



invisiron®
sentry S-6000



invisiron® sentry S-6000

Super Charged Defence System

Invisiron® Sentry S-6000 is built for large networks and data centres. Supports up to 2 x 10GB ports and copper as well as fibre-optic connections.

Key Features

Automatic Threat Mitigation

Invisiron® offers a pro-active Cyber Defence platform with auto threat mitigation.

DDoS Protection¹

We are able to mitigate both volumetric and protocol-based DDoS attacks.

Advanced Threat Protection

Our device protects your organisation against advanced persistent threats and many other attacks and malware.

DNS Security (Data Exfiltration)²

Our DNS threat analytics ruleset is able to detect and automatically block data exfiltration attempts via DNS.

Cyber Threat Intelligence (Invisiron-CTI™)

Invisiron-CTI™ comes from over 30 globally validated sources, which are updated and pushed down to every Invisiron® device every hour, automatically.

Threat Commander Remote Monitoring Utility

Every malicious packet that is mitigated by Invisiron® can be reviewed in our Remote Monitoring System and allows our Managed Detection and Response (MDR) teams to perform forensics on compromised assets.

High Availability

Invisiron® devices support High Availability.

¹ Only Applicable to S-6000DDoS

² Only Applicable to S-6000DNS

Bi-Directional Deep Packet Inspection (DPI)

Our powerful DPI engine is capable of inspecting a packet down to a single byte level for both incoming and outgoing Internet traffic.

Invisible Stealth Mode

Invisiron® devices do not require a MAC or IP address to operate. Hackers will not be able to detect the presence of an Invisiron device in a network.

Ultra-Fast In-Line Packet Processing Speed

Packets are processed at near line speed without degradation of your Internet bandwidth.

No Changes to Existing Network Infrastructure

A plug-and-play complete Cyber Defence solution, without having the need to make any changes to existing IT infrastructure networks.

Geo IP Blocking

Invisiron® devices are able to block network connections based on geographical locations and countries.

LAN IP Isolation

Proactively isolates suspicious LAN IPs using a machine learning algorithm.

Designed for Large Enterprises & Data Centres



Technical Specifications

Processor	Intel Xeon
Memory	8 GB of DDR4 memory
Storage	HPE Dynamic Smart Array configured in disk mirroring mode
Disk Drives	2x 1 TB low form factor SATA disk drives
Packet Processing	2x 10GB Ethernet ports. High performance Intel NIC with SFP Optical as well as copper SFP modules supported
Management	1GB Ethernet (RJ45) for Management
Power and Cooling	Dual redundant 900W switching power supplies, 100-240 Volt AC High efficient cooling for warm environments
Form Factor	2U (W x D x H) 43,47 x 63.43 x 8.76 cm
Embedded OS	Linux
Cyber Threat Intelligence	Cloud-based Invisiron-CTI™
DPI Rules	Up to 10,000 rules
Reputation Detection	Up to 1,500,000 domain names and URLs
IP Address Filtering	Up to 250,000 IP addresses, both IPv4 and IPv6
DGA Detection	Supported on DNS queries and replies
Configuration	Graphics User Interface over encrypted link
Alerts and Notifications	By Graphical User Interface and E-Mails
Evidence Collection	Packets captured in PCAP data format. Event logging in JSON format
System Upgrades	Software updates provided from the cloud



HAT Distribution

1300 121 215
sales@hatdisti.com

©2020 Invisiron Pte Ltd. All rights reserved.

Cyber 
Defence
Fortified™