allot
See. Control. Secure.

Use Cases

Media & Telecom

Enterprise

INTRODUCTION

This document provides a selection of customer use cases applicable for the media and telecom sector. Each use case describes an individual challenge faced by media and telecom 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 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 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 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

- Prevent excessive, non-organizational use of a network
- Improve user productivity and satisfaction
- Optimize Internet-link performance

Acceptable Usage Management in Action

- Define acceptable usage tiers and quotas for non-organization-related traffic
- Assign user/department/facility to relevant tiers
- Automatically enforce acceptable usage in real time
- Block the use of inappropriate and risky applications and content on an organization's network

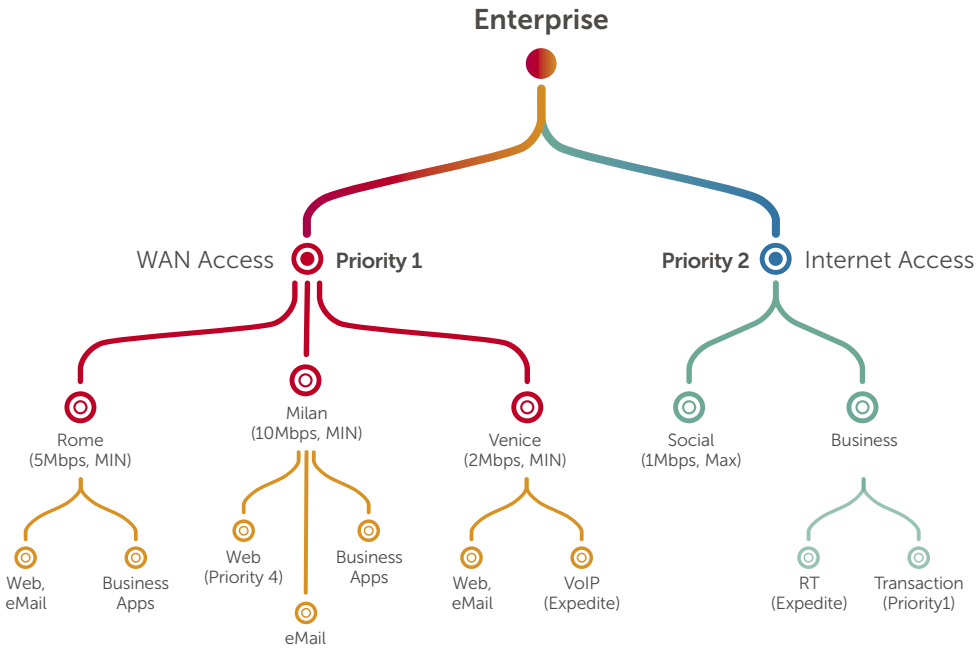
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

MEDIA & TELECOM
ACCEPTABLE USAGE MANAGEMENT

Internet connectivity is essential to the success of all enterprises. Local and national government organizations can manage this resource by establishing an acceptable usage policy that controls the utilization by individual facilities, departments, users, and applications. For example, management would be advised to block P2P downloads of shared content with applications such as BitTorrent because they consume bandwidth, may be used to export valuable corporate information, and invite malware into a network. In addition, the organization may limit access or assign quotas to social networks during business hours, and prioritize business applications over other Internet traffic. Through acceptable usage rules, governmental organizations can prevent individuals and applications from monopolizing Internet bandwidth, ensure quality of service for all users, and minimize non-business Internet activity to improve productivity and postpone costly infrastructure investments.

TRAFFIC MANAGEMENT & ACCEPTABLE USE POLICY

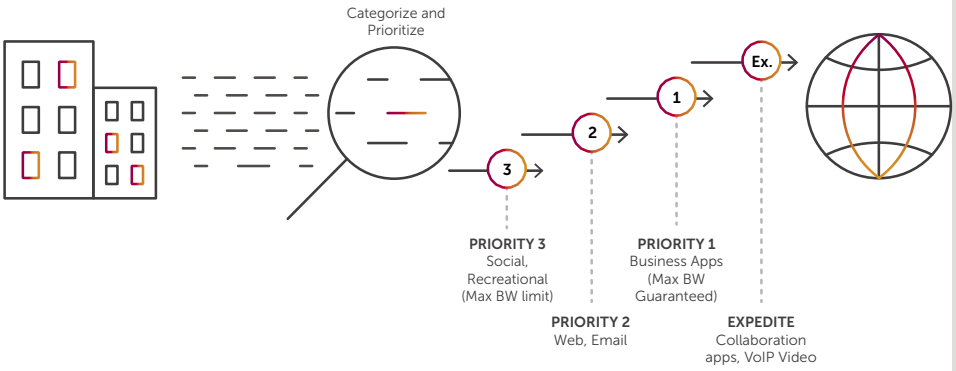


MEDIA & TELECOM

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



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.

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)

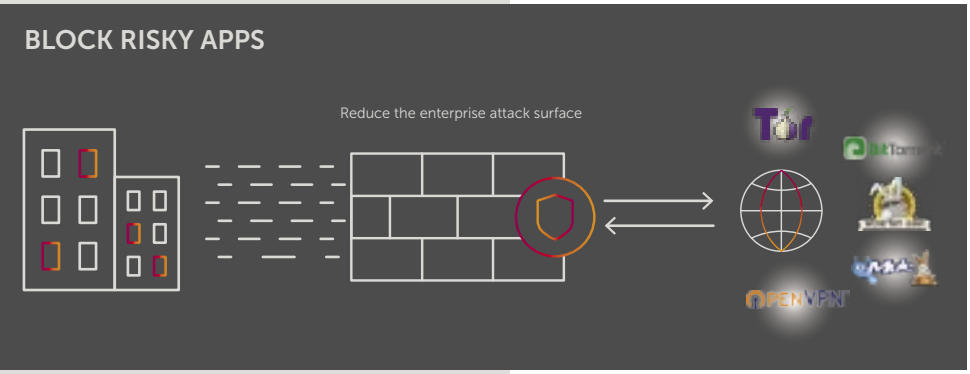
- Allot Gateway Manager
- Allot ClearSee Analytics

Key Benefits

- Reduce the attack surface by blocking risky applications
- Identify and control the use of risky applications and unsanctioned IT applications, Virtual Private Networks (VPNs), and anonymizers
- Block traffic that circumvents security controls

Control Risky and Unsanctioned Applications in Action

- Detects and controls a range of anonymizers, peer-to-peer, and file-sharing applications
- Bi-weekly application recognition updates
- Blocks and limits user traffic that employs unsanctioned IT applications



Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

MEDIA & TELECOM
CONTROL RISKY AND UNSANCTIONED APPLICATIONS

Heavy use of low priority or recreational applications and websites consumes considerable bandwidth and can congest and impair your network operations. Furthermore, some applications pose high levels of risk that extend beyond operational effectiveness, for example:

Peer-to-peer applications provide a backdoor to host data that can be accessed by anyone on the peer-to-peer network, and programs or content that is downloaded can include malware or violate copyrights.

Anonymizers/VPN tunnels are typically used to hide a user's identity and are in use by some to access illegal content or purchase illegal goods, such as drugs.

Although these applications can be used for the intended purpose of privacy, they are also used to hide illegal activities or they are exploited for cyberattacks. By nature, they are designed to bypass conventional security controls such as firewalls and Intrusion Detection System (IDS). They achieve concealment using encryption and obfuscation and identifying them is not a trivial effort. Allot employs advanced mechanisms to detect encrypted applications that enable an enterprise to identify risk and/or malicious apps without having to decrypt them. These methods include the following and apply to encrypted HTTP and non-HTTP traffic:

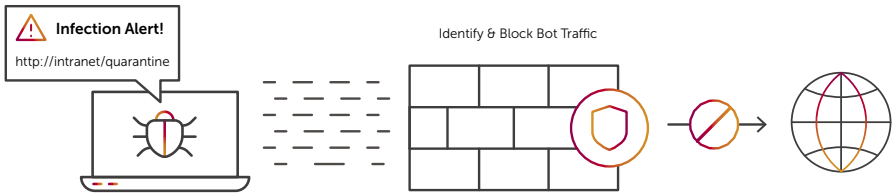
- Traffic statistics
- Server Name Indicator (SNI) detection
- Machine learning algorithms
- Pattern detection
- Certificates analysis
- Secure Sockets Layer (SSL) extensions analysis
- Traffic heuristics

MEDIA & TELECOM

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

- Prevent Wi-Fi network congestion
- Ensure Wi-Fi service availability to all users
- Enhance customer satisfaction

Wi-Fi Optimization in Action

- Map congestion conditions into fair usage policy rules
- Utilization threshold automatically triggers fair usage policy enforcement
- Rate-limit all users or only excessive users
- Automatically restore regular policy when congestion subsides

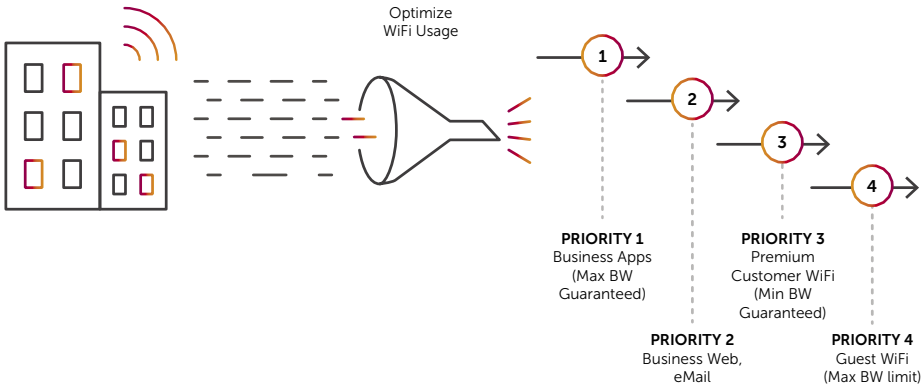
Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure

MEDIA & TELECOM
WI-FI OPTIMIZATION

A growing number of Wi-Fi service providers are the national media and telecom companies who offer Wi-Fi services to attract customers and enhance their in-house experience. This service can be easily monopolized by a few heavy users, and therefore requires fair usage management. For example, a media company cannot afford to enable its employees to download and stream high-definition movies during business hours. DPI-based solutions enable these enterprises to monitor Wi-Fi utilization in real time and enforce QoS based on dynamic network conditions.

WI-FI OPTIMIZATION

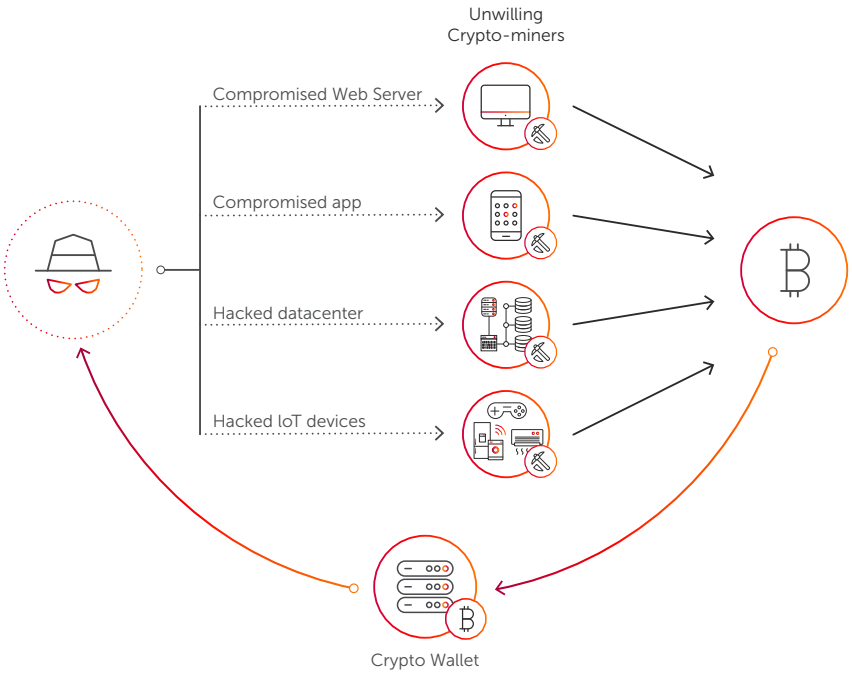


MEDIA & TELECOM

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