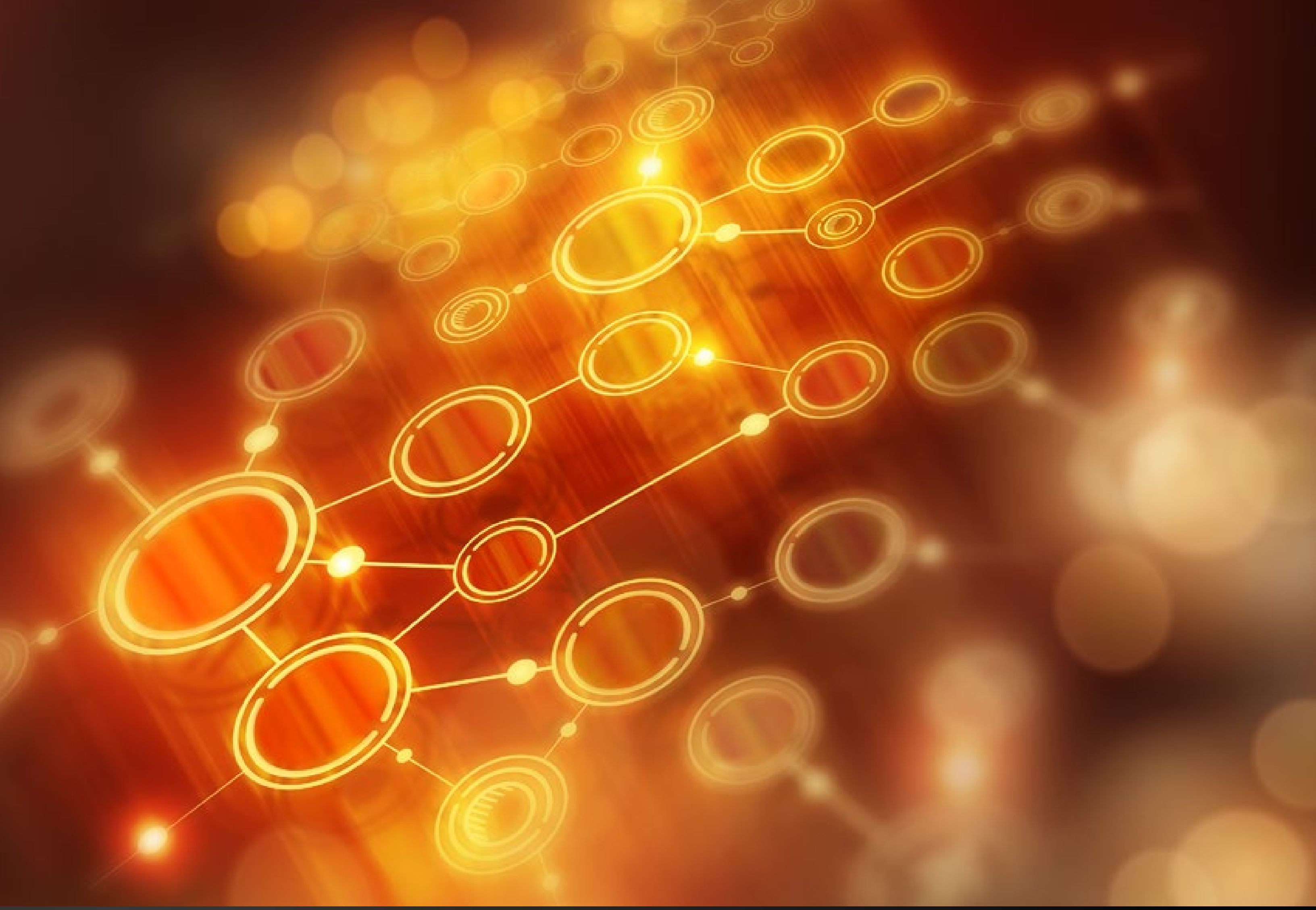

radware

SHARE THIS BROCHURE

in f t g+

MSSP Portal Solution

Service Delivery Platform for DDoS Detection and Mitigation

Managed Security Service Providers (MSSPs) can benefit greatly from technologies that deliver high-value, revenue-generating services. To that end, Radware's MSSP Portal enables Operators and Service Providers to resell cyber security protection capabilities to their customers as managed services.

Radware's Portal for MSSPs is a turnkey, multi-tenant DDoS detection and mitigation service delivery platform that provides reliable, flexible, and scalable cyber security protection. An add-on component to Radware's industry-leading Attack Mitigation System, the Portal collects and aggregates security attack measurements and events (including traffic utilization, attack distribution and alerts), and displays them in real-time and historical reports.

If you are an MSSP looking for a service delivery platform for DDoS detection and mitigation to expand your business, the MSSP Portal is the right solution for you.

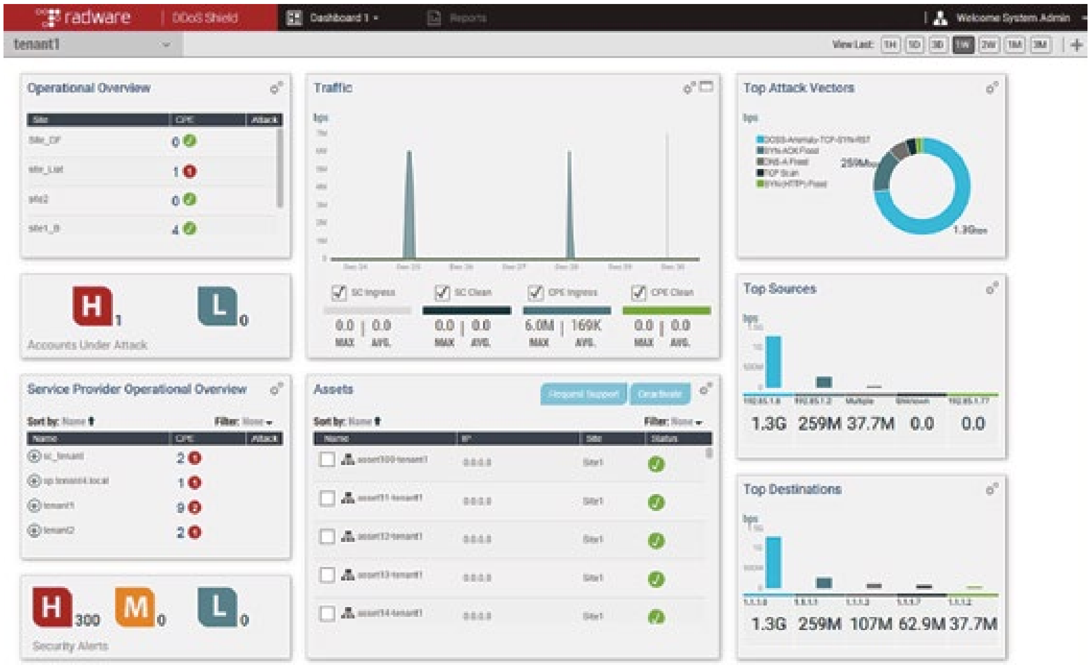

Figure 1: MSSP Portal Dashboard UI

Real-Time Dashboard

The Portal dashboard displays real-time information at the account (tenant) level, in a collection of dynamic, predefined widgets that enable activation/deactivation of traffic diversion to the scrubbing center and displays the service status and statistics of accounts managed by an MSSP. It contains information about all protected assets,their current status, real-time attacks and traffic information.

Each MSSP Portal user can customize and access three dashboards that are persistent; even after logging-out and logging back into the Portal. The dashboards retain their look and settings, on a per-user level.

Widget Repository

The dashboard presents a set of widgets, where the user can personalize which widgets are displayed, how they are displayed (location/size), how the data is rendered (chart type/units/scale) and which data they display (depending in time filter/context/etc.). The widgets have several pre-defined sizes, where each shows a different level of information (e.g. summary, distribution by category, tabular view, etc.).

When changing the dashboard context and date frame, the data on the widgets adjusts accordingly. In addition, several widgets have their own attributes that can override some of the global filters (e.g. selected account, time filter, etc.).

Widgets can be displayed depending on the logged-in user role. The following table describes the available widgets and access level.

Widget Name	Description	Access Level
Security Status	Displays whether the account is under attack or not	Account, Service Provider, Operator
Assets	Displays a list of account’s assets, their containing sites and status, and enables activation/deactivation of traffic diversion to the scrubbing center	Account, Service Provider, Operator
Operational Overview	Displays the CPE and attack status per accounts sites	Account, Service Provider, Operator
Top Attacks	Displays top attacks by sources /destination/vectors	Account, Service Provider, Operator
Traffic Monitor	Displays incoming and clean traffic utilization per CPE and SE	Account, Service Provider, Operator
Security Alerts	Displays a list of security alerts reported by the security devices	Account, Service Provider, Operator
Operational Alerts	Displays operational alerts such as CPE status change, etc.	Account, Service Provider, Operator
Accounts Under Attack	Displays a list of attacks on respective account and assets, across the entire portal accounts	Service Provider, Operator
Service Provider Operational Overview	Displays a list of accounts and their CPE and attack status, across the entire portal accounts	Service Provider, Operator

Reports

The reporting section allows users to define and run ad hoc reports, and then schedule, export and email them.Report templates can be saved, loaded and executed to generate reports with fresh data. Users can define complex reporting criteria using the report’s criteria panes, enabling operators to automate routine tasks. For example, users can automatically generate a monthly summary of DDoS protection service usage per each account, and receive an email summary report.

Flexible User and Entity Models

The MSSP Portal provides the flexibility and ease-of-use required to deploy, manage and secure multi-tenant accounts, securing networks from the inside out - from the enterprise core to the perimeter, and remote sites. The Portal Persona (user types) represents one or more user accounts that can be defined for each of the following personas.

- **Operator** - owns and manages the Portal infrastructure with access to all tenants and administration tasks
- **Service Provider** - an optional tier of users that can directly offer the Portal to end-customers, and manage one or more tenants
- **Account** - a tenant, representing a customer that uses the DDoS protection service. An account contains a set of sites and assets, where:
- **Site** - a logical container for a set of assets (such as geographically-based, customer SLA-based,or service groups)
- **Asset** - an entity to be protected by the MSSP Portal (including networks, servers, subnets, or set of subnets)

The MSSP Portal Components

The MSSP Portal supports virtual IT environments, and is a fully integrated solution that encompasses behavioral-based attack mitigation, DDoS attack detection and prevention, and centralized attack management, monitoring and reporting.

- **MSSP Portal** - deployed in the Operator or Service Provider’s data center as a virtual appliance supporting VMware or KVM hypervisors
- **DefensePro** - a real-time, behavioral-based attack mitigation device that protects infrastructure against network and application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft, and other emerging cyber attacks
- **DefenseFlow** - a network-wide DDoS attack detection and cyber command and control application designed to protect networks against known and emerging network attacks that threaten network resource availability
- **APSolute Vision** - a centralized attack management, monitoring and reporting solution across multiple DefensePro and DefenseFlow devices and locations. It provides user real-time identification, prioritization, and response to policy breaches, cyber attacks and insider threats
- **Additional Cloud Scrubbing** (e.g. Radware’s Cloud DDoS Protection Service) can be used for Peak Protection

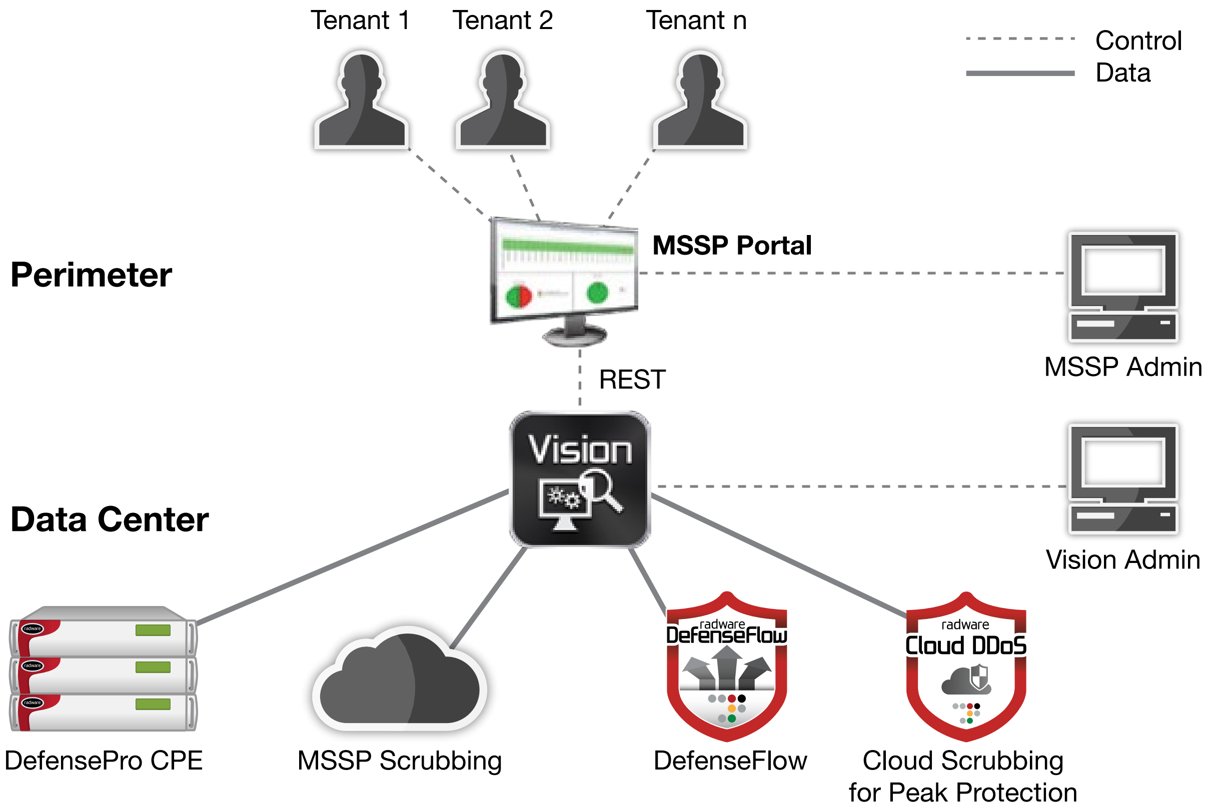

Figure 2: MSSP Portal Architecture Diagram

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency.

Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube and the Radware Connect app for iPhone®.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.