



Bytescreen Firewall Technology Whitepaper

Version 1.0, 2025

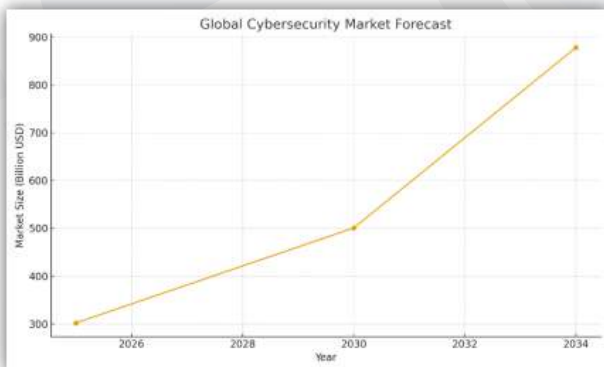
Table of Contents

- EXECUTIVE SUMMARY
- THE CYBERSECURITY LANDSCAPE IS
- GLOBAL & INDIAN CYBERSECURITY MARKET
- WHY NGFW IS ESSENTIAL TODAY
- VERTICAL-BASED SOLUTION APPROACH
- BYTESCREEN: A COMPLETE NETWORK SECURITY PLATFORM
- WHY TRADITIONAL NETWORKS FAIL
- THE BYTESCREEN DIFFERENCE
- TRADITIONAL MULTI-VENDOR ENVIRONMENT VS BYTESCREEN AI-DRIVEN NETWORK SOLUTION
- PMTA
- BYTESCREEN NGFW: MODERN SECURITY SIMPLIFIED
- TOP FEATURES
- CENTRALIZED MANAGEMENT WITH BYTESCREEN FUSION MAESTRO
- TOTAL COST SAVINGS
- COMPLETE SECURITY STACK
- PROBLEMS WE SOLVE
- INNOVATION & DIFFERENTIATION
- CONCLUSION



EXECUTIVE SUMMARY

The digital world is undergoing a massive transformation. Organizations of all sizes, schools, hospitals, banks, public infrastructure, manufacturing plants, retail chains, and enterprises are now deeply dependent on internet connectivity, cloud services, remote access, mobile users, and SaaS applications.



At the same time, cyberattacks are increasing at an alarming rate, and threat actors are becoming more sophisticated, hiding inside encrypted traffic and exploiting cloud-based environments.

Traditional firewalls and multi-vendor networks can no longer provide the reliability, visibility, or security that modern businesses require. They create complexity, increase cost, and fail to keep pace with the evolving digital ecosystem.

Bytescreen introduces a **new era of intelligent, unified, AI-driven network security**. It brings together:

- A powerful **Next Generation Firewall (NGFW)**
- A feature-rich **SD-WAN platform** with PMTA aggregation
- A centralized **Network Management System (NMS)**
- A robust **AAA & Identity Management framework**
- **FWaaS (Cloud-delivered Firewall)**

This combined approach simplifies network operations, enhances security, increases visibility, reduces cost, and ensures reliable, uninterrupted connectivity.

THE CYBERSECURITY LANDSCAPE IS

The threat landscape has evolved significantly over the past decade. Old firewall models, built for simple networks, cannot cope with today's challenges. Key changes include:

1. Massive Growth in Encrypted Traffic

- Nearly 90% of global internet traffic is now encrypted.
- Attackers use HTTPS to hide malware, avoiding detection by outdated firewalls.
- TLS 1.3 encryption prevents deep visibility unless advanced inspection is used.

2. Rapid Increase in Cyberattacks

- Global attacks have increased more than 30% year-over-year.
- Attackers target every sector: education, BFSI, healthcare, manufacturing, and government.
- Zero-day vulnerabilities and ransomware remain the top threats.

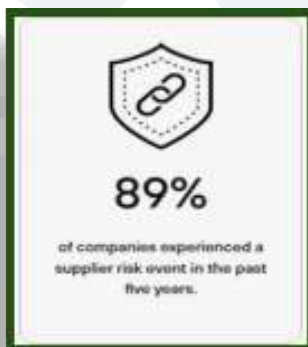
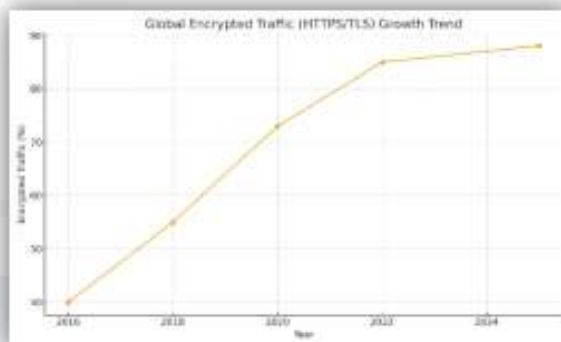
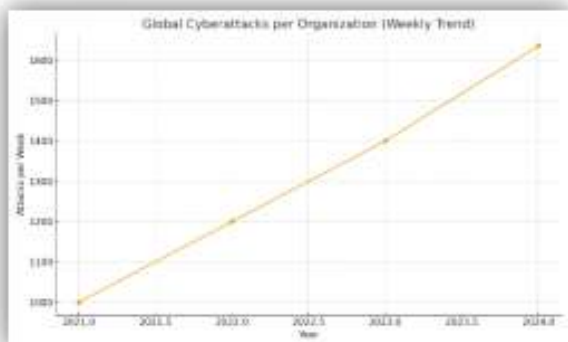
3. The Rise of Cloud & Remote Work

- More teams work remotely or in hybrid environments.
- Businesses rely on cloud apps like Microsoft 365, Google Workspace, Zoom, Teams, and Salesforce.
- Traditional firewalls struggle to secure users outside the office network.

4. IoT & Smart Devices Expanding the Attack Surface

- Cameras, sensors, machines, access points, phones—all connected.
- Each device becomes a potential security risk.

Bytescreen addresses all these challenges with a modern, unified approach that ensures visibility, control, and protection in all environments.



GLOBAL & INDIAN CYBERSECURITY MARKET

Cybersecurity is now one of the fastest-growing technology sectors worldwide. According to leading research: Global Growth

The global cybersecurity market is valued at **USD 301.91 billion in 2025.**

It will reach **USD 878.48 billion by 2034.**

This represents a **12.6% CAGR**, driven by cloud adoption, AI threats, and remote work.

Indian Market Growth

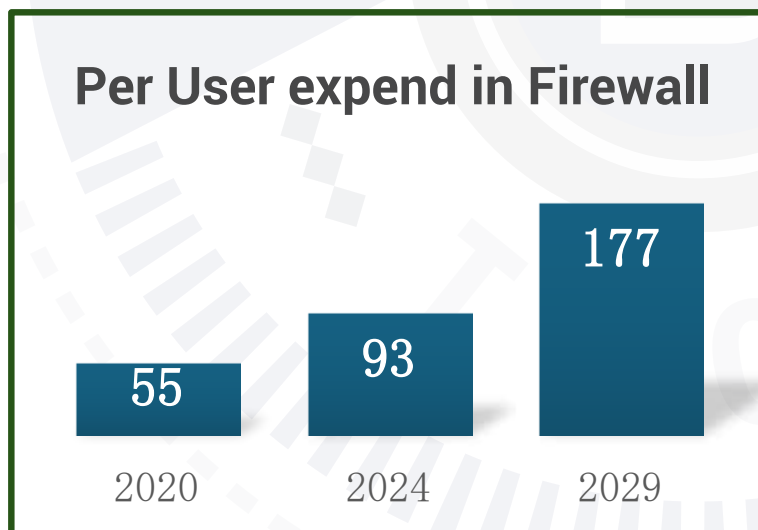
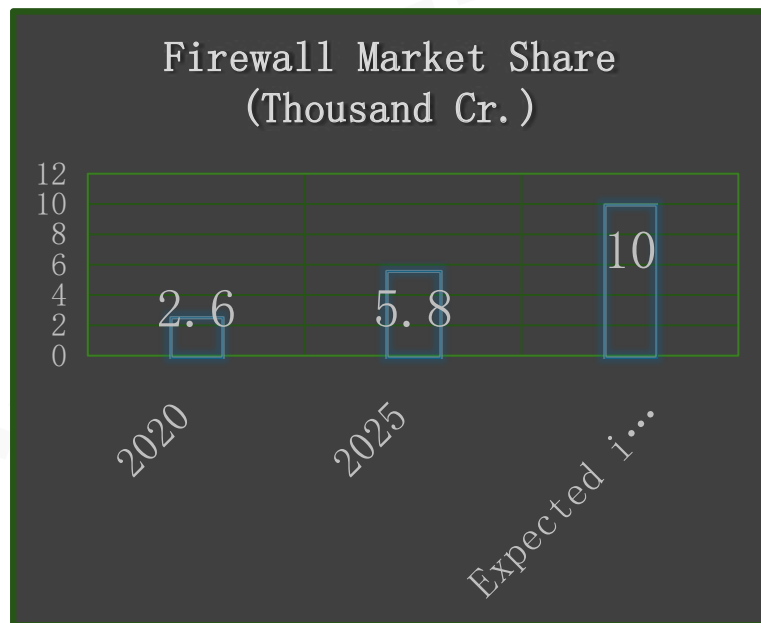
India's network security market will reach **₹10,000 Crores by 2029.**

The Indian FWaaS segment is growing at **22.3% CAGR.**

What This Means

Organizations are increasingly adopting NGFW, SD-WAN, ZTNA, and FWaaS.

Legacy firewalls are being replaced at an accelerated rate. Businesses are prioritizing automation, cloud-based security, and unified network solutions.



WHY NGFW IS ESSENTIAL TODAY

Traditional firewalls were designed for a time when:

- Traffic was mostly unencrypted
- Users worked inside office premises
- Applications were hosted on local servers
- Networks had simple architectures

This model no longer works.

Modern NGFWs Are Needed Because:

1. Encrypted Traffic Dominates

NGFWs with SSL/TLS inspection can see inside encrypted data, identify malware, and block hidden threats.

2. Application Visibility Is Critical

Applications like YouTube, WhatsApp, Facebook, Teams, and gaming apps require fine control. NGFWs identify and manage each app at a granular level.

3. Users Work from Anywhere

NGFWs support secure VPN, ZTNA, and identity-based rules for remote users.

4. Cloud Services Require New Security Models

Access control, threat analysis, and cloud visibility are built into NGFWs like Bytescreen.

VERTICAL-BASED SOLUTION APPROACH

Every industry has different network requirements. Bytescreen follows a **solutions-first approach**, not a product-first approach.

1. Public Infrastructure

- Large-scale surveillance
- Mission-critical connectivity
- Centralized network control
- High uptime

2. Education

- Safe internet access for students
- Blocking harmful content
- Managing campus Wi-Fi
- Protecting internal data

3. Enterprise

- Application-aware traffic shaping
- Remote workforce support
- Secure branch connectivity
- Strong identity management

4. Hospitality

- Guest Wi-Fi isolation
- Secure POS terminals
- Data protection for guests
- Fast and stable connectivity

5. BFSI

- High compliance requirements
- Transaction security
- Encrypted traffic inspection
- Continuous monitoring

6. Healthcare

- Protecting patient data
- Maintaining 24/7 uptime
- Securing IoT medical devices
- Ransomware prevention

Deployment

Cloud



private/public

On-Prim



Hardware/Server

Virtual



VMware

BYTESCREEN: A COMPLETE NETWORK SECURITY PLATFORM

Bytescreen is not just a firewall.

It is a **full suite of network solutions** designed for modern businesses.

Here's what Bytescreen includes:

- Next Generation Firewall (NGFW)
- SD-WAN with PMTA aggregation
- Centralized Network Management System (NMS)
- AAA (Authentication, Authorization, Accounting)
- AI-based threat intelligence
- Zero Trust Network Access
- AP Controller for multi-brand access points
- Network DLP (Data Loss Prevention)
- Virtual Firewall & Cloud FWaaS

This unified approach eliminates the need for multiple vendors and tools.

BYTESCREEN OFFERS THE FOLLOWING

1. Intuitive Management

Easy-to-use dashboards simplify configuration, monitoring, and troubleshooting—even for non-specialists.

2. High Performance

Optimized hardware and intelligent software ensure smooth, fast performance even under heavy load.

3. Advanced Threat Protection

AI-driven security analyzes patterns, detects anomalies, and blocks new and unknown threats.

4. On-Prem or Cloud Deployment

You can deploy Bytescreen anywhere—branch office, data center, or cloud.

5. Low Cost of Ownership

One platform replaces multiple products, reducing hardware, software, licensing, and manpower costs.

WHY TRADITIONAL NETWORKS FAIL

Many organizations rely on a combination of:

- Old routers
- Multiple firewalls
- Separate SD-WAN devices
- Multiple access points
- Fourth-party monitoring tools
- VPN appliances
- Content filtering devices

This creates:

1. High Complexity

Managing multiple devices and vendors increases operational burden.

2. Performance Bottlenecks

Different systems cannot optimize traffic collectively.

3. High Cost

More devices = more licenses, more hardware, more manpower.

4. Troubleshooting Delays

Without a single management console, diagnosing problems becomes slow and difficult. Bytescreen consolidates all these into a single, powerful system.

WHY TRADITIONAL NETWORKS FAIL

Many organizations rely on a combination of:

- Old routers
- Multiple firewalls
- Separate SD-WAN devices
- Multiple access points
- Fourth-party monitoring tools
- VPN appliances
- Content filtering devices

This creates:

1. High Complexity

Managing multiple devices and vendors increases operational burden.

2. Performance Bottlenecks

Different systems cannot optimize traffic collectively.

3. High Cost

More devices = more licenses, more hardware, more manpower.

4. Troubleshooting Delays

Without a single management console, diagnosing problems becomes slow and difficult. Bytescreen consolidates all these into a single, powerful system.

THE BYTESCREEN DIFFERENCE

Bytescreen transforms networks through:

Unified Connectivity + Security

WAN, LAN, Wi-Fi, firewall, VPN, DLP—everything controlled from one console.

AI-Enabled Intelligence

AI analyzes performance issues, predicts failures, and optimizes connectivity automatically.

Centralized Orchestration

All branches, devices, and users managed from a single cloud dashboard.

PMTA for Link Aggregation

Ensures reliable, non-stop internet connectivity across all links.

Policy-Driven Automation

Rules automatically adjust based on user, device, location, and application.

The result:

Stable, secure, and simple networking.

AI-ENABLED CIPS (Content Intelligence Protection System)

Bytescreen uses AI to:

- Analyze content patterns
- Detect malicious behavior
- Block harmful websites
- Identify unusual traffic patterns
- Predict attacks before they occur

This makes the network smarter and safer without manual intervention.

AI-LSO: WAN SELECTION & OPTIMIZATION

AI-LSO chooses the best path for each packet based on:

- Latency
- Jitter
- Link congestion
- Traffic type
- Application requirement

This ensures:

- Smooth video meetings
- Faster SaaS access
- Better remote work experience

TRADITIONAL MULTI-VENDOR ENVIRONMENT VS BYTESCREEN AI-DRIVEN NETWORK SOLUTION

Traditional Multi-Vendor Networks Are Too Complicated for Modern Environments

Most organizations today still use a combination of different devices to run their networks:

- Router from one vendor
- Firewall from another
- SD-WAN from a third
- Wi-Fi controller from another brand
- VPN/AAA appliance separately
- DLP or URL filter from a cloud vendor

At first, this appears flexible but in reality, it creates a **fragile, expensive, hard-to-manage system**.

Problems with Traditional Multi-Vendor Networks

1. High Operational Complexity
2. Troubleshooting Becomes a Blame Game
3. No Unified Visibility
4. Slow Response to Failures
5. High Cost of Ownership
6. No AI Support

Bytescreen AI-Driven Unified Network Solution: The Modern Approach

Bytescreen replaces all these individual systems with an **intelligent, unified platform** powered by AI, PMTA, SD-WAN, NGFW, and NMS.

1. One Platform Instead of Five

Routing + Firewall + SD-WAN + Wi-Fi Management + AAA + Security Analytics — all built into a single solution.

2. AI-Driven Automation

AI identifies issues, predicts failures, optimizes WAN traffic, and suggests actions.

3. Zero-Touch Deployment

Branches can be set up in minutes without sending engineers onsite.

4. Unified Visibility & Logging

One dashboard shows:

- WAN health
- LAN behavior
- Connected devices
- Threats & attacks
- Application usage
- Vulnerabilities

5. Auto-Healing Network

PMTA + AI-LSO automatically reroute traffic, fix link issues, and maintain uptime.

6. Lower Cost with Higher Efficiency

No need for multiple vendors =
Less hardware + fewer licenses + streamlined operations.



**BYTESCREEN NewAge AI
Enabled Networking**

1

Hardened & Intelligent
Network Security

2

Advanced WAN
Optimization &
Redundancy

3

Cutting-Edge Security &
Threat Intelligence

4

Centralized Control &
Intelligent Security

5

Cost-Effective, Scalable
& Future-Ready

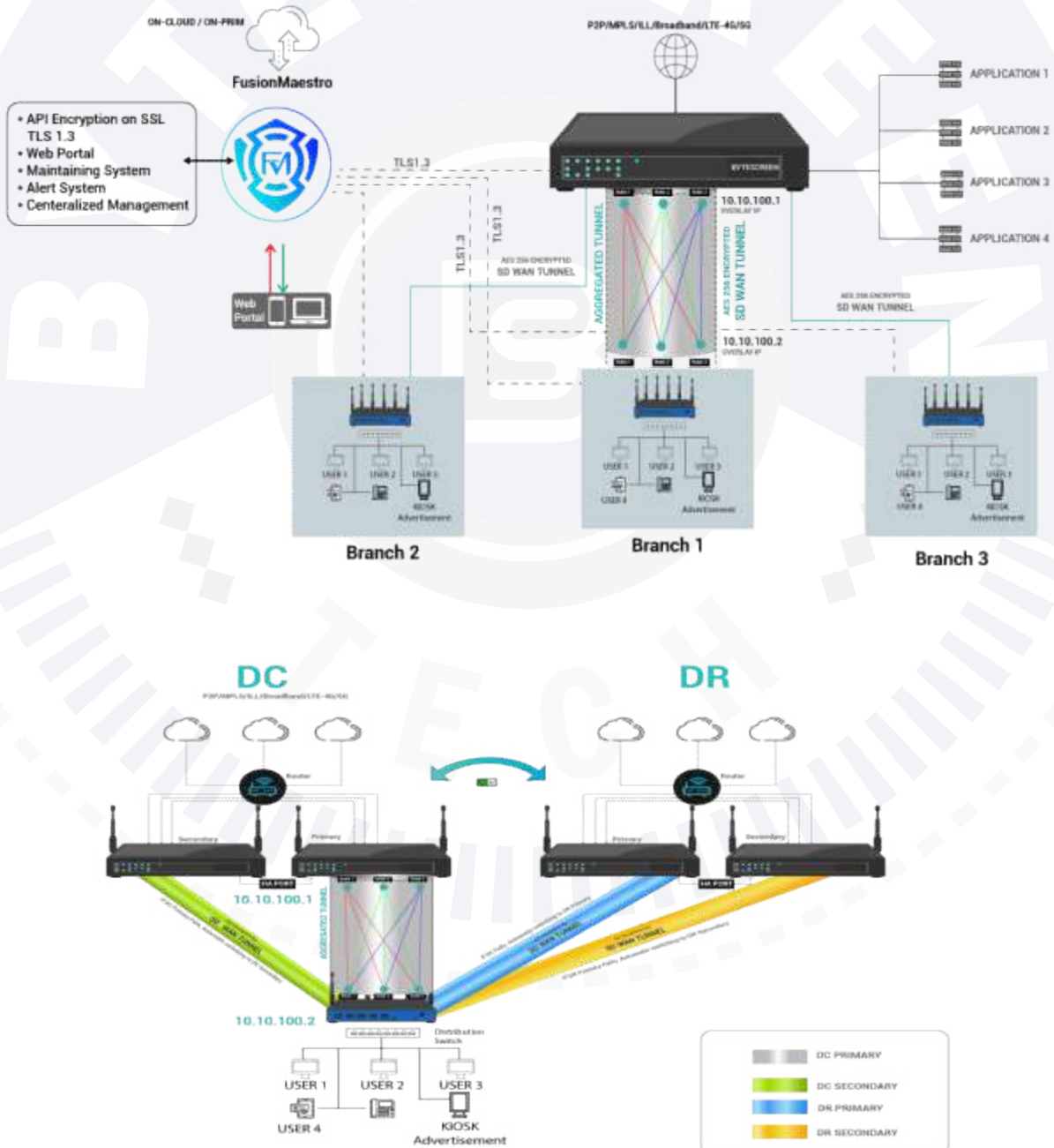
Simple | Flexible | Economical | Intent Aware

PMTA: A GAME-CHANGING CONNECTIVITY TECHNOLOGY

Packet-Based Multi-Tunnel Aggregation allows Bytescreen to:

- Combine multiple WAN links into one virtual super-link
- Maintain sessions even when one link fails
- Improve bandwidth utilization
- Reduce downtime to zero
- Enable seamless video calls, VoIP, and cloud apps

PMTA is designed for environments where every second of uptime matters.



BYTESCREEN NGFW: MODERN SECURITY SIMPLIFIED

Bytescreen NGFW delivers:

Unmatched Security

Detects, blocks, and prevents advanced cyber threats.

Enhanced Performance

Optimizes network usage without sacrificing speed or user experience.

Granular Control

Allows detailed control over applications, content, and user behavior.

Increased Visibility

Shows what users, apps, and devices are doing in real time.

Cost Efficiency

Reduces total cost across licensing, hardware, and manpower.

TOP FEATURES

The Bytescreen NGFW provides deep, intelligent protection using advanced AI techniques, granular content control, and multi-layer traffic inspection.

- 1. Advanced Content Filter:** Blocks harmful, inappropriate, or risky content using weighted keyword analysis, search-engine keyword blocking, and precise URL filtering that can block or allow specific full URLs
- 2. Malicious URL Detection:** Real-time detection of phishing, malware-hosting, and suspicious domains using threat intelligence.
- 3. AD Blocker:** Blocks intrusive ads and tracking scripts, improving user experience and reducing risk.
- 4. Application Filter:** Controls thousands of applications including social media, messaging, gaming, file sharing, and cloud apps.
- 5. Network DLP (Data Loss Prevention):** Prevents leakage of sensitive data such as PDFs, documents, financial info, customer data, etc.
- 6. AIHD — Auto Infected Host Detection:** Identifies compromised systems inside the network by monitoring unusual traffic behavior without requiring any agent on the system
- 7. Advanced Threat Protection (ATP):** Real-time detection of malware, ransomware, botnets, and zero-day attacks.
- 8. AI-Enabled IPS/IDS:** Over 50,000+ signatures with behavioral detection for unknown threats.
- 9. Access Point Management:** Control and manage multi-brand access points from the NGFW interface.
- 10. AI-Enabled WAN Link Selection:** AI chooses the best internet link based on latency, jitter, packet loss, and live app requirements.
- 11. LAN Micro-Segmentation:** Isolates critical devices and departments to prevent internal attacks and lateral movement.
- 12. Auto-Healing Network Support:** Automatically resolves link issues and re-routes traffic without user impact.

Other features to enhance security

- SNI-based HTTPS filtering
- Keyword-based filtering
- File & MIME extension blocking
- Zero-day protection
- Malware scanning through DPI
- DDoS and DoS protection
- Behavioural anomaly detection
- PMTA multi-tunnel aggregation
- Multi-WAN support (4G/5G, MPLS, ILL, Broadband)
- WAN compression
- Multi-path, multi-direction routing
- IDENTITY & ACCESS
- Role-based access
- ZTNA
- NAS
- Auto-device discovery
- VLAN analytics
- NMS
- Syslog
- REST API
- Advanced reports
- SLA monitoring

CENTRALIZED MANAGEMENT WITH BYTESCREEN FUSION MAESTRO

Unified Control for the Entire Network

Fusion Maestro is Bytescreen's advanced centralized management and orchestration system. It brings **all Bytescreen devices, branches, users, WAN links, security policies, and cloud workloads into one intelligent control center.**

This eliminates the need for multiple tools, complex configurations, and time-consuming manual tasks. What Fusion Maestro Offers

1. Single-Pane-of-Glass Visibility

All devices across all sites appear in **one unified dashboard**. IT teams can view

2. Real-Time Network Intelligence

Fusion Maestro uses AI-based analytics for, This allows IT teams to prevent incidents before they happen.

3. Zero-Touch Deployment for Branch Offices

New devices are automatically configured when connected. Fusion Maestro pushes policies remotely, reducing:Branches can be live in minutes.

4. Centralized Policy Orchestration

Security rules, VLAN settings, user access policies, and WAN optimizations can be applied: ensures consistent security across the entire organization.

5. Unified Logging & Security Analytics

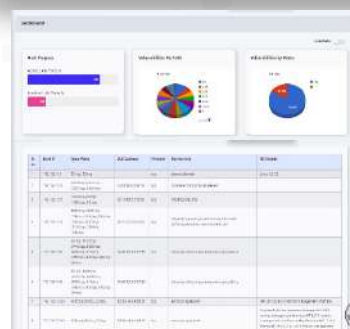
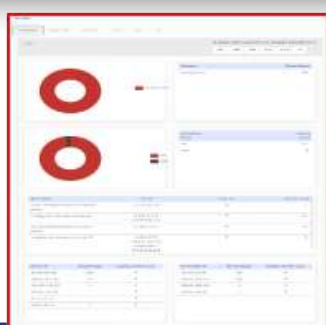
Fusion Maestro consolidates: This enables easy auditing and fast troubleshooting.

6. Built-in Network Automation

Automated tasks improve reliability: Fusion Maestro reduces manual workload by up to **75%**.

7. Scalable for All Sizes of Organizations

Fusion Maestro can manage: It grows with your network and adapts to your needs.



TOTAL COST SAVINGS

Our Full Stack approach drops Total Cost of Ownership with high Security

This unified approach leads to simplified architecture with significant cost savings across the Network Lifecycle. At same time it enhances the security posture of the organization enabling improvement in Security audits and compliance across multiple threat vectors.



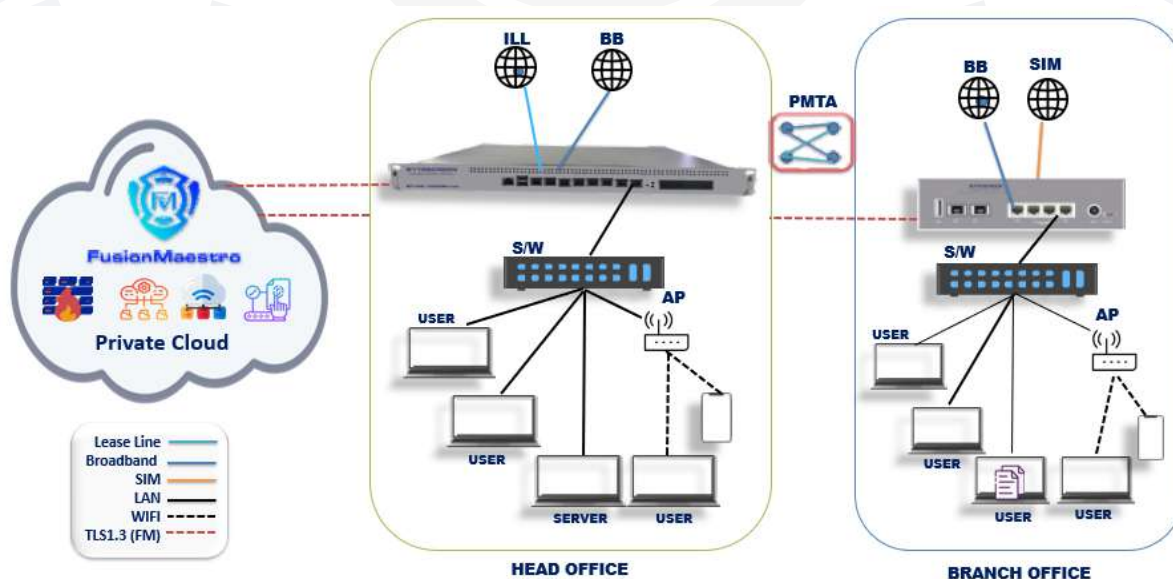
COMPLETE SECURITY STACK

Bytescreen's full security stack includes:

Bytescreen delivers a fully integrated, end-to-end network security stack designed to protect every layer of your network — users, applications, devices, WAN, LAN, and cloud workloads. This unified approach reduces complexity, eliminates the need for multiple vendors, and enhances your overall security posture.

The Bytescreen Security Stack Includes:

- NGFW (Next Generation Firewall)
- SD-WAN (Software-Defined WAN)
- NMS (Network Management System)
- DLP (Data Loss Prevention)
- ZTNA (Zero Trust Network Access)
- AAA (Authentication, Authorization, Accounting)
- AP Controller (Multi-Brand Access Point Management)
- VPN (IPSec/SSL VPN)
- Geo-Fencing & Geo-Filtering
- Vulnerability Assessment (VA Dashboard)
- Threat Intelligence
- Log Analytics & Reporting



PROBLEMS WE SOLVE

- **Hidden risks within encrypted traffic**

Bytescreen decrypts, inspects, and analyzes encrypted traffic to expose threats that traditional firewalls cannot see, ensuring complete visibility even inside HTTPS and TLS 1.3 streams.

- **Zero-day malware**

AI-driven behavioral detection and large signature databases identify and block new, unknown, or evolving malware before it can enter or move through the network.

- **Business downtime**

Technologies like PMTA and AI-LSO ensure uninterrupted connectivity, automatically rerouting traffic during link failures to maintain consistent uptime and application performance.

- **Unreliable WAN links**

Bytescreen intelligently aggregates broadband, MPLS, and 4G/5G connections, optimizing each packet's path to deliver stable, high-quality WAN performance even on fluctuating links.

- **Shadow IT**

The platform detects unauthorized devices, applications, and services, allowing administrators to monitor and control everything connected to the network.

- **Poor visibility across branches**

Fusion Maestro and NMS provide centralized real-time insights into all branch locations, devices, usage patterns, and potential issues from a single pane of glass.

- **High infrastructure cost**

Multiple products—firewall, SD-WAN, Wi-Fi controller, DLP, VPN, AAA—are consolidated into one unified system, reducing hardware, licensing, and manpower expenses.

- **Complex multi-vendor environments**

Bytescreen replaces fragmented tools with an integrated, AI-driven solution that simplifies operations, accelerates troubleshooting, and delivers consistent policies across the network.

- **One Unified Solution**

All connectivity, security, and management features operate together seamlessly, reducing complexity and enhancing overall network reliability.

INNOVATION & DIFFERENTIATION

Bytescreen stands out due to:

- **Customer-Centric Innovation**

Bytescreen features are built directly from real-world customer challenges, ensuring practical functionality, intuitive workflows, and solutions tailored for everyday operational needs.

- **Custom Deployment Approaches**

The platform adapts to diverse industries—education, healthcare, BFSI, enterprise, public infrastructure—offering flexible deployment models that meet unique structural and compliance requirements.

- **Auto-Healing Network Architecture**

Using AI and smart routing, Bytescreen automatically detects faults, reroutes traffic, restores connectivity, and resolves issues without human intervention, reducing downtime drastically.

- **AI-Driven Operations**

AI optimizes WAN links, identifies threats, isolates infected hosts, and streamlines policy management, reducing manual effort, configuration errors, and dependency on skilled manpower.

- **User-Friendly Management**

A clean, intuitive management interface allows even non-technical users to monitor, control, and manage network security efficiently, backed by centralized dashboards and easy-to-use tools.

CONCLUSION

The future of networking demands security, intelligence, and simplicity. Bytescreen delivers all three in a unified, powerful platform.

Businesses need:

- Security
- Speed
- Reliability
- Cost-efficiency
- Ease of management

Bytescreen NGFW, SD-WAN, NMS, AAA, and FWaaS combine to create a **future-ready network security ecosystem** that protects and empowers modern organizations.

Bytescreen is not just a firewall. It is a complete network transformation platform.