



## DATA SHEET

# CISCO GUARD XT 5650



## PRODUCT OVERVIEW

The Cisco® Guard XT 5650 DDoS Mitigation Appliance from Cisco Systems® delivers a powerful and extensive distributed denial-of-service (DDoS) protection system. Designed to meet the performance and scalability requirements of the largest and most demanding enterprise environments, the Cisco Guard XT provides unprecedented levels of protection against today's increasingly complex and elusive attacks.

Featuring two Gigabit Ethernet interfaces, a single Cisco Guard XT can process attack traffic at line rates as high as a full gigabit-per-second (Gbps). Working together, multiple Cisco Guard XTs can incrementally scale to support multi-gigabit rates, delivering an extensible solution that easily adapts to large and growing enterprise environments.

## DDoS Attacks Evolving

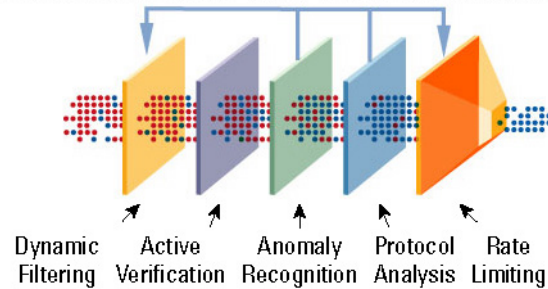
Today's DDoS attacks are more malicious, more virulent, more destructive, and more focused than ever. Launched by disgruntled users or unscrupulous businesses targeting specific sites or competitors, these attacks easily elude and overwhelm the most common defenses. Composed of legitimate-appearing requests, massive numbers of "zombies" and spoofed identities that make it virtually impossible to identify and block these malicious flows, DDoS attacks literally paralyze their victims and prevent them from conducting business, costing billions of dollars per year in lost revenue.

The Cisco Guard XT defends against this new wave of DDoS attacks, enabling businesses to defeat these attacks without compromising their mission-critical and revenue-bearing operations. Based on a unique multiverification process (MVP) architecture, the Cisco Guard XT employs the most advanced anomaly recognition, source verification, and anti-spoofing technologies to identify and block individual attack flows while allowing legitimate transactions to pass. Combined with an intuitive, graphical user interface (GUI) and extensive multilevel monitoring and reporting designed to provide a comprehensive overview of all attack activity, the Cisco Guard XT delivers robust and comprehensive DDoS defense for protecting business operations.

**Figure 1**

The Cisco Guard XT MVP Architecture

Anomaly Recognition and Protocol Analysis Update the Dynamic Filtering and Rate Limiting Modules in Real-Time to Block Newly Identified Attack Traffic



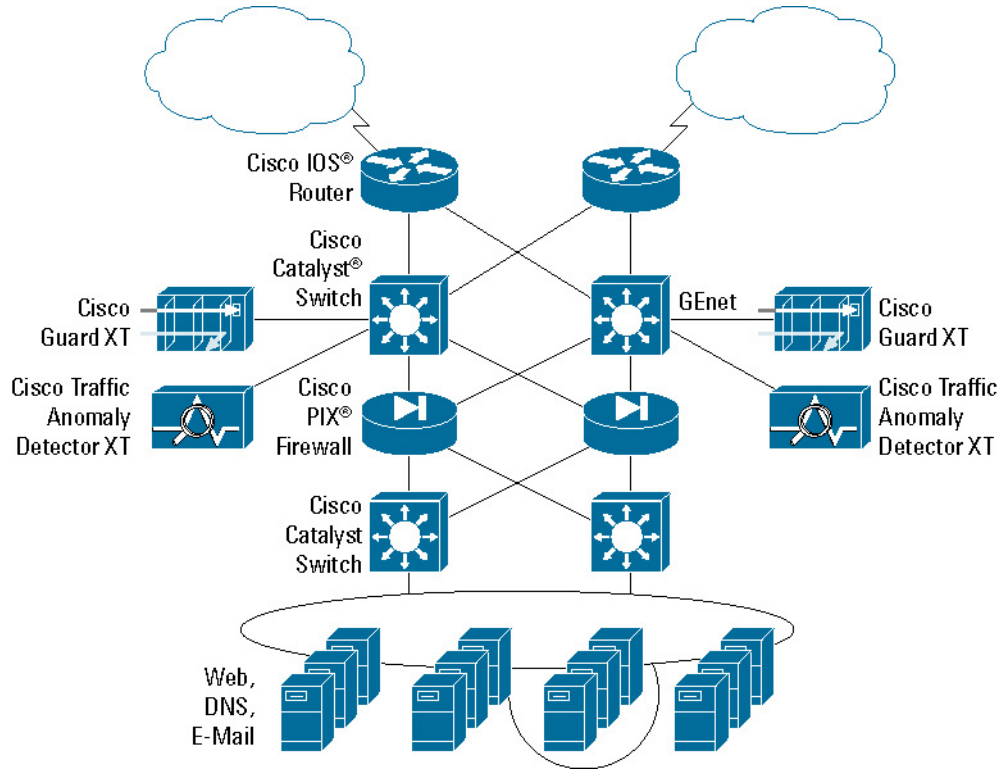
## APPLICATIONS

The Cisco Guard XT is one part of a complete detection and mitigation solution that protects enterprises, hosting centers, government agencies, and service provider environments from DDoS attacks. Combined with the Cisco Traffic Anomaly Detector XT, which detects the presence of DDoS, worm, and other attacks, the Cisco Guard XT performs the detailed per-flow level attack analysis, identification and mitigation services required to block attack traffic and prevent it from disrupting network operations.

When the Cisco Traffic Anomaly Detector XT identifies a potential attack, it alerts the Cisco Guard XT to begin diverting traffic destined for the targeted devices—and only that traffic—for inspection. All other traffic continues to flow freely, reducing the impact on overall business operations while increasing the number of devices or zones a single Cisco Guard XT can protect.

Diverted traffic is rerouted through the Cisco Guard XT, which is typically deployed off the critical path at any point in the network—from enterprise entrance access points to peering points off an ISP backbone. The diverted traffic is subjected to intense scrutiny to identify and separate “bad” flows from legitimate transactions. Specific attack packets are identified and removed, while legitimate traffic is forwarded to its original destination, ensuring that real users and real transactions always get through, and guaranteeing maximum availability.

Figure 2



## KEY FEATURES AND BENEFITS

### Multistage Verification

The Cisco Guard XT performs detailed, granular, per-flow analysis and blocking to stop attack traffic with surgical precision—while allowing legitimate transactions to flow freely.

The innovative blocking techniques are based on the MVP architecture, developed by Cisco Systems, which delivers multiple interactive layers of defense to identify and block all types of attacks with extreme accuracy. Integrated dynamic filtering and active verification technologies, driven by a sophisticated profile-based anomaly recognition engine, enables rapid, automatic protection against all types of assaults, even Day Zero attacks that have never been seen before. Additional protocol analysis and rate limiting features help ensure only valid traffic gets through, and only in volumes that won't overwhelm downstream devices.

The Cisco Guard XT also features integrated “Zombie Killer” technologies that help identify and block all types and sizes of attacks, including those launched by hundreds of thousands of distributed zombie hosts—one of the most prevalent and difficult-to-stop DDoS attack sources.

## **Multi-Gigabit Performance**

Each Cisco Guard XT features dedicated network processors that support attack analysis and cleaning at full gigabit line rates in standalone mode, defending against large-scale DDoS attacks, including those launched by massively distributed attackers such as compromised zombie hosts.

The Guard XT also supports a unique clustering architecture that supports incremental scaling of both attack processing rates and zombie defense capacities—sufficient for protecting even the largest enterprise and service provider environments against the most serious threats.

Deployed off the critical path as a routing peer to ensure maximum reliability and straight-forward installation, the Cisco Guard XT diverts and cleans only that traffic destined for a targeted zone, enabling cost-effective resource and scaling.

## **Multilevel Monitoring and Reporting**

The Guard XT features an intuitive, Web-based GUI that simplifies the policy definition, operational monitoring, and report generation processes.

Multiple monitoring and reporting levels provide network operators, security administrators, and clients with a wide range of detailed real-time and historical information. Attack reports provide details for individual attacks—including characteristics, lists of identified zombies, and specific enforcement actions used—enabling security experts to review and tune the Cisco Guard XT's security policies.

Meanwhile, customer-level historical summaries enable service providers to easily report on successful protection against the variety, duration and scale of attacks. In addition, an interactive mode allows users to review and approve recommended actions and policies prior to activation, providing manual control over attack responses if desired.

## **SUMMARY**

Designed for service providers, hosting centers, and online enterprises, the Cisco Guard XT can help ensure uninterrupted business operations, even in the face of the most malicious assaults. For users, that translates into a significant competitive advantage by ensuring uncompromised availability and unparalleled protection of the most valuable business assets.

## PRODUCT SPECIFICATIONS

Table 1. Product Specifications

<b>Memory</b>	2 GB DDRAM
<b>Hard Drive</b>	80 GB
<b>Interfaces</b>	Two Gigabit Ethernet Two 100BASE-T (management)
<b>Power Supply</b>	Dual 110-220V, 350W
<b>Weight</b>	62 lbs/28.2 kg
<b>Height</b>	3.36 in. / 8.53 cm
<b>Width</b>	17.5 in. / 44.5 cm
<b>Depth</b>	27.5 in. / 69.9 cm
<b>Rackmountable</b>	Yes
<b>Management</b>	Secure Web-based GUI CLI: Console, Telnet, SSH Cisco (Riverhead) SNMP MIB and MIB II TACACS+ Syslog
<b>Certifications</b>	UL recognized CE FCC Rules Part 15 compliant
<b>Attack Protection</b>	<ul style="list-style-type: none"><li>• Spoofed and non-spoofed attacks<ul style="list-style-type: none"><li>– TCP (syns, syn-acks, acks, fins, fragments)</li><li>– UDP (random port floods, fragments)</li><li>– ICMP (unreachable, echo, fragments)</li><li>– DNS</li></ul></li><li>• Client Attacks<ul style="list-style-type: none"><li>– Inactive and total connections</li><li>– HTTP Get flood</li></ul></li><li>• BGP attacks</li></ul>

## ORDERING INFORMATION

**Table 2.** Ordering Information

Product Name	Part Number	SMARTnet® Number
Cisco Guard XT 5650 with 10/100/1000BASE-T Ethernet Ports, Dual AC Power, RAID	AGXT-5650-GET-A-K9	CON-SNT-AGX5650G
Cisco Guard XT 5650 with 1000BASE-SX Multimode Fiber Optic Ports with LC Connectors, Dual AC Power, RAID	AGXT-5650-MMF-A-K9	CON-SNT-AGX5650M
Cisco Guard XT 5650 MVP-OS R3.0.8 Software	SC-AGXT-3.0.8-K9	

To place an order, visit the [Cisco Ordering Home Page](#).

## TECHNICAL SUPPORT SERVICES

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement
- Cisco Technical Support Services include:
  - Cisco SMARTnet support
  - Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit: [http://www.cisco.com/en/US/products/svcs/ps3034/serv\\_category\\_home.html](http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html)

**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica  
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR  
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico  
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia  
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan  
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, PIX, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R) BG/LW6448 0604