



Data Resolve

Cyber Security & Intelligence
for Enterprises

INDEFEND BUSINESS

Server Activity Monitoring

An Additional Layer of Security

www.dataresolve.com

The Challenge of Managing Server Security and Integrity

With organizations ever growing demand for more servers for data storage and running various business applications like CRM, ERP, databases and so on, there is also a growing need to ensure their security. It becomes important for organizations that once these servers become a part of their production environment, such servers need to be granted access via a very stringent and controlled process.

Further, it is also important to track any changes to the configuration and infrastructural health of these servers, to ensure that any undesirable or unnecessary changes do not occur on these servers. Such actions can be performed by the organization's system administrators, either intentionally or unintentionally.

During the up-gradation and maintenance activities for various applications running on a server, many operations need to be done at the server. Along with this, the administrator can also indulge in activities that could be malicious or harmful to the organization's information security.

Hence, to ensure the confidentiality, integrity and availability of the data at the server, continuous monitoring is required.

How inDefend-SAM can help?



In today's time it is utmost need of hour to keep an eagle's eye on various activities being performed on your organization's servers. With inDefend-SAM, a comprehensive solution to track various activities performed by administrators after logging onto such servers, organizations can now feel comfortable by adding one more layer of security, auditing and surveillance on their critical IT infrastructural assets. Henceforth, 3600 view can be easily achieved for monitoring administrators' activities on such servers.

inDefend-SAM Capabilities

Centralized Console

inDefend provides easy to use single centralized administration console for all the administration and management purposes.

- Advanced Reporting and Analytics Framework for all kinds of device and network activities
- Silent monitoring of all activities (stealth mode)
- Centralized installation and upgrades management

Monitoring Aspects

Session Monitoring

- Server activity monitoring via screenshots at high frequency providing detailed user activity
- Log-in and log-out time
- Remote Desktop Sessions taken on server through system can be monitored
- Various applications accessed on server can be monitored via active application monitoring
- Continuous monitoring of online availability of the servers

Browser Activity

- Monitoring/Blocking usage of anonymous proxies
- Monitoring/Blocking activities done in private browsing and/or incognito mode
- Monitoring/Blocking files uploaded via the server to any third party portals/destinations
- Tracking of malicious files downloaded to server

Incident Reporting

- Real Time Alerts to the administrator for any sensitive activities occurring on the server
- Daily Cyber Intelligence reporting with summarized information of the sensitive activities
- Detailed view of the incidents along with forensics reports
- Provision to detect and audit sensitive events occurring in offline mode or off office hours

Additional Features

- Stealth mode helping in monitoring employees in an invisible manner
- Offline policies and monitoring ensuring the malicious activities are captured and synchronized with the server when connected to internet
- Temporary Policies for uplifting the user privileges for a defined duration
- Customization of the report that will be generated can be done as per admin requirements
- Tamper Proof and password-protected uninstall
- Easy extraction of analytics and logs via PDF Reports features
- Central management of agent version upgrades via server dashboard

Integrated Solution Architecture

Data Resolve's inDefend-SAM supports hybrid hosting models

O n - C l o u d

In this model, the server is hosted on cloud so no additional hardware procurement is needed and all the machines directly communicate with the server via any internet connectivity. And its dashboard can be accessed 24*7 across the globe.

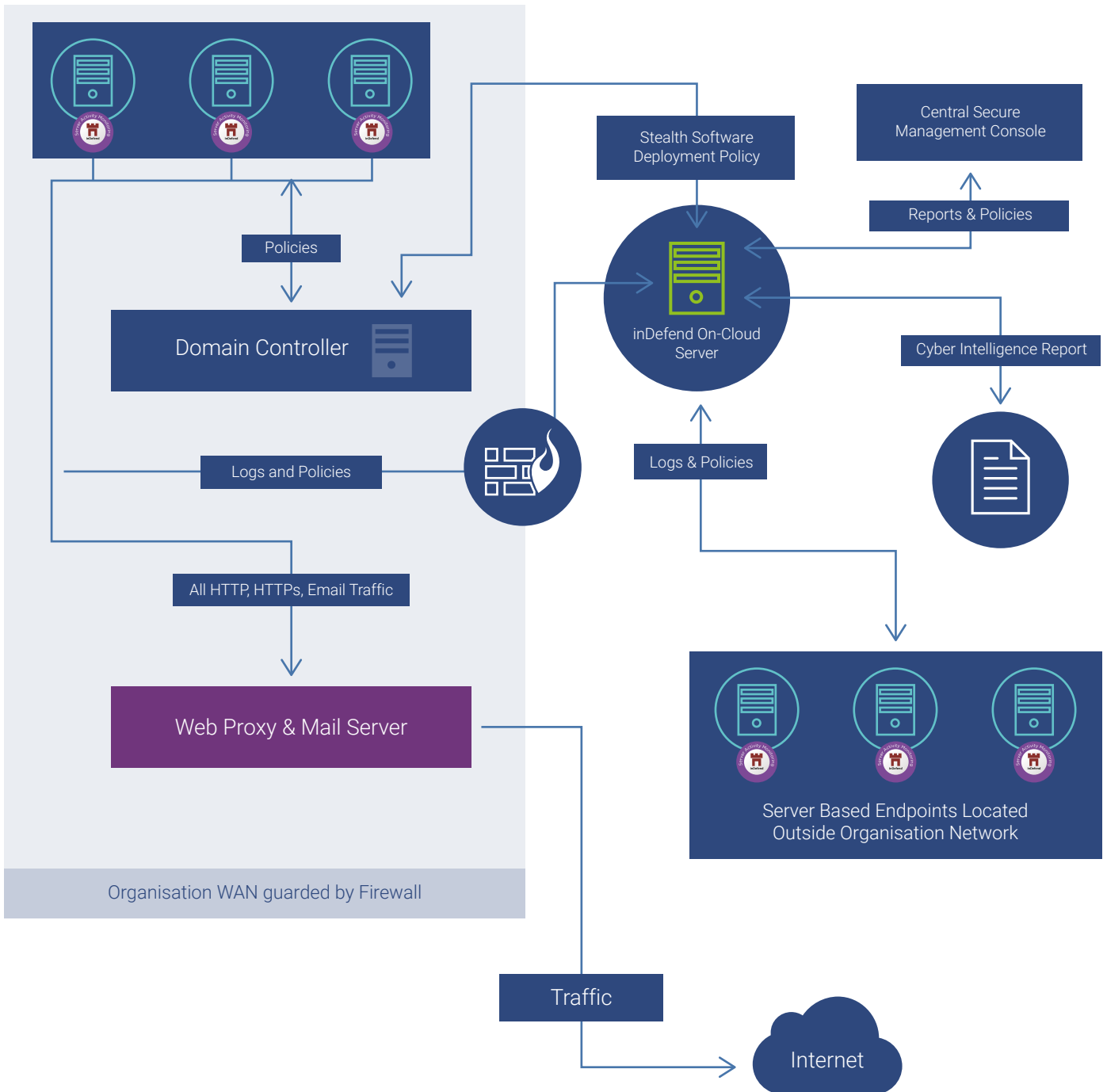


Figure 1.0: On-Cloud Network Topology For inDefend-SAM

O n - P r e m i s e

In this model, the server is hosted within the organizational network and dashboard is accessible from within the company WAN.

In this model, end points are connected to the inDefend-SAM server via the server's internal IP address. Connectivity of remote end points with the inDefend-SAM server can be managed with the public IP address based port forwarding.

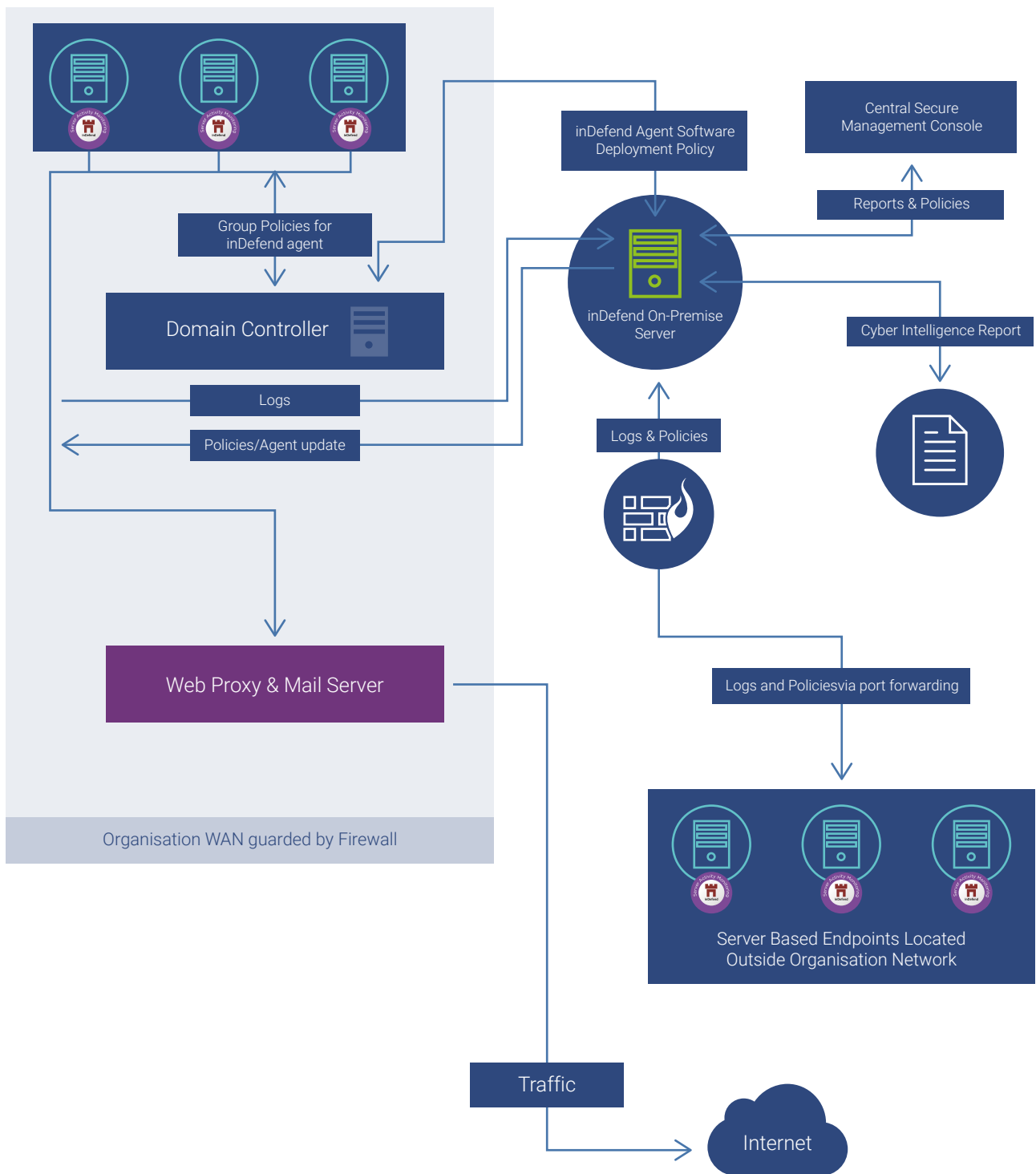


Figure 1.1: On-Premise Network Topology For inDefend-SAM

System Requirements

inDefend-SAM Server Requirements

The configuration of the inDefend-SAM server depends on the number of systems you need to protect. For example, an organization with up to 300 systems to be protected can be supported by a dedicated server computer with:

Platform Supported

- Windows Server 2008
- Windows Server 2012

Linux (64 bit) flavors of the following distributions

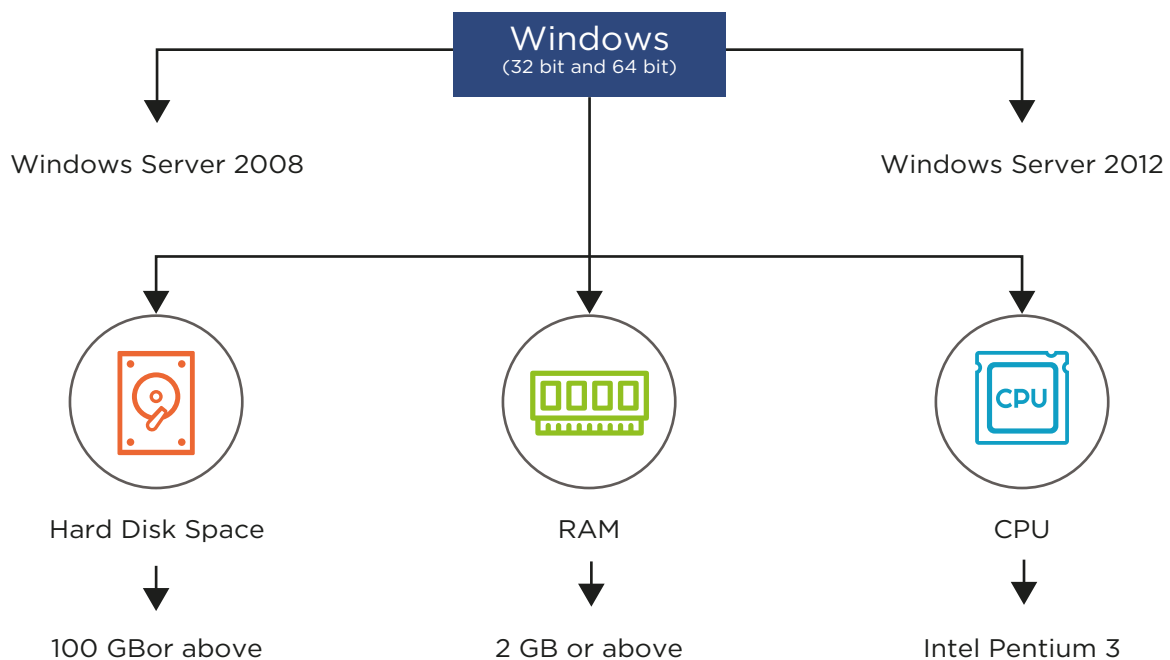
- RHEL – 7.x or above
- CentOS – 7.x or above
- Ubuntu – 14.x or above

RAM- 8 GB

Hard Disk Space- 900 GB or above

CPU- Intel Xeon 3.3.ghz 4 core

End Point System Requirements



Key Benefits

- A 360 degree view to monitor your server activities
- Insights about the access levels granted to your administrators
- Security of the business critical data from insider threats
- Provision to audit and monitor administrators set of activities across the organizational servers
- Comprehensive framework of incidents and analytics reporting



Data **Resolve**

*Terms and conditions are applicable on the features as mentioned in this document. For any clarification, please connect with team Data Resolve

CLOUD PARTNERS



* All logos used are copyrights of the respective owners

DISTRIBUTED
IN INDIA BY



BD SOFTWARE
DISTRIBUTION
PVT. LTD.

SALES : +91 8291601105
EMAIL : sales@bdsoft.in