

ALSCO®



Patents COMPANY PROFILE

ALSCO®: Leading the Future of Cybersecurity with 3 Patented Innovations under Secure Gateway®

Discover how ALSCO® is revolutionizing cybersecurity with Secure Gateway® – an innovative solution powered by three U.S.-patented innovations. Step into the future of secure communication, advanced threat prevention, and unmatched data protection.

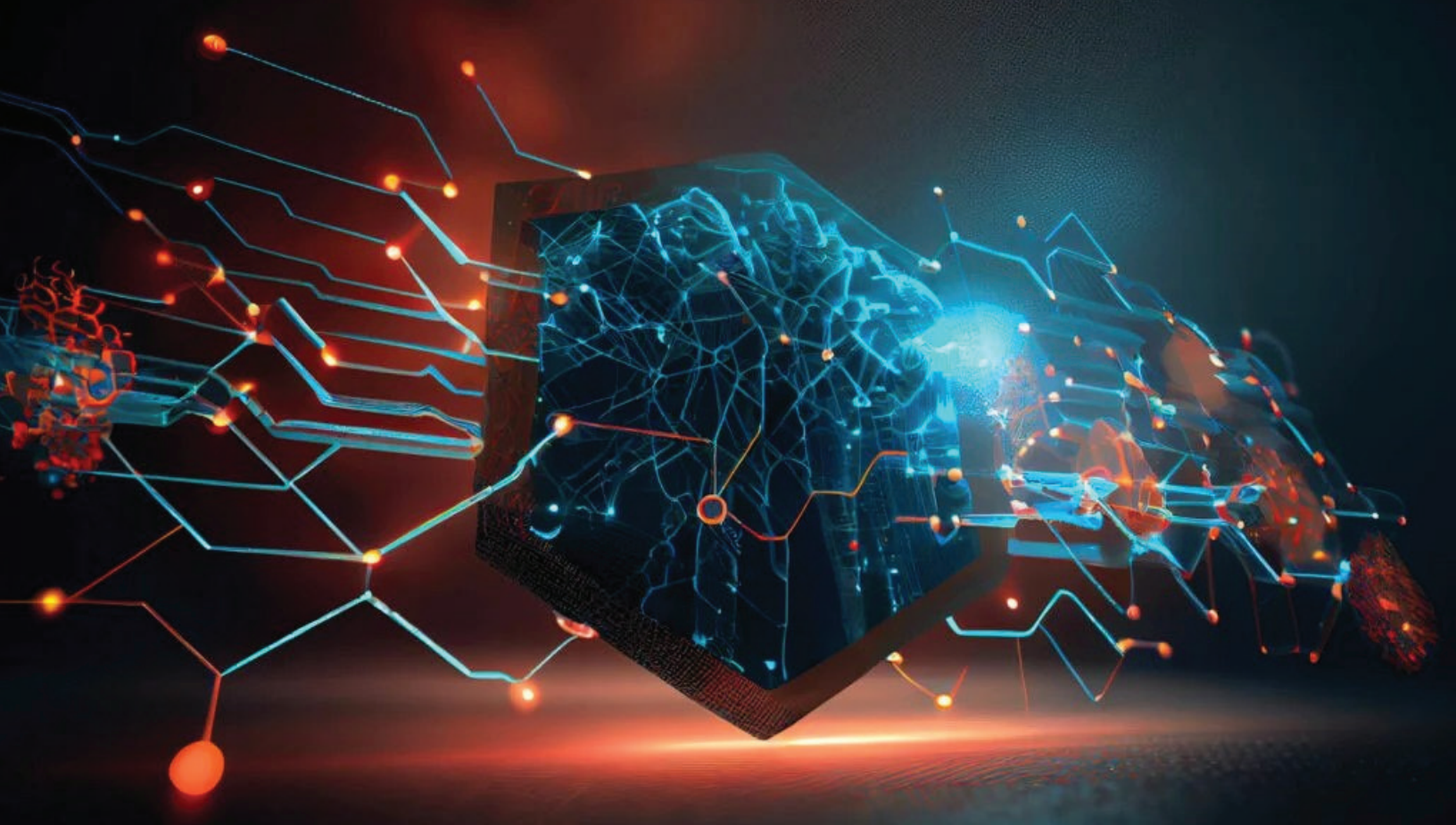
OUR PATENTS

- 01 **ALSCO® U.S. Patent No. 10,498,760 B1(2019):**
Revolutionizing Online Security Under Secure Gateway®
- 02 **ALSCO® U.S. Patent No. 10,630,721 B1(2020):**
Revolutionizing Email and Database Protection Under Secure Gateway®
- 03 **ALSCO® U.S. Patent No. 11,777,927 B1(2023):**
Establishing Secure Communication Channels Under Secure Gateway®



Phone: +1-917-284-8942

E-Mail: info@alscotoday.com | **Website:** <https://alscotoday.com/>



ALSCO® U.S. Patent No. 10,498,760 B1 (2019): REVOLUTIONIZING ONLINE SECURITY UNDER SECURE GATEWAY®

OVERVIEW:

U.S. Patent No. 10,498,760 B1, titled "**Monitoring System for Detecting and Preventing Malicious Program Code**," granted to ALSCO Software LLC on December 3, 2019, introduces a transformative cybersecurity technology. Branded as **Secure Gateway®**, this patented system redefines server protection by detecting and blocking malicious code uploads without relying on traditional access methods such as APIs, passwords, user IDs, biometrics, handshake protocols, or authentication mechanisms.

By eliminating backend server dependencies and performing thorough binary-level validation, **Secure Gateway® Patent No. 10,498,760** ensures unmatched protection against modern cyber threats while maintaining complete isolation of sensitive infrastructure. This innovative approach establishes it as a gold standard for enterprises and governments managing high-value data.

KEY FEATURES OF SECURE GATEWAY® PATENT NO. 10,498,760

No Reliance on Backend Access or Authentication:

Secure Gateway® operates without the need for traditional server access methods such as:

- APIs
- Passwords or user IDs
- Challenge-Handshake Authentication
- Biometric Authentication

This eliminates vulnerabilities associated with credential theft, API exploitation, or authentication bypass. Backend systems remain completely isolated, ensuring their security.

AI-Powered Real-Time Threat Detection:



Secure Gateway® intercepts all client-server interactions and analyzes data in real-time using advanced AI algorithms.



Malicious code hidden in files like images, videos, PDFs, or executables is detected and blocked, even when heavily disguised or deeply embedded.

Example:

A hacker hides malware in a video's metadata or embeds a script within an image file. Secure Gateway® identifies the threat at the binary level and blocks it before it reaches the server.

Binary-Level Validation:

- All files are converted into binary format for precise analysis.
- Binary data is segmented into smaller portions and cross-referenced against a centralized database of known malicious patterns.
- This method ensures even the most complex & concealed malware is detected with exceptional accuracy.

No Reliance on Backend Access or Authentication:

Secure Gateway® Patent No. 10,498,760 goes beyond basic logging by offering administrators powerful tools for threat analysis and management:



Customizable Filters:

Tailor searches based on IP addresses, domains, severity levels, countries, and more.



Real-Time Insights:

Continuously updated logs enable administrators to respond to active threats instantly.



Historical Threat Analysis:

Archived logs provide data for audits, compliance, and forensic investigations.



Automated Alerts and Actions:

Configurable alerts and automatic responses enhance proactive defense.

Example:

A multinational corporation detects an unusually high volume of requests from a suspicious IP cluster. Secure Gateway® identifies the pattern, flags it as a potential DDoS precursor, and blocks the activity before it impacts critical systems.

Complete Backend Independence:

- ✓ Secure Gateway® intercepts all client-server interactions and analyzes data in real-time using advanced AI algorithms.
- ✓ Malicious code hidden in files like images, videos, PDFs, or executables is detected and blocked, even when heavily disguised or deeply embedded.

Comprehensive Logging and Diagnostics:

➤ Maintains detailed logs for every interaction, including:

- IP addresses
- Domains
- Threat types and Rule IDs
- Request URLs
- Country origin
- HTTP status
- Severity levels

- ### ➤ Detected threats are converted into human-readable text and displayed on a diagnostic interface, aiding rapid response.



Adaptable Defense Mechanism:

Secure Gateway® is built to evolve with emerging threats:

- ✓ **Dynamic Threat Database:**
Regular updates ensure defense against zero-day exploits and advanced persistent threats.
- ✓ **Self-Learning AI Models:**
AI learns from every interaction, enhancing accuracy and minimizing false positives.
- ✓ **Global Threat Intelligence Integration:**
Aligns with external intelligence sources for preemptive threat detection.
- ✓ **Scalable Defense:**
Handles high data volumes across diverse infrastructures seamlessly.
- ✓ **Behavioral Analysis:**
Monitors user activity for deviations, identifying sophisticated attacks like slow-drip data exfiltration.

Example:

A ransomware variant spreads globally. Secure Gateway® updates its database immediately, blocking the threat before it reaches the organization.

HOW SECURE GATEWAY® PATENT NO. 10,498,760 BENEFITS ENTERPRISES AND GOVERNMENTS



Unmatched Server Isolation: Ensures zero interaction between backend servers and external systems by eliminating credentials or API-based access.



Proactive Threat Detection: Blocks malicious code before it interacts with the server, offering defense against zero-day exploits and evolving threats.



Effortless Deployment: No backend software or code integration is required, ensuring seamless deployment in both on-premises and cloud environments.



Enhanced Visibility: Comprehensive logs provide insights for audits, compliance, and forensic investigations.



Regulatory Compliance: Meets global standards like GDPR, HIPAA, and SOC 2, making it suitable for industries requiring high accountability

WHAT SETS SECURE GATEWAY® APART



Innovative Design:

Provides server protection without backend access, inherently reducing the attack surface.



AI Precision and Adaptability:

Detects threats regardless of disguise and adapts to emerging attack vectors.



Zero Backend Dependencies:

Requires no software installations or backend changes, ensuring seamless integration.



Future-Ready Scalability:

Designed to handle high-volume, complex data while adapting to evolving infrastructures.



Real-World Applications:

- Scenario 1: A government agency detects hidden malware in a video file. Secure Gateway® isolates and blocks it.
- Scenario 2: An enterprise intercepts a PDF with embedded exploits. Secure Gateway® identifies and neutralizes the threat.

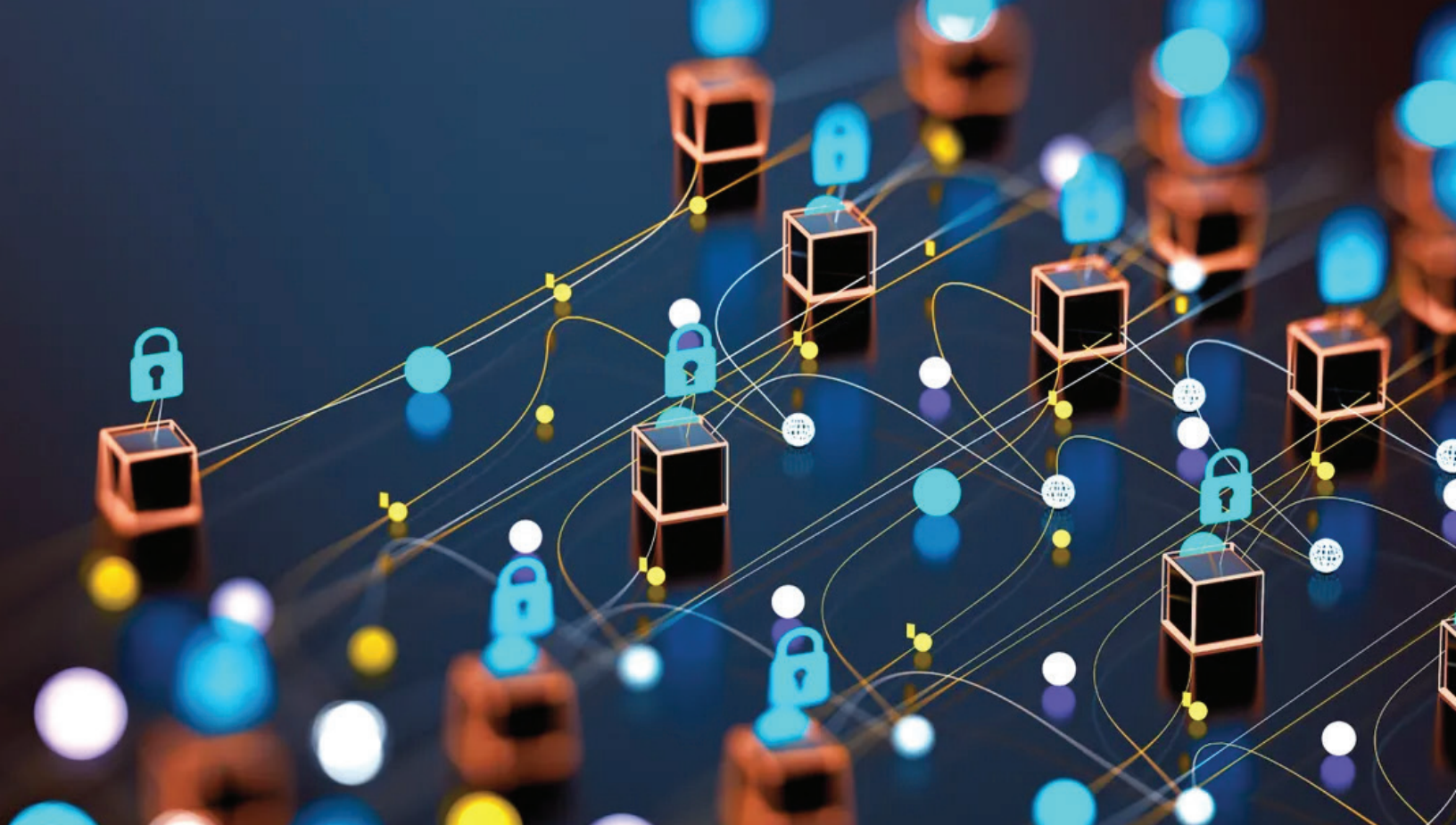
CONCLUSION: A BREAKTHROUGH IN CYBERSECURITY

Secure Gateway®, protected under U.S. Patent No. 10,498,760 B1, combines artificial intelligence, binary-level validation, and backend independence.

It:

- Blocks malicious code before it interacts with servers.
- Maintains complete backend isolation.
- Simplifies deployment with no code integration.
- Detects deeply embedded and evolving threats.
- Enhances visibility through advanced logging and diagnostics.

Secure Gateway® sets a new benchmark in cybersecurity, making it the ultimate choice for organizations seeking robust, scalable, and future-ready protection.



ALSCO® U.S. Patent No. 10,630,721 B1 (2020): REVOLUTIONIZING EMAIL AND DATABASE PROTECTION UNDER SECURE GATEWAY®

OVERVIEW:

U.S. Patent No. 10,630,721 B1, titled "**Monitoring System for Detecting and Preventing Malicious Program Code,**" granted to ALSCO Software LLC on April 21, 2020, introduces a revolutionary advancement in email and database file security. Operating under the **Secure Gateway®** platform, this patented system protects email systems, database operations, and web servers from malicious file uploads and embedded threats.

Secure Gateway® Patent No. 10,630,721 employs **binary-level validation, AI-powered threat detection,** and a fully **independent architecture** to provide unparalleled protection. Its capability to protect systems without requiring backend server or database access makes it invaluable for enterprises and governments managing sensitive data.

KEY INNOVATIONS OF SECURE GATEWAY® PATENT NO. 10,630,721 FOR EMAIL AND DATABASE SECURITY

Advanced Email Security:

- **Real-Time Threat Analysis:** Emails and their attachments are intercepted, scanned, and analyzed for hidden threats, including malicious links, scripts, and embedded ransomware.
- **Binary-Level Validation of Attachments:** Attachments, such as PDFs, images, videos, spreadsheets, or compressed files, are converted to binary format. Each segment is compared against a comprehensive database of known malicious binary patterns.
- **Dynamic Quarantine:** Detected threats are quarantined securely, and actionable insights are provided to administrators for further investigation and response

Database File Protection:

Secure Gateway® goes beyond traditional email and web protection by safeguarding database interactions:

01

File Validation Before Insertion:

Files intended for insertion into databases (e.g., user-uploaded documents, media files, or data backups) are scanned for malicious code. This ensures only validated and clean data is allowed into critical systems.

02

Binary-Level Database Validation:

Files are dissected at the binary level to identify hidden exploits that could otherwise compromise database integrity.

Use Case Example:

An uploaded CSV file containing hidden SQL injection commands is intercepted, scanned, and flagged before it reaches the database.

HOW SECURE GATEWAY® PATENT NO. 10,630,721 ENHANCES SECURITY FOR EMAILS AND DATABASES

Intercept and Validate Files at the Gateway:

- Files, whether part of an email or destined for database insertion, are intercepted and converted into binary format for granular analysis.
- Threats such as malware embedded in metadata, macros within spreadsheets, or hidden scripts in CSV files are detected and neutralized.

Quarantine and Diagnostic Reporting:

- Detected threats are securely quarantined without reaching backend systems or databases.
- Malicious content is converted into readable text, enabling administrators to analyze and implement corrective measures.
- **Example:** A database update script with embedded malicious code is intercepted and logged before it can execute unauthorized changes.

Comprehensive Logging and Auditing:

Every interaction, including database file validations, is logged with key metadata:

- » **File origins:** Sender or upload source.
- » **Type of content:** Attachment formats and file metadata.
- » **Threat insights:** Severity levels, detection rules, and impacted systems.
- » **Database activity:** Validation outcomes for uploaded files intended for database insertion.
- » Searchable logs allow for quick analysis and compliance with audit requirements.



TECHNICAL BENEFITS OF SECURE GATEWAY® PATENT NO. 10,630,721

Binary-Level Validation for File Integrity:

- ✓ **Granular Threat Detection:** Files are analyzed at the binary level, enabling detection of threats disguised within non-standard file formats or deeply embedded in multi-layered structures.
- ✓ **Universal File Support:** Supports validation of diverse file types such as multimedia files, compressed archives, and database-oriented file formats (e.g., CSV, JSON, XML).

Use Case Example:

A user uploads an XML file to update database records. The file contains hidden malicious scripts designed to exploit server vulnerabilities. Secure Gateway® detects and isolates the threat, ensuring database integrity.

AI-Powered Adaptability for Emerging Threats:

- ✓ **Dynamic Threat Intelligence:** Regular updates to the threat database ensure real-time protection against new malware strains, ransomware variants, and advanced persistent threats (APTs).
- ✓ **Self-Learning Algorithms:** AI models learn from past threats, improving detection accuracy and reducing false positives.

Backend and Database Independence:

Operates without accessing backend servers, database configurations, or requiring API integrations.

This ensures:

- **Database Protection:**
Malicious payloads cannot bypass Secure Gateway® to reach critical database systems.
- **Zero Compatibility Issues:**
Works seamlessly with legacy and modern databases without modifications.
- **Isolated Deployment:** Secure Gateway® functions independently, maintaining complete separation between client uploads and backend systems.

Proactive Threat Containment:

Real-Time File Screening: Ensures that threats are intercepted and neutralized before they interact with sensitive systems.

Example:

A compressed file uploaded as a database backup contains an encrypted ransomware payload. Secure Gateway® decrypts and analyzes the binary content, identifying the threat and blocking the upload.

Regulatory Compliance and Forensic Insights:

- **Comprehensive Auditing:** Logs include all email and database file validation activities, aiding compliance with GDPR, HIPAA, and SOC 2 standards.
- **Forensic Analysis:** Malicious patterns are stored securely, providing valuable insights for threat research and legal investigations.

WHY SECURE GATEWAY® PATENT NO. 10,630,721 IS A CYBERSECURITY BENCHMARK



Binary-Level Accuracy:

Provides granular analysis of files, ensuring threats hidden in metadata, file headers, or compressed formats are detected.



Infrastructure Agnostic:

Works seamlessly across legacy, on-premises, and cloud environments without requiring backend software installation or code modifications.



Scalability and Future-Readiness:

Handles increasing data volumes and adapts to emerging cyber threats with ease.



End-to-End Threat Neutralization:

Covers the entire lifecycle of a file—from interception to quarantine—ensuring zero interaction with sensitive systems.

APPLICATIONS FOR SECURE GATEWAY® PATENT NO. 10,630,721 IN EMAIL AND DATABASE PROTECTION

01

Government Systems:

Protects classified email communications and sensitive database operations from phishing attacks and malicious file uploads.

Example:

A government database update receives a CSV file containing hidden SQL injection commands. Secure Gateway® blocks the malicious script before it can compromise national infrastructure.

02

Enterprises and Financial Institutions:

Shields against spear-phishing emails and ensures only validated files enter financial systems and databases.

Example:

A malicious Excel file with macros targeting financial databases is intercepted, scanned, and quarantined before delivery.

03

Healthcare and Critical Infrastructure

Safeguards patient records and operational data from ransomware attacks and data breaches.

Example:

A healthcare provider uploads patient data as a compressed archive containing hidden malware. Secure Gateway® identifies and blocks the threat, ensuring regulatory compliance.

CONCLUSION

Secure Gateway®, protected under U.S. Patent No. 10,630,721 B1, represents the next step in email and database security. By combining AI-driven threat detection, binary-level validation, and backend independence, it offers unmatched protection for enterprises and governments.

Secure Gateway® empowers organizations to:

- Prevent malicious uploads into databases and email systems.
- Maintain operational integrity and regulatory compliance.
- Deploy seamlessly without backend dependencies.

Secure Gateway® Patent No. 10,630,721 is the gold standard for scalable, robust, and future-proof cybersecurity solutions.



ALSCO® U.S. Patent No. 11,777,927 B1 (2023): ESTABLISHING SECURE COMMUNICATION CHANNELS UNDER SECURE GATEWAY®

OVERVIEW:

U.S. Patent No. 11,777,927 B1, titled "Monitoring System for Providing a Secure Communication Channel Between a Client Computer and a Hosting Computer Server," granted to ALSCO Software LLC on October 3, 2023, introduces a revolutionary advancement in secure communication and multi-factor authentication (MFA) under the Secure Gateway® platform.

For the first time in the cybersecurity industry, Secure Gateway® Patent No. 11,777,927 enables the creation of a secure, tamper-proof communication channel that operates entirely independent of backend systems, APIs, and traditional authentication methods. This groundbreaking approach allows clients to authenticate and establish a fully validated session before any interaction with the hosting server, effectively decoupling server access from authentication and verification mechanisms.

This innovative process eliminates common vulnerabilities in conventional systems, such as reliance on:

- Passwords or User IDs.
- Challenge-Handshake Authentication Protocols (CHAP).
- APIs or server-access credentials.
- Biometric Authentication mechanisms.

CORE INNOVATIONS OF SECURE GATEWAY® PATENT NO. 11,777,927

First-of-its-Kind Secure Channel Independent of Backend Servers:




| | |
|----|--|
| 01 | Isolation-First Architecture: Secure Gateway® implements a completely isolated validation layer between the client and the hosting server. No direct connection to the backend server is initiated until the client has been fully authenticated. |
| 02 | Channel Establishment Before Backend Exposure: Traditional systems authenticate users by initiating requests to backend servers. Secure Gateway® reverses this logic by establishing a secure and validated communication pathway before backend systems are involved, ensuring that servers remain invisible until authentication is complete. |
| 03 | Encryption from Entry Point: All communication between the client and Secure Gateway® is encrypted at the session's inception using dynamic cryptographic keys, ensuring confidentiality and preventing interception by unauthorized entities. |

Technical Example:

When a client device sends an authentication request, Secure Gateway® intercepts the request and validates it against pre-configured multi-factor authentication mechanisms (such as IP verification and SMS-based authentication). If the validation fails, the backend server remains completely inaccessible, preserving server invisibility.

Revolutionary Multi-Factor Authentication Without Backend Reliance:

Secure Gateway® eliminates traditional authentication dependencies such as APIs or stored credentials, replacing them with advanced MFA mechanisms:

-  **IP Address-Based Validation:** Client requests are analyzed in real-time, and only those originating from authorized IPs or geolocations are permitted access.
-  **Session Token Validation:** Each user session is assigned a unique, dynamically generated token. Reuse or unauthorized modification of tokens results in automatic session invalidation.
-  **Secure Mobile App Integration for SMS Verification:** A one-time SMS code is delivered to the user via an encrypted mobile app, ensuring that no intermediary can tamper with or intercept the verification process.

Technical Use Case Example:

An enterprise employee attempts to log into a corporate network.

Secure Gateway® first validates the request against:

- The whitelisted corporate IP range.
- A one-time SMS code delivered via a secure mobile app.
- A unique session token generated at login, ensuring that no duplicated or expired session can be used.

If any of these checks fail, the request is rejected before the backend server is contacted.



Dynamic Logging and IP Tracking for Comprehensive Oversight:

Secure Gateway® Patent No. 11,777,927 provides unparalleled transparency with logging & tracking capabilities:

- **Logs all authentication attempts with granular details, including:**
 - IP Address, ASN (Autonomous System Number), and ISP details.
 - Browser fingerprint and user-agent string.
 - Geolocation (latitude/longitude) with timestamp.
- Enables forensic investigations by correlating suspicious authentication attempts with IP patterns, browser anomalies, or geolocation inconsistencies.

Advanced Example:

During a targeted attack, an administrator identifies multiple failed login attempts originating from an unauthorized IP address in a foreign location. Secure Gateway® not only blocks these attempts but also logs comprehensive metadata (e.g., ASN, browser details) to aid in understanding the attack vector.

Seamless, Infrastructure-Agnostic Deployment:

- Requires no software installation or backend server modifications, making it compatible with legacy infrastructures, modern cloud platforms, and hybrid environments.
- Operates as a standalone validation layer, ensuring minimal operational disruption during deployment.

Technical Use Case Example:

A financial institution with a complex hybrid infrastructure deploys Secure Gateway® as an intermediary validation system. Without requiring changes to its existing servers, Secure Gateway® provides secure access for employees, customers, and third-party vendors, all while preserving backend server invisibility.

Binary-Level Threat Detection and Pre-Validation Scanning:

Before allowing any communication with backend servers, Secure Gateway® conducts binary-level validation to ensure that no malicious payloads or scripts are embedded in the communication stream.

- 01 Binary Deconstruction:** Each request is converted into binary format for precise analysis, bypassing obfuscation techniques commonly used by attackers to evade detection.
- 02 Threat Pattern Matching:** The binary stream is checked against a dynamic database of known threat patterns, ensuring that even zero-day malware or disguised attacks are identified.
- 03 Payload Isolation:** Suspicious files (e.g., PDFs, compressed files, or media with hidden scripts) are quarantined for administrator review.

Technical Use Case Example:

A financial institution with a complex hybrid infrastructure deploys Secure Gateway® as an intermediary validation system. Without requiring changes to its existing servers, Secure Gateway® provides secure access for employees, customers, and third-party vendors, all while preserving backend server invisibility.

HOW SECURE GATEWAY® PATENT NO. 11,777,927 STANDS OUT

- First-to-Market Innovation:** Secure Gateway® is the first system in the industry to fully decouple authentication from backend server access. By creating an independent validation layer, it eliminates vulnerabilities commonly exploited in traditional systems.
- Advanced Threat Resilience:** With its binary-level threat detection and pre-validation scanning, Secure Gateway® neutralizes sophisticated attacks such as:
 - Obfuscated malware.
 - Zero-day exploits embedded in communication streams.
 - Session hijacking and token replay attacks.
- Unparalleled Accountability and Transparency:** Dynamic logging tracks every authentication request, providing organizations with real-time insights into access attempts and anomalies.
- Future-Proof Security Architecture:** The modular and infrastructure-agnostic design ensures compatibility with evolving cybersecurity needs, including cloud-native and hybrid environments.

CONCLUSION

Secure Gateway® Patent No. 11,777,927 is a transformative solution in the cybersecurity landscape, providing unmatched secure communication and MFA capabilities. **By enabling:**

- A fully isolated, tamper-proof communication channel.
- Multi-layered authentication mechanisms independent of backend servers.
- Comprehensive logging and threat detection at the binary level.

Secure Gateway® Patent No. 11,777,927 redefines industry standards, empowering organizations to protect sensitive systems and data with unprecedented security and transparency.