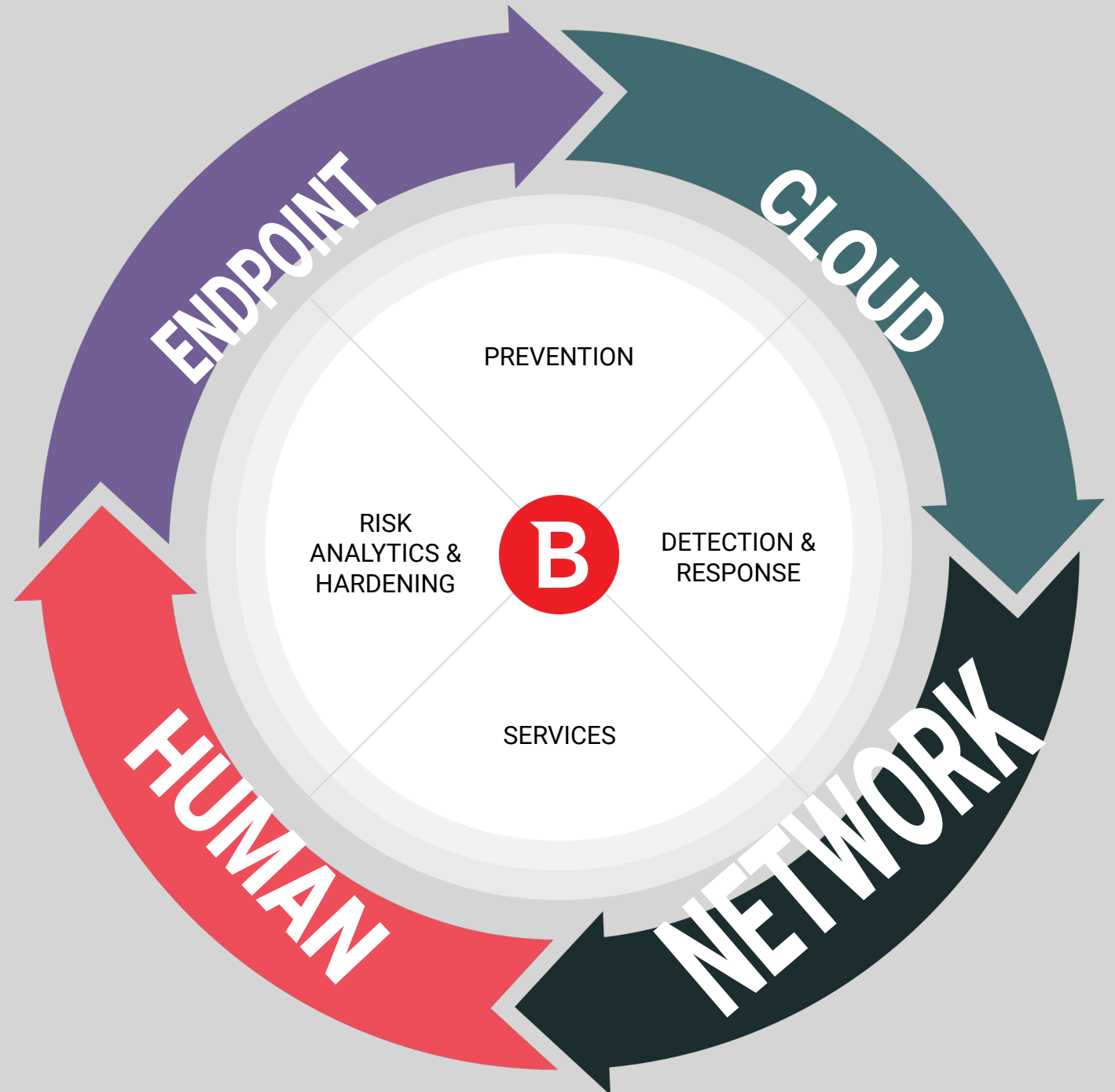


# SUMMARY

# BITDEFENDER GRAVITYZONE®

## THE FIRST UNIFIED SECURITY AND RISK ANALYTICS PLATFORM

Unified Prevention, Detection, Response and  
Hardening Across Endpoint, Network, Cloud  
and Human





Bitdefender®

[WWW.BITDEFENDER.COM](http://WWW.BITDEFENDER.COM)

# DEMO

# TEST CERTIFICAZIONE



# Bitdefender eLearning

[\*https://elearning.bitdefender.com/\*](https://elearning.bitdefender.com/)

Effettuare login con il proprio account personale.

Selezionare (in basso)

**English - Business Portfolio Technical Training 2021**

Sezione **Certification - Final assessment**

**English - Business Portfolio Technical Test 2021**

# TEST CERTIFICAZIONE

## *risorse*

- **Queste slide**  
GotoWebinar - Documenti
- **GravityZone - Solution Comparison**  
<https://www.bitdefender.com/business/compare.html>
- **GravityZone - Protection Layers Availability**  
<https://www.bitdefender.mobi/support/gravityzone-protection-layers-availability-2399.html>
- **GravityZone - User Guides**  
<https://download.bitdefender.com/business/GravityZoneEnterprise/Current/Documentation/>
- **GravityZone - VA Download**  
<https://download.bitdefender.com/business/GravityZoneEnterprise/Current/>

# AVANGATE

*Distributore a valore aggiunto*



*Roberto Novasconi*

# GRAZIE