allot

See. Control. Secure.

Use Cases

# E-Commerce

## Enterprise

# INTRODUCTION

This document provides a selection of customer use cases applicable for the e-commerce sector. Each use case describes an individual challenge faced by e-commerce companies along with detailed descriptions of the products available that can be used to mitigate and manage those issues.

Allot's solutions empower you to increase productivity and protect your operations and users against ransomware, Denial-of-Service attacks, and Bot infection. By delivering full visibility and granular control over applications, users, and network utilization, the Allot Secure Service Gateway (SSG) enables you to remove risky applications from your network, control recreational traffic, and most importantly, ensure that your network runs according to your business priorities. In addition, Allot's solutions will reduce the total cost of ownership of your security investment by

*Allot is a leading provider of intelligent IP service optimization solutions that help enterprises and data centers run more efficient networks that better satisfy their users.*

Allot leverages DPI technology to provide a clear and accurate view of network usage. Armed with this valuable insight, IT managers can dynamically control the delivery of critical applications to comply with SLAs, to protect network assets against attack, and to accelerate the Return on Investment (ROI) on their IT infrastructure.

Allot solutions are deployed worldwide in data centers and enterprise networks across a broad range of business sectors including e-commerce, education, energy, utilities, finance, government, healthcare, higher education, hospitality, media and telecom, retail stores, and transportation.

The use cases in this booklet are based on the key benefits that can be obtained directly by an enterprise or through managed services providers. Each case leverages both security and network intelligence capabilities for application, user and device behavior, and control for enterprises to:

- Understand how network resources are consumed before making infrastructure investments
- Define real-time traffic management policies that align performance to business priorities and adjust IP traffic flows dynamically when links are congested
- Define tiered traffic management policies based on individual levels of service for specific user profiles
- Reduce the enterprise attack surface and increase productivity by identifying and blocking risky applications such as anonymizers and peer-to-peer applications
- Control the use of unsanctioned IT applications such as cloud storage and social media
- Increase availability with real-time DDoS protection combined with traffic management to automatically remove DDoS attack traffic within seconds while maintaining maximum Quality of Experience (QoE) for all legitimate and business-critical network services
- Detect and neutralize web threats, phishing, ransomware, quarantine botnets, and malware-infected hosts

## Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

## Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

## Powered by Allot Secure Service Gateway (SSG)

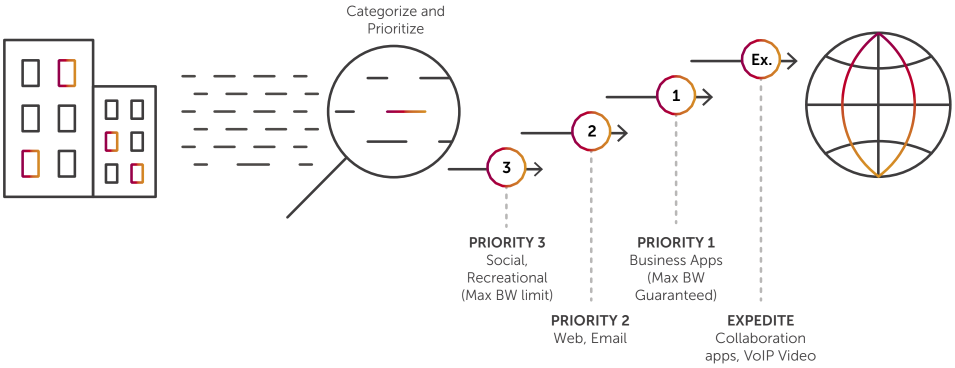
- Allot Gateway Manager
- Allot ClearSee Analytics

E-COMMERCE

# BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes. Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery.

### CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
Ex.
1
2
3
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

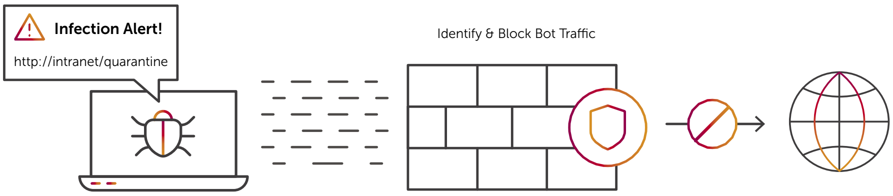
Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

## E-COMMERCE

# REAL-TIME BOT CONTAINMENT

Defend your network against malicious bots by neutralizing malware-infected hosts and spam activity before it adversely affects network performance and integrity. Prevent unintended spam and Internet Protocol (IP)- scanning traffic from eating up valuable bandwidth and quickly identify infected hosts that require cleanup. Allot security solutions monitor connection establishment rates and other symptoms of anomalous user behavior, enabling enterprises to surgically treat the root cause (that is, the malware-infected host) without having to resort to broader measures such as blocking entire subnets, links, or ports. Behavior-based anomaly detection enhances existing security layers with frontline mitigation of bots and other malware.

### INFECTION ALERT



### Key Benefits

- Protect network integrity through the rapid treatment of bot infections
- Ensure business productivity by containing infected hosts
- Reduce help-desk time spent on problems resulting from malware

### Real-time Bot Containment in Action

- Detect anomalous host behavior consistent with malware
- Identify malware through network behavior (mass-DNS, spam-bots, and port scanning)
- Block, limit, or quarantine user traffic within seconds
- Notify user and redirect to clean-up portal

### Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Host Behavior Analysis Engine

## Key Benefits

- Protect data center availability and efficiency
- Ensure data center Service Level Agreements (SLAs) and minimize the risk of outages
- Gain visibility into attackers and their targets in your cloud

## Real-time DDoS Attack Mitigation in Action

- In-line detection and mitigation in seconds, provides immediate remediation for short-lived attacks
- Detects traffic anomaly consistent with DDoS attacks including zero-day attacks-blocked memcached amplification attacks on first instance
- Creates custom signatures to precisely filter attack packets
- Mitigation applied automatically, or upon manual verification
- System issues detailed attack report and statistics

## Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Network Behavior Analysis Engine

# E-COMMERCE
# REAL-TIME DDoS ATTACK MITIGATION

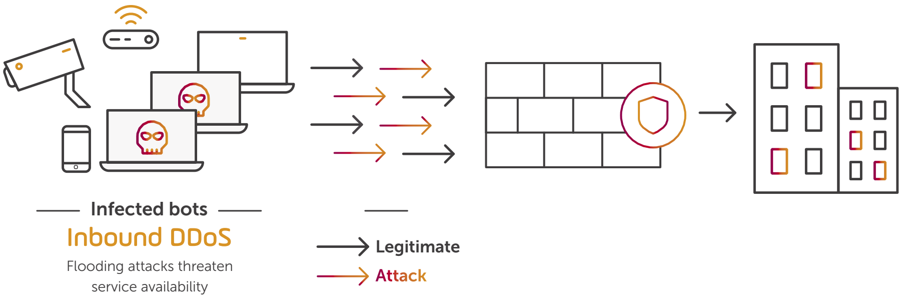
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day business operation and even minutes of downtime can result in significant revenue loss. By combining advanced traffic management with behavioral Distributed Denial of Service (DDoS) detection and mitigation, zero downtime can be achieved even under attack by maintaining critical business applications. In-line DoS/DDoS protection neutralizes flooding attacks within seconds of emergence by rapidly detecting, identifying, and filtering DDoS packets, while enabling legitimate traffic to flow unimpeded.

## DDoS PROTECTION

In-line detection and mitigation blocks attacks in seconds

Protect perimeter devices; Firewalls, IPs and Load Balancers

Assure service availability with dynamic congestion management and critical application prioritization

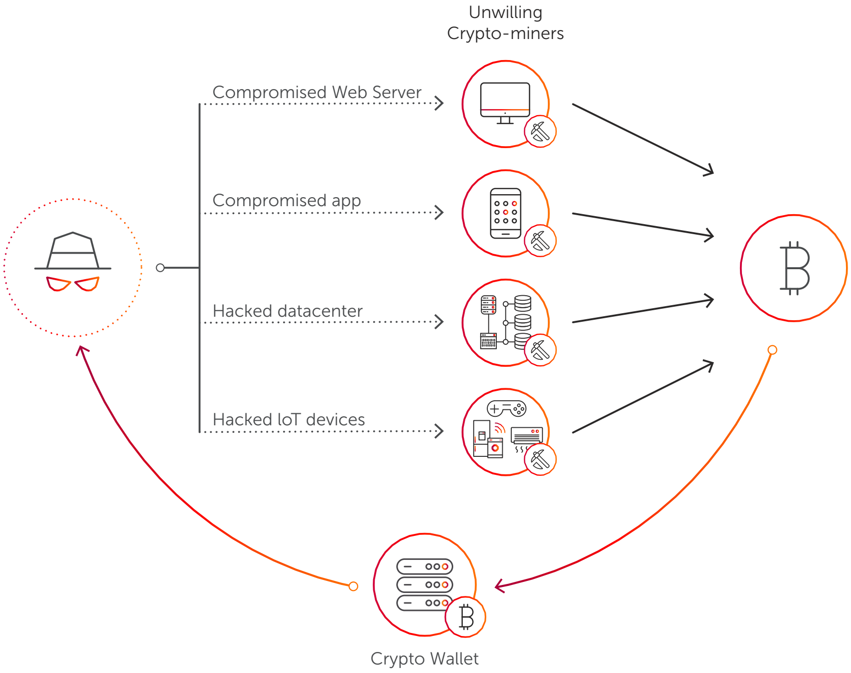


# E-COMMERCE

## CRYPTOJACKING IDENTIFICATION AND MITIGATION

Cryptocurrency hijacking, or "cryptojacking" is one of the key threats Enterprise IT teams are facing today. Cryptomining requires massive amounts of computer processing resources, and cryptojackers are targeting CPU and GPU power located in companies and organizations as a means of mining for free. Network monitoring is certainly the best way to protect against cryptojacking. Cryptojackers must be able to communicate with their targeted servers, receive new hashes, calculate them, and return them to their own servers. Allot's NetworkSecure and Secure Service Gateway can identify this activity and protect valuable enterprise resources from cryptojacking attacks.

### CRYPTO INFECTION ALERT



### Key Benefits

- Isolate Coinhive libraries, which mines the Monero cryptocurrency
- Broad recognition and policy enforcement of cryptomining protocols & applications
- Prevent server resources from being hijacked and impairing business application performance
- Prevent valuable networking hardware from damage through overheating, and saving electricity consumption costs associated with cryptomining

### Cryptojacking Identification and Mitigation in Action

- Identify and block Crypto malware
- Block access to web sites that inject Cryptomining software
- Identify and block Cryptomining protocols
- Identify and block P2P, VPNs, and other applications that enable Cryptojacking attacks

### Powered by Allot Secure Service Gateway (SSG)

- Allot Web Security
- Allot Visibility & Control

# FINAL WORD

The true business of your network is business processes. Bandwidth, throughput, latency, and other common communications metrics are all aspects of evaluating how well your network supports your internal and external processes to conduct business. And sometimes it is your network that is the business.

As demonstrated in the use cases contained in this booklet, Allot SSG provides added value to operations, planning, and your business. All our customers found immediate value the minute they turned on the lights in their networks and actually saw live application, user, and network behavior. In our experience, there is often a misalignment between the way companies think their business processes are working and the way they actually work.

Processes generally underperform for the following reasons:

- The flow of applications that compose the process is broken
- The network is experiencing congestion and other traffic or equipment malfunctions
- Security-related anomalies are impairing or causing denial of service

Network visibility and control solutions can highlight all of these issues in real time and provide the tools to fix them. Your IT team will be able to identify specific protocols and applications, either encrypted or not, and monitor and measure any static or dynamic policy element that you define.

Increased visibility will also provide IT with insights into how to increase network performance. For example, seeing which employees are using what applications and when, you can prioritize access and define traffic management policies that meet your business goals and user expectations and make fully informed decisions about the size and timing of future network investment.

For more information, visit: https://www.allot.com/enterprise