USE CASE BRIEF

AppLogic NETWORKS

# Enterprise Acceptable Use Policy (AUP) Enforcement

## APPLICATION-AWARE CONTROL TO PROTECT PRODUCTIVITY, COMPLIANCE, AND NETWORK PERFORMANCE

## Enterprise AUP Enforcement Solution Delivers:

### Application-Aware Usage Control

Works alongside firewalls, secure web gateways, and endpoint controls rather than replacing them, by identifying and classifying applications, application categories, and content types in real time, enabling precise enforcement of acceptable use policies beyond IP- or domain-based controls. This ensures policies are applied consistently, even as applications evolve or encrypt traffic.

### Granular Content and Website Enforcement

Enforces acceptable use policies using native application intelligence combined with always-current third-party URL categorization databases, enabling enterprises to block, filter, or restrict access to inappropriate, non-business, or prohibited content such as adult material, gambling, violence, drugs, and malware-hosting sites.

### Policy Enforcement Beyond Traditional Web Filters

Controls modern application traffic, embedded services, and evasive techniques that often bypass legacy firewalls and proxy-based filters. This closes enforcement gaps created by encrypted traffic, dynamic domains, and application masquerading.

### Flexible Shaping, Throttling, and Blocking Controls

Applies differentiated actions based on policy intent—blocking disallowed content outright, throttling non-business traffic, or allowing limited access during defined time windows—without impacting business-critical applications.

### Unified Visibility and Policy Validation

Correlates acceptable use enforcement with user behavior, location, application performance, and network conditions, and provides complete visibility in the Enterprise Insights portal, showing which traffic is allowed, shaped, or blocked, who is affected, and how policies affect network usage and application experience.

## EXECUTIVE SUMMARY

**Modern enterprises depend on open internet access to run their business, collaborate, and innovate. At the same time, unrestricted access to non-business, inappropriate, or prohibited content exposes organizations to productivity loss, legal risk, regulatory non-compliance, and reputational damage. Acceptable Use Policies (AUP) are therefore a foundational requirement for enterprise IT and security teams, defining what applications, websites, and content types are permitted, restricted, or blocked across the corporate network.**

AppLogic Networks enables enterprises to enforce Acceptable Use Policies with precision, intelligence, and operational simplicity. By combining native application intelligence, deep traffic classification, third-party URL categorization, and real-time policy enforcement, AppLogic Networks allows enterprises to move beyond coarse firewall rules and static web filtering. The solution delivers consistent, enforceable AUP compliance across users, locations, devices, and applications—without compromising visibility, user experience, or operational agility.

## BUSINESS CHALLENGES

Every enterprise struggles to balance user productivity and network control. Application ecosystems evolve, and traffic becomes more encrypted and dynamic. Traditional firewalls and proxy-based web filters rely heavily on IP addresses or domain lists, which are constantly changing and often insufficient to identify modern applications, embedded services, or evasive traffic techniques. This results in policy gaps where prohibited content bypasses controls or legitimate business traffic is unintentionally blocked.

Productivity loss remains a persistent issue as non-business applications such as social media, streaming media, online gaming, and entertainment consume network resources during working hours. At the same time, access to legally restricted or inappropriate content—such as adult material, gambling, violence, hate speech, or malware-hosting sites—creates government regulation compliance and legal exposure, particularly in regulated industries and government-mandated environments.

## APPLOGIC NETWORKS' UNIQUE APPROACH

AppLogic Networks takes an application-aware, intelligence-driven approach to Acceptable Use Policy enforcement. Instead of relying solely on IP addresses or basic URL matching, the solution identifies and classifies traffic at the application, application category, and content levels in real time. This enables policies to be defined in business terms—such as “block adult content,” “limit recreational streaming,” or “allow social media for marketing teams only”—rather than strict technical constructs.

Native application intelligence is augmented with third-party URL categorization through integrations such as Netstar’s Internet Filtering Database (IFD). These databases classify websites into hundreds of granular content categories, including adult content, gambling, drugs, violence, extremism, malware, and anonymizers. Because URL and content databases change continuously, AppLogic Networks distributes frequent updates using the iFeeds system, ensuring enforcement decisions are always based on current intelligence.

## KEY BENEFITS AND OUTCOMES:

- Organizations reduce legal and regulatory exposure by ensuring that prohibited content is blocked in accordance with corporate and government mandates, while maintaining auditable visibility into enforcement actions.
- Productivity improves, and network congestion is reduced as non-business and recreational traffic is controlled without disrupting legitimate business applications. Rather than blanket blocking, enterprises can selectively slow or restrict traffic types.
- Operational efficiency increases through unified visibility and control. IT and security teams gain a single solution that combines policy definition, real-time enforcement, and detailed analytics, eliminating the blind spots familiar with traditional filtering tools.
- Finally, the solution provides long-term adaptability. As applications evolve, encryption increases, and content categories change, AppLogic Networks' intelligence-driven approach ensures Acceptable Use Policies remain effective, measurable, and aligned with business objectives—without constant manual reconfiguration.

Most importantly, AppLogic Networks tightly couples enforcement with visibility. Every shaping, filtering, or blocking action is observable in Enterprise Insights, allowing IT and security teams to validate policy effectiveness, understand user behavior, and continuously refine AUP rules based on real usage patterns rather than assumptions.

## CORE CAPABILITIES

AppLogic Networks' Enterprise Acceptable Use Policy Enforcement solution combines advanced application intelligence, comprehensive content filtering, automated database distribution, and complete control and visibility to help enterprises enforce corporate policy, meet compliance mandates, and improve network productivity.

### Native Application Intelligence

AppLogic Networks' advanced application intelligence classifies network traffic not only at the application level, but also at the content level within each application. It distinguishes how an application is being used—for example, separating YouTube live streaming from adaptive video streaming, or identifying WhatsApp media downloads separately from voice and video calls. This encryption-agnostic classification provides enterprises with precise visibility into both business and non-business usage patterns across more than 95% of network traffic. With per-application content awareness, IT teams can define highly granular Acceptable Use Policies that allow legitimate business functions while shaping bandwidth-intensive entertainment usage, restricting high-risk content, or applying time-based controls—without over-blocking entire applications or disrupting critical workflows.

### Comprehensive Content Filtering via ContentLogic and URL Databases

ContentLogic, powered by the Internet Filtering Database (IFD), provides extensive URL categorization with over 200 content categories—including adult content, gambling, violence, illegal content, dating sites, streaming media, and productivity applications. This comprehensive categorization enables enterprises to block websites by category automatically. The IFD database contains URL entries with domain-level, path-level, and page-level categorization, enabling precise enforcement beyond simple domain blocking.

Customers can create and upload their custom databases, such as lists of safe URLs or blocked domains on specific ports.

### Automated Database Distribution via iFeeds

Content databases require frequent updates to remain effective—new websites launch daily, existing sites change purpose, and threat intelligence evolves continuously. AppLogic Networks' Intelligent Feeds (iFeeds) system automates the distribution of ContentLogic and other databases across the enterprise deployment, ensuring that all enforcement points maintain current, accurate categorization data without manual intervention. Four daily updates ensure categories remain current as new sites emerge and existing sites change categorization.

### Traffic Shaping and Filtering Enforcement

Once applications, content, and websites are classified and categorized, AppLogic Networks enforces policy through two complementary mechanisms.

- Traffic Shaping: Rather than blocking all non-compliant traffic, enterprises often prefer to shape bandwidth-intensive entertainment traffic. AppLogic Networks can shape traffic by application or content category, limiting throughput for streaming services, gaming platforms, and social media while preserving bandwidth for business-critical applications.
- Traffic Filtering/Blocking: For prohibited content categories, AppLogic Networks can block traffic at line rate with immediate rejection.

### Contextual Enforcement

Policies leverage complete application and user context—combining application classification, content category, user identity, location, device type, and time of day—to create sophisticated enforcement rules. For example: "Block social media for all users except the Marketing department, during business hours."

### ABOUT APPLOGIC NETWORKS

AppLogic Networks' cloud-based App QoE portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit **https://www.applogicnetworks**.com or follow AppLogic Networks on X **@AppLogic Networks**.

AppLogic NETWORKS

**USA**
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

**EUROPE**
Neptunigatan 1
211 20, Malmö
Skåne
Sweden
T. +46 340.48 38 00

**CANADA**
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

**ASIA**
Arliga Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the AppLogic Networks website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by AppLogic Networks Corporation and its affiliated companies ("AppLogic Networks"), and AppLogic Networks assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect AppLogic Networks proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of AppLogic Networks technology in generalized terms. AppLogic Networks reserves the right to periodically change information that is contained in this documentation; however, AppLogic Networks makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.