RioRey rVM

Comprehensive DDoS Defense Meets the Economies of Virtualization

rVM Benefits

Intelligent, full-spectrum DDoS protection for virtualized environments.

Automatic DDoS detection and mitigation.

Rich reporting, visibility and control over your mitigation.

Proven analytics platform for network, transport and application-layer DDoS.

1, 5, 10, 40 or 100Gbps VM filtering.

Monthly subscription based sales models.

Supported Hypervisors: KVM and VMWare.

Rapid implementation, delivering immediate DDoS defense where and when needed.

Centralized management and reporting across all RioRey appliances, virtual and physical.

The RioRey Virtual Machine

Recognizing the wide-reaching benefits of virtualized infrastructure, RioRey offers its comprehensive DDoS mitigation appliance as a virtual machine. The RioRey rVM complements server virtualization strategies while providing the same intelligent, multi-layer protection against the full spectrum of DDoS threats, from massive floods to advanced, application-layer attacks as our hardware solutions. The RioRey rVM gives network administrators the flexibility to deploy DDoS defenses when and where necessary, and the agility to adapt quickly as deployment strategies and requirements evolve.

High quality DDoS mitigation hardware deployments historically have required capital investments, while the alternative virtualized options have been based upon different or stripped down version of the underlying software or often a different non-dedicated DDoS solution entirely. The RioRey rVM uses the exact same RIOS filtering software for our VM solutions as is deployed in our provider grade DDoS hardware. Combined with our monthly subscription sales model, the rVM lowers the barrier to entry and term commitment of top tier DDoS protection for enterprise, MSSPs, and SMB. Organizations with costly cloud scrubbing contracts that include limited scrubbing instances and potentially large bills if caps are exceeded can stabilize their costs, have fine grained visibility and controls by deploying the rVM as the on-prem portion of a hybrid solution. This allows clients to contain layer 7 attacks and smaller floods locale, only sending traffic to expensive cloud scrubbing services when the attacks are very large.

RioRey's Full-Function DDoS Mitigation

RioRey rVM extends to virtual environments the same mature, analytics-driven, multi-layer DDoS detection and mitigation capabilities of our physical DDoS appliances. Our solutions utilize a rich set of detection and mitigation algorithms based on their underlying methodology as outlined in our comprehensive taxonomy of known DDoS attack classes. Our DDoS mitigation is free of reliance on threat intelligence feeds, signatures of names attack tools, or maintaining ever changing blacklists, all which become quickly outdated. By concentrating on the underlying methodologies that all attacks utilize, we change the notion of what constitutes a "zero day" DDoS and are able to keep ahead of attacker innovation much better than traditional defenses. Our embedded intelligence enables RioRey DDoS defense solutions to immediately and systematically analyze monitored traffic against known attack techniques and

RioRey, Inc.
4302 East-West Highway
Bethesda, Maryland 20874

U.S.:
1.877.4997.0331

International:
1.240.497.0330

Email:
sales@riorey.com

Web:
www.riorey.com

behaviors, automatically filtering attack traffic with precision without compromising legitimate flows. RioRey's software-defined mitigation approach further enables rapid adaptation to emerging DDoS threats, whether large-scale volumetric or sophisticated multi-vector attacks.

Centralized Management and Reporting

RioRey also offers its powerful ***rWeb*** centralized management system as either a virtual machine or hardware-based platform. Whether VM or device-based, ***rWeb*** delivers unified, multi-tenant management and reporting across all RioRey appliances, both physical and virtual, providing the ultimate deployment model flexibility. RioRey's ***rWeb*** enables network or security staff to establish distinct, isolated customers and zones for both mitigation control and reporting. ***rWeb***'s granular reporting capabilities offer visibility at the network, customer, and zone level, providing real-time and historic traffic data and statistics to support DDoS attack analysis as well as billing and detailed customer reporting. A robust API extends the system's functionality and visibility to third-party applications.

Technical Specifications

Supported Hypervisors	KVM, VMware ESX/ESXi				
	rVM-1	**rVM-5**	**rVM-10**	**rVM-40**	**rVM-100**
vCPU Support (Minimum / Optimum)	3 / 4	3 / 5	7 / 9	21 / 25	30 / 32
Supported Network Interface Types (Gbps)	1 / 10	10 / 40	10 / 40 / 100	40 / 100	40 / 100
Memory Requirements	13 GiB	18 GiB	24 GiB	82 GiB	120Gib
Storage Requirements	4 GB	4 GB	4 GB	4 GB	4 GB
Unlimited User License	Yes	Yes	Yes	Yes	Yes
System Performance					
Packet Throughput PPS	Up to 1.5 million	Up to 3 million	Up to 5 million	Up to 24 million	Up to 50 million
Bandwidth Throughput	1 Gbps	5 Gbps	10 Gbps	40Gbps	100 Gbps
VLAN Support 802.1q	Inspects IP payload inside VLAN tags. QinQ supported				
GRE Tunnel (Pass-through)	Inspects IP payload inside GRE tunnels; tunnel headers are ignored				
Jumbo Frames	Supported, up to MTU of 9000 Bytes (subject to NIC or driver limitations)				
Maximum Simultaneous Victim IPs	Layer 4: 256 (TCP), 256 (UDP), 256 (ICMP), Layer 3/7: 16,384				
Concurrent Sessions (TCP)	4 million per interface	8 million per interface	16 million per interface	64 million per interface	100 million per interface
New Sessions/Second (TCP)	1.5 million per interface	3 million per interface	4 million per interface	16 million per interface	24 million per interface
Detection Time Frame	DDoS detection and mitigation time is typically 0 - 90 seconds				
Number of Zones	1000				
Number of prefixes	50,000 prefixes				
Source white list	50,000				
Source black list	100,000				