# Smart Centralized Scanning

## Balancing the Security to Performance Scales

Cybersecurity requirements for businesses are expanding due to the increased sophistication of threats and the diversity of environments businesses now have to manage.  Datacenters now mostly reside in large virtual server farms that are sometimes on-premises, but increasingly in public and private clouds.  The number of virtual systems running on servers continues to rise, and this rise leads to greater virtual machine density.  This increased density elevates the requirement for more CPU, Ram, and storage. Hybrid and cloud environments pose different challenges around deployment and management of cybersecurity solutions for those diverse environments, as well as costs considerations. Businesses don't want to be burdened by security solutions whose resource consumption elevates operating costs.

Security solutions continue to evolve to face the modern security threats. By adding features necessary such as machine learning, artificial intelligence, detailed attack analysis, risk mitigation and more—security solutions can sometimes require more random access memory, processing power, disk space, and bandwidth to operate.  As companies migrate to the cloud, businesses need to be cognizant of the costs involved in hosting their infrastructures in the cloud.  Compute, Network, and Storage costs can all be affected by cybersecurity solutions.  More than ever, cybersecurity solutions must be lightweight and scalable, while remaining resilient against the most sophisticated of cyber-attacks.  To address these challenges, cybersecurity companies have developed centralized scanning technology.  This technology allows multiple systems to be scanned from a central scan server in order to alleviate the workload requirements on endpoints, while providing easy scalability. This configuration helps alleviate some of the concerns around protecting large virtual environments, but it does bring with it unique challenges.  Deployment, management, and what occurs if the central server is unavailable, can create unnecessary headaches for security teams.

Protection for large virtual environments provide unique security challenges:

- Deployment, management, and increased technology requirements can create unnecessary work for security teams
- Increased security requirements for cloud workloads can significantly increase operating costs
- Performance impact of legacy cybersecurity solutions can negatively affect systems Centralized scanning solutions may have inadequate redundancy features for production environments

## At-a-Glance

Smart Centralized scanning is a patented solution that was designed for virtualized environments and cloud workloads. The technology provides Bitdefender's award-winning cybersecurity solutions through a configuration with diminished resource consumption ideal for datacenters and cloud workloads.  Businesses no longer have to compromise between robust cybersecurity and system performance.

## Key Benefits

- **Eliminates file scanning duplication** – two-level caching helps to avoid redundant scanning, significantly reducing performance impact Truly smart scanning – only file fragments capable of executing malicious code are scanned improving scanning speed, efficiency and reduce IOPS
- **Centralized management** – integration with EXSi®, VMWare®, Citrix®, Microsoft Hyper-V®, Nutanix virtualization hosts and Amazon Elastic Compute Cloud (EC2) environments allow for seamless deployment and management.

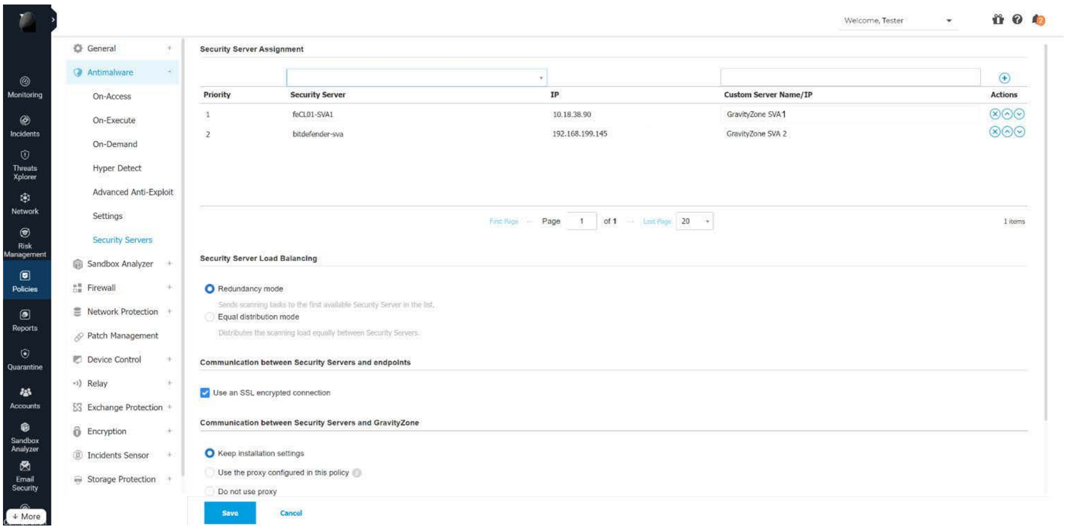
*"Because **MyCyberIQ** uses minimal resources, there has not been any impact on endpoint response time or latency.  With our IT staff based at IRSAP's headquarters, it's useful to be able to centrally and remotely manage all our physical and virtual endpoints. Overall, security administration has become more efficient"*

*Marco Broetto,*
*IT Manager, IRSAP*

# Solution Overview

Security for Virtualized Environment is a technology specifically designed for today's demanding datacenter and cloud workload environments. With our patented technology, we remove resource consumption concerns related to endpoint and cloud workload protection. Through the Smart Centralized Scanning technology used by the Endpoint Protection, the normally intensive machine scanning routines are offloaded to hardened security server virtual appliances. This configuration ensures that physical or virtual endpoints aren't burdened by a resource-intensive security solution. The unique configuration
is available to protect environments running physician and virtual Windows workstations and servers, Linux systems including servers, desktops, and containers, and Mac OS endpoints as well.

The Smart Centralized Scanning technology is ideal for businesses that are looking to protect physical environments, virtual environments, and cloud workloads. It allows security teams to seamless deploy protection across the entire business from the centralized management console. For VMWare VSphere environments, we offer agent-less protection through the integration with vShield Endpoint™.



Security Server Assignment

| Priority | Security Server | IP | Custom Server Name/IP | Actions |
|---|---|---|---|---|
| 1 | feCL01-SVA1 | 10.18.38.90 | GravityZone SVA 1 | ⊗⊙⊙ |
| 2 | bitdefender-sva | 192.168.199.145 | GravityZone SVA 2 | ⊗⊙⊙ |

First Page ← Page 1 of 1 → Last Page 20 · 1 items

Security Server Load Balancing

● Redundancy mode
Sends scanning tasks to the first available Security Server in the list.
○ Equal distribution mode
Distributes the scanning load equally between Security Servers.

Communication between Security Servers and endpoints

☑ Use an SSL encrypted connection

Communication between Security Servers and GravityZone

● Keep installation settings
○ Use the proxy configured in this policy
○ Do not use proxy

Save Cancel

**Figure 1.1:** Using the policy settings, security teams can configure endpoints to communicate with several different Security Server virtual appliances either in redundancy mode for fallback capabilities, or equal distribution mode for load balancing.

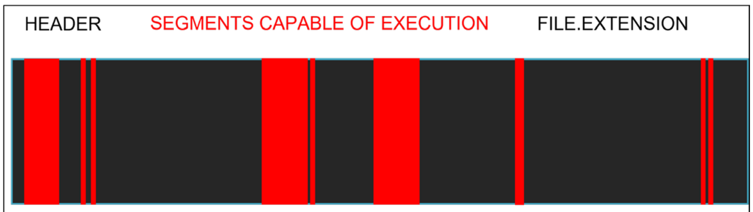
# The Technology

Security teams can easily download the Security Server Virtual appliance that will be used as the central scanning station from the management console. The Security Server VA is available for EXSi® standalone, VMWare® VSphere, Citrix® Xen servers™, Microsoft Hyper-V®, Nutanix Prism® virtualization hosts and offers integration with Amazon Elastic Compute Cloud (EC2) environments. The Security Server virtual image can then be deployed as just another virtual machine. After a simple series of steps to configure the network communication, security teams will then be ready to set up the endpoint protection to communicate with the deployed Security Servers.

Using the management console, security teams can create a featherweight agent package configured to run in our patented Smart Centralized Scanning mode. The featherweight agent maintains key components like application control, web threat protection, patch management, process inspector, ransomware mitigation, and advanced anti-exploit, while offloading more input/output intensive tasks like scanning and product updates. It also allows collaboration with the Security Server to deliver HyperDetect and Sandboxing functionality.

## Improved Server Density

Unlike traditional security solutions, our platform is designed from the ground up to be optimized for servers and cloud workloads.  The Smart Centralized Scanning technology minimizes the security footprint by leveraging a two-level caching mechanism that ensures file scans are not duplicated.  The Security Server virtual appliance inspects each file only once, even if it appears on multiple endpoints.  This helps avoid redundant scanning, significantly reducing CPU, RAM, IO, and network load. Security Server virtual appliances can also be configured for redundancy or load balancing, they can automatically detect when a virtual machine is created, moved, or deleted.  The security server can subsequently apply the assigned security policy to any machine based on resource pool assignment, groups, or networks the virtual machine is added to.



FILE.EXTENSION

| | |
|---|---|
| • Full file size | 25 MB |
| • Size of segments capable of execution (i.e., file areas subject to inspection) | 2.5 MB |
| • Saved resource expenditure | 22.5 MB |

**Figure 2.1:** Platform employs a highly efficient scanning technique which only examines fragments capable of execution, so as not to have to transmit entire files from a VM to an SVA, significantly reducing CPU, RAM, IO, and network load.

## Truly Smart Scanning

The optimization doesn't stop at eliminating the duplication of scanning.  Smart Centralized scanning further reduces the bandwidth and resources needed for identifying threats by only transferring the fragments of files capable of executing malicious code to the Security Server virtual appliance.  These fragments are transferred over a secure TCP/IP port from the endpoints to the Security Server.  Once on the Security Server, the file fragments are then scanned, and if any malicious code is detected, the entire file will be flagged for action – deny, quarantine, or delete—depending on what is defined in the policy.

By not requiring the scanning of the entire file to identity threats, Smart Centralized scanning allows the endpoint protection to run with minimal system impact even during large scan tasks.

## Ideal for Data Centers and Cloud Workloads

Smart Centralized scanning technology improves the speed at which threats can be identified while not burdening systems with increased resource consumption.  This makes the technology ideal for data centers and cloud workload environments where the endpoints are disparate, numerous, and can encompass various network configurations. Multiple Security Server virtual appliances can quickly be spun up or spun down, and can be configured through policies for optimal load balancing or redundancy.

Using the integration with VMware vCenter, Citrix XenServer and Amazon Elastic Compute Cloud (EC2), it allows security teams to manage their machine inventory from a consolidated, easy to operate interface.  Security teams will be able to review events, assign policies, trigger actions, on all systems being managed, whether on premises or in the cloud, from a single interface. Everything from running detailed reports on web content filtering activity, to isolating hosts during investigations, to configuring notifications for detected threats, to scheduling reoccurring security scans, and more will be available from the console.  Smart Centralized Scanning provides maximum flexibility and scalability for businesses of all sizes.

### Reduced Security Costs

The Smart Centralized Scanning technology helps reduce security costs by minimizing the footprint of the cybersecurity solution.   This unique configuration reduces the need to upgrade expensive hardware for on-premises and hybrid environments, and reduces the operating costs –compute, and networking— for PaaS, IaaS, and SaaS environments.

## Cybersecurity without Compromises

Businesses no longer have to decide between increased cybersecurity and system performance.  With Smart Centralized Scanning, security teams have a powerful, scalable security solution that is easy to deploy and manage for environments of all sizes. The patented technology's reduced footprint allows businesses to keep their systems protected with our partner's award-winning security without compromising on features, or negatively impacting their systems.

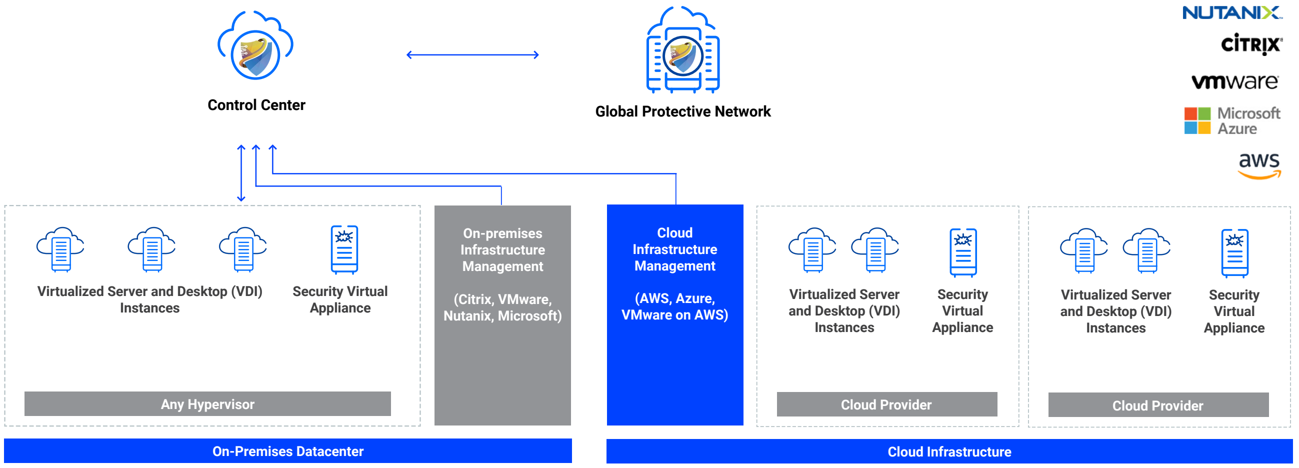

Control Center
Global Protective Network
NUTANIX
CITRIX
vmware
Microsoft Azure
aws
Virtualized Server and Desktop (VDI) Instances
Security Virtual Appliance
Any Hypervisor
On-premises Infrastructure Management
(Citrix, VMware, Nutanix, Microsoft)
Cloud Infrastructure Management
(AWS, Azure, VMware on AWS)
Virtualized Server and Desktop (VDI) Instances
Security Virtual Appliance
Cloud Provider
Virtualized Server and Desktop (VDI) Instances
Security Virtual Appliance
Cloud Provider
On-Premises Datacenter
Cloud Infrastructure

**Figure 3.1:** Smart Centralized Scanning offloads the typically resource-intensive scanning tasks from the physical and virtual machines to the Security Server virtual appliance.  This creates significant performance improvements over legacy security solution configurations. Security teams can deploy and manage this from a single console to physical and virtual environments on premises or in the cloud.