RIOREY
THE DDOS SPECIALIST®

# Dedicated DDoS Protection

## When downtime is not a risk you can take.

Two popular gaming networks go down at the height of the holidays, suspending play for two days. A massive attack hits a DNS hosting provider on Cyber Monday, cutting access to thousands of customer sites. These are the high-profile cases that make headlines. But dedicated denial of service (DDoS) attacks compromise networks, web sites, and data centers every day. And the attacks continue to grow – in frequency, severity, and sophistication.

Designed to render network resources, information, or services unavailable to legitimate users, DDoS events threaten any organization that relies on its online presence or online operations. And the fallout from attacks goes well beyond inconvenience. Even moderate DDoS disruptions can mean lost revenue from online transactions, bloated staff-hours for mitigation and customer support, lost productivity for end users, and damaged credibility for service and hosting providers. According to analysts, DDoS attacks can cost businesses between tens of thousands and millions of dollars per hour.

As DDoS attack vectors become more dogged and sophisticated, conventional defense strategies can't keep pace. Reactively throwing bandwidth and engineers at the problem proves too time consuming, too costly, and ultimately unsustainable. Meanwhile the add-on DDoS capabilities of existing equipment (DNS servers, routers, firewalls, load-balancing devices) provide only porous protection. They are too quickly overrun by high-volume attacks and too frequently outwitted by more complex ones. Even slow packet DDoS attacks can overwhelm or dodge patchwork defenses, ultimately depleting resources and bringing down services. Neutralizing the expanding DDoS threat requires dedicated solutions that can rapidly stop attack traffic, preserve legitimate traffic, and adapt to the evolving profiles of emerging DDoS strikes. RioRey consistently delivers on all three fronts.

# Setting the Standard for DDoS Protection

For nearly a decade, RioRey has armed network operators large and small with comprehensive, automated DDoS defense systems that isolate attacks with precision and stop attacks before they can impede business operations, productivity, and security. As DDoS specialists from the outset, we developed our defense platforms from the ground up to address dedicated denial of service attacks in all their possible permutations. Our DDoS defense systems are analytics-driven, providing intelligent, multi-layer protection against the full spectrum of today's DDoS threats, from massive floods that overwhelm network resources to stealthy Layer 7 "surgical" attacks. Easy to deploy and manage, and available as both virtualized and physical device-based appliances, RioRey's dedicated DDoS solutions meet the most rigorous security requirements of enterprises, government agencies, service and hosting providers, and telcos.

## The Science of DDoS Detection

With Internet-based attacks designed to resemble any variety of legitimate traffic, effective defense requires a high level of inherent intelligence to recognize and thwart all types of strikes, whether TCP-based, TCP HTTP-based, UDP-based, or ICMP-based. That's why RioRey approaches DDoS protection as a science. Underpinning our mitigation platform is RioRey's comprehensive taxonomy of known DDoS attack classes. Based on this detailed conceptual model of current attack types, RioRey has derived a full set of defense analytics by which our appliance measures the characteristics and behaviors of IP traffic flows. Focusing on protocols, attack techniques, and traffic behavior rather than on the signatures of individual attack tools, RioRey rapidly identifies and responds to all DDoS threats, immediately and automatically filtering attack traffic while sustaining full access for legitimate users.

RIOREY THE DDOS SPECIALIST

## Taxonomy of DDoS Attacks

| | | Attack Types | Attack Matrix Dimensions | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Nature of IP | Handshake | Source IP Range | Packet Rate | Packet Size | Packet Content | Fragmenting | Session Rate | Session Duration | VERB Rate |
| TCP BASED | 1 | SYN Flood | Spoofed | None | Large | High | Small | --- | --- | --- | --- | --- |
| | 2 | SYN-ACK Flood | Spoofed | None | Large | High | --- | --- | --- | --- | --- | --- |
| | 3 | ACK & PUSH ACK Flood | Spoofed | None | Large | High | --- | --- | --- | --- | --- | --- |
| | 4 | Fragmented ACK | Spoofed | None | Large | Moderate | Large | --- | High | --- | --- | --- |
| | 5 | RST or FIN Flood | Spoofed | None | Large | High | --- | --- | --- | --- | --- | --- |
| | 6 | Synonymous IP | Spoofed | None | Single IP | High | --- | --- | --- | --- | --- | --- |
| | 7 | Fake Session | Spoofed | None | Large | Low | --- | --- | --- | --- | --- | --- |
| | 8 | Session Attack | Non-Spoofed | Yes | Small | Low | --- | --- | --- | Low | Long | --- |
| | 9 | Misused Application | Non-Spoofed | Yes | Small | Variable | --- | --- | --- | High | Short | --- |
| TCP HTTP BASED | 10 | HTTP Fragmentation | Non-Spoofed | Yes | Small | Very Low | Small | Valid | High | Very Low | Very Long | Very Low |
| | 11 | Excessive VERB | Non-Spoofed | Yes | Small | High | --- | Valid | --- | High | Short | High |
| | 12 | Excessive VERB Single Session | Non-Spoofed | Yes | Small | Low | --- | Valid | --- | Low | Moderate | High |
| | 13 | Multiple VERB Single Request | Non-Spoofed | Yes | Small | Very Low | Large | Valid | --- | Low | Long | High |
| | 14 | Recursive GET | Non-Spoofed | Yes | Small | Low | --- | Valid | --- | Low | Short | Low |
| | 15 | Random Recursive GET | Non-Spoofed | Yes | Small | Low | --- | Valid | --- | Low | Short | Low |
| | 16 | Faulty Application | Non-Spoofed | Yes | Small | Low | --- | Valid | --- | Low | Short | Low |
| UDP BASED | 17 | UDP Flood | Spoofed | --- | Very Large | Very High | Small | Not Valid | --- | --- | --- | --- |
| | 18 | Fragmentation | Spoofed | --- | Moderate | Very High | Large | Not Valid | High | --- | --- | --- |
| | 19 | DNS Flood | Spoofed | --- | Very Large | Very High | Small | Valid | --- | --- | --- | --- |
| | 20 | VoIP Flood | Spoofed | --- | Very Large | Very High | Small | Valid | --- | --- | --- | --- |
| | 21 | Media Data Flood | Spoofed | --- | Very Large | Very High | Moderate | Valid | --- | --- | --- | --- |
| | 22 | Non-Spoofed UDP Flood | Non-Spoofed | --- | Small | Very High | --- | Valid | --- | --- | --- | --- |
| ICMP BASED | 23 | ICMP Flood | Spoofed | --- | Very Large | Very High | Variable | Not Valid | --- | --- | --- | --- |
| | 24 | Fragmentation | Spoofed | --- | Moderate | Very High | Large | Not Valid | High | --- | --- | --- |
| | 25 | Ping Flood | Spoofed | --- | Very Large | Very High | Small | Valid | --- | --- | --- | --- |

***RioRey's Taxonomy is an industry standard for DDoS classification.***

## The Power of Defense Analytics

DDoS defense is by its nature two-pronged, tasked with keeping malicious traffic off the network and legitimate traffic on. So accurate threat detection is vital. False positives (and false negatives) prove as disruptive as the attacks themselves. RioRey's intelligent, algorithmic-based solutions are the most effective at distinguishing and separating attack traffic from legitimate flows, minimizing the impact of DDoS events – on your network, on your customers, and on your business.

**RioRey DDoS Protection:**
Analytics-driven, Software-defined

*Comprehensive, proactive defense against all known and emerging classes of DDoS attacks.*

*Automated, "always-on" detection and mitigation, minimizing analyst intervention.*

*Virtualized and device-based solutions for flexible and scalable deployments.*

*Common software and defense analytics across RioRey product line, providing full-spectrum protection for all deployment models.*

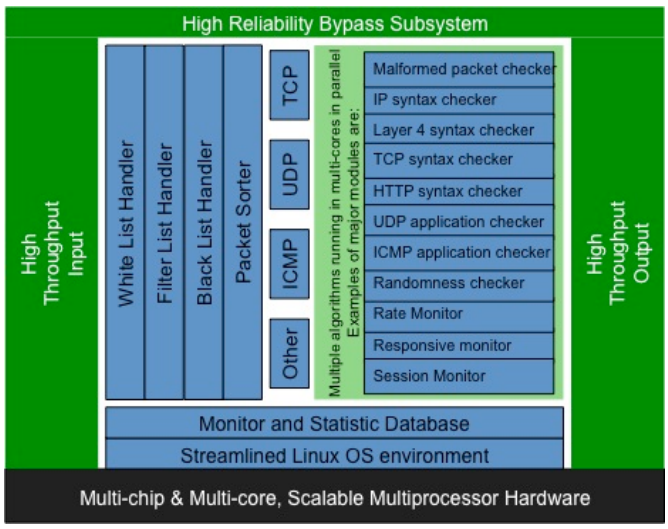
*Rapid deployment and immediate protection, requiring no signatures, rules, or waiting.*

*Unified, multi-tenant management across multiple RIOS instances and platforms.*

RioRey's solutions feature mature and comprehensive DDoS defense analytics, enabling the system to rapidly examine underlying attack methodologies rather than rely on traffic base-lining and reactive signature updates. The result is a high-performance defense appliance that deploys rapidly, defends immediately, and provides "always-on" protection, accurately detecting and mitigating both network and application attacks with minimal manual intervention.

## The Value of Software-Defined Mitigation

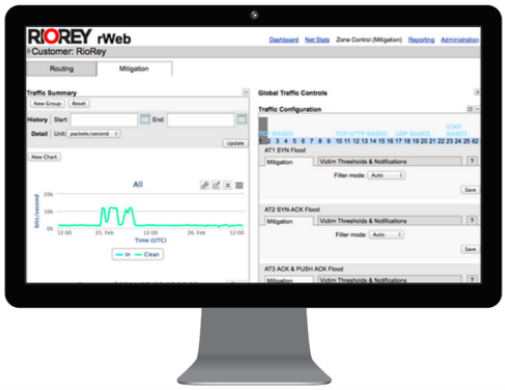
RioRey's DDoS defense solutions are software-based, enabling maximum deployment flexibility and scalability. This software-defined mitigation (SDM) approach means that each RioRey platform shares common software and delivers the same intelligent, full-spectrum DDoS protection regardless of appliance model or defense configuration, allowing customers to easily scale, port, and adjust as their networks and needs evolve. Because RioRey's platforms are software-defined and analytics-driven, they also adapt rapidly and seamlessly to emerging DDoS threats. Our widely deployed products range in throughput from 100Mbps to 200Gbps, protecting a wide range of customers, from small enterprises and hosting providers to large multi-nationals and telcos.




**The RioRey RIOS Architecture**

For optimal flexibility and efficiency, RioRey also offers RioRey VM, a virtualized version of our proven DDoS mitigation system that extends the full capabilities of our industry-leading DDoS defense analytics to virtual environments and cloud-based infrastructures. RioRey VM's flexible licensing options and portability facilitate custom and easily adaptable deployment models. The RioRey Virtual Machine works in conjunction with physical RioRey appliances for hybrid deployments, with our intuitive, web-based interface simplifying and unifying management across all RioRey platforms and instances.

## Superior Visibility and Control




RioRey ***rWeb*** provides unified, multi-tenant management and reporting across all RioRey appliances, both physical and virtual. Through ***rWeb***'s powerful, intuitive interface, system administrators can easily establish distinct customers and zones for both mitigation control and reporting, not only enabling customer and service isolation but also facilitating incremental service revenue opportunities. ***rWeb***'s comprehensive and granular reporting capabilities deliver superior 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 makes ***rWeb***'s extensive functionality and visibility easily available to third-party applications.

## RioRey: The DDoS Specialist

Since its founding in 2006, RioRey has focused on developing dedicated, high-performance DDoS defense systems for networks and data centers of all sizes. RioRey's analytics-driven solutions provide automated DDoS detection and mitigation, protecting e-commerce, finance, government agency, hosting, gaming, and entertainment networks and services around the globe. Thousands of companies rely on specialized DDoS protection from RioRey. The company offers both on-premises and virtualized, cloud-based solutions, enabling flexible and scalable deployments that meet customers' unique and evolving security requirements. Headquartered in Bethesda, Maryland, RioRey supplies and services its DDoS solutions throughout North America, EMEA, and Asia.

**RioRey, Inc.**, 4302 East-West Highway, Bethesda, Maryland 20874 U.S.: 1.877.497.0331
www.riorey.com sales@riorey.com International: 1.240.497.0330