IBM Sterling Secure Proxy

Multilayered frontline defense to prevent cyber-attacks for critical data exchanges over public and private networks.

Highlights

Provides a DMZ architecture with session termination for security

Offers In-Flight anti-virus scanning of inbound files

Prevents data leaks with proactive Data Loss Prevention scans

Captures detailed audit logs to meet compliance requirements

Sophisticated cyber threats and ransomware attacks increasingly target vulnerable external file transfers, risking critical operational continuity. Direct firewall connections expose internal networks, fail to inspect content or enforce DLP, or isolate sessions. Attackers exploit these gaps for data breaches and lateral movement.

IBM® Sterling Secure Proxy fortifies MFT and B2Bi environments against advanced cyber threats. Operating as an edge security proxy with a DMZ architecture (no data at rest), it isolates internal networks. By enforcing session breaks, real-time malware and DLP scanning, the solution blocks malicious activity. It provides end-to-end encryption, ensures compliance, and seamlessly integrates with IBM® Sterling File Gateway and IBM® Sterling B2B Integrator.

IBM® Sterling Secure Proxy provides a scalable, compliant, multi-layered solution that secures file exchanges without direct public network exposure, proactively mitigating advanced threats and ensuring uninterrupted operations.

Highlights

Provides a DMZ architecture with session termination for security
Legacy architectures expose internal networks via direct external connections, expanding the attack surface. IBM Sterling Secure Proxy mitigates this with a robust DMZ deployment, enforcing session breaks to prevent direct internal network access. All transactions are processed in-memory, eliminating data persistence within the DMZ and removing a key data theft vector.
Internal network-managed configuration further denies initial access. This per-session, Zero Trust architecture effectively blocks lateral movement and unauthorized access, providing a hardened perimeter for critical B2B infrastructure.

Offers In-Flight Anti-Virus scanning of Inbound Files
Escalating ransomware and malware attacks necessitate real-time file transfer scanning at the perimeter. Internal network infiltration allows malware to evade detection, making DMZ-level quarantine critical. IBM Sterling Secure Proxy integrates with enterprise anti-virus engines to scan inbound files before internal access. This best-practice, proactive in-flight scanning, blocks malicious payloads at the edge, preventing operational disruptions and mitigating latent infections and zero-day exploits which traditional defenses might overlook.

Prevents data leaks with proactive Data Loss Prevention scans
Organizations must prevent accidental or intentional exposure of their sensitive data during file transfer operations. IBM Sterling Secure Proxy provides an interface to send the outbound files for Data Loss Prevention scanning to inspect for any confidential information, regulatory violations or proprietary content. By integrating with DLP scanning engines, IBM Sterling Secure Proxy enforces policy driven controls to detect and block any unauthorized data transfers helping enterprises comply with GDPR, HIPAA and other industry regulations.

Captures detailed audit logs to meet compliance requirements
Meeting HIPAA, PCI DSS, NIST, and other mandates demands meticulous audit trails. IBM Sterling Secure Proxy captures comprehensive logs of all file transfers, authentication, malware/DLP events, ensuring full traceability for regulatory compliance and audits. Now, with real-time streaming of security events to IBM Sterling Control Center Monitor, organizations can receive instant alerts on brute-force and unauthorized access attempts, and flag weak cipher usage. Centralized monitoring delivers summaries of virus scans and certificate expiry, enabling proactive threat response, strengthened MFT security, and continuous compliance.

Summary

IBM Sterling Secure Proxy fortifies B2B data exchange against ransomware attacks and data breaches. Multi-layered security through session breaks, deep inspection, proactive malware scanning and DLP measures at the edge ensures robust security along with detailed logs for compliance and audits.

Ultimately, IBM Sterling Secure Proxy empowers enterprises to safeguard their sensitive data and maintain operational integrity without sacrificing performance, establishing a resilient and trusted foundation for secure B2B data exchanges.

For more information

To learn more about **IBM Sterling Secure Proxy**, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/secure-proxy

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
April 2025

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.