

Secure ICAP Gateway

Optimierte Datensicherheit für Web-Proxy-Infrastrukturen und MFT

Als Teil einer umfassenden Security-Strategie müssen Unternehmen Inhalte schützen, die über das Web hoch- oder heruntergeladen oder über verwaltete Dateitransfer-Lösungen (MFT-Lösungen) ausgetauscht werden.

Das Secure ICAP Gateway ergänzt bestehende Web-Proxy-Infrastrukturen und MFT-Software und bietet eine zusätzliche Datensicherheitsebene. Eine Engine zur tiefgreifenden Inhaltsuntersuchung erkennt sensible oder kritische Daten, sowie aktive Bedrohungen und wendet geeignete Maßnahmen an, die einen sicheren Informationsfluss gewährleisten sowie Unterbrechungen der Geschäftsprozesse reduzieren.

Das Secure ICAP Gateway wird von Sicherheits-, Finanz- und Gesundheits-Organisationen sowie von Behörden und Ministerien eingesetzt, die sicherstellen müssen, dass ihre Richtlinien zur Datensicherheit über sämtliche Kanäle hinweg konsistent sind. Diese vollständig automatisierte Lösung gewährleistet die Datensicherheit, unterstützt die Compliance-Anforderungen und vermeidet unerwünschte Datenschutzverletzungen.

ICAP-Integration

Das SECURE ICAP Gateway wurde gemäß Branchenstandard mithilfe der ICAP-Protokollschnittstelle entwickelt und bietet erweiterte Funktionen zum Schutz vor Datenverlust (Data Loss Prevention - DLP) sowie Bedrohungen für bestehende Web-Proxy-Gateways mit ICAP-Unterstützung, wie beispielsweise F5, Blue Coat, Cisco und Squid. Dieses Produkt lässt sich mühelos und ohne störende Auswirkungen in die bestehende Infrastruktur integrieren.

MFT-Integration

Die Integration des Secure ICAP Gateways mit GoAnywhere MFT von HelpSystems minimiert das Datensicherheits-Risiko für Inhalte, die mithilfe verwalteter Dateitransfer-Lösungen übermittelt werden. Die kombinierte Lösung bietet eine sichere Plattform für den Austausch von Dokumenten, die Inhalte entsprechend der Unternehmensrichtlinie überwacht, blockiert, redigiert oder bereinigt und somit sicherstellt, dass Cyber-Bedrohungen beseitigt werden und somit für den Empfänger keine Bedrohung darstellen.

PRODUKT-ZUSAMMENFASSUNG

KEY FEATURES

- Integration in bestehende Infrastrukturen mit ICAP-Unterstützung
- Forward- und Reverse-Proxy-Modi schützen Benutzer und Web-Server
- Threat Protection und Sanitization zur Bekämpfung von Malware und Phishing
- Bidirektionale Daten-Bereinigung
- in Dokumenten und Bildern zur Sicherstellung der Compliance
- Granulare Richtlinien kontrollieren den Zugriff auf Websites und Cloud-Anwendungen
- Überwachungsmodus zur Feinabstimmung von Richtlinien vor der Implementierung

SYSTEM MANAGEMENT

- Flexible und granulare Richtliniensteuerung
- Aktive Directory- oder LDAP-Integration
- Benutzerfreundliche Web-basierte Bedieneroberfläche mit rollenbasierter Zugangskontrolle
- Umfassende Workflow-Optionen
- SNMP- und SMTP-Management-Alarme

BEREITSTELLUNGSOPTIONEN

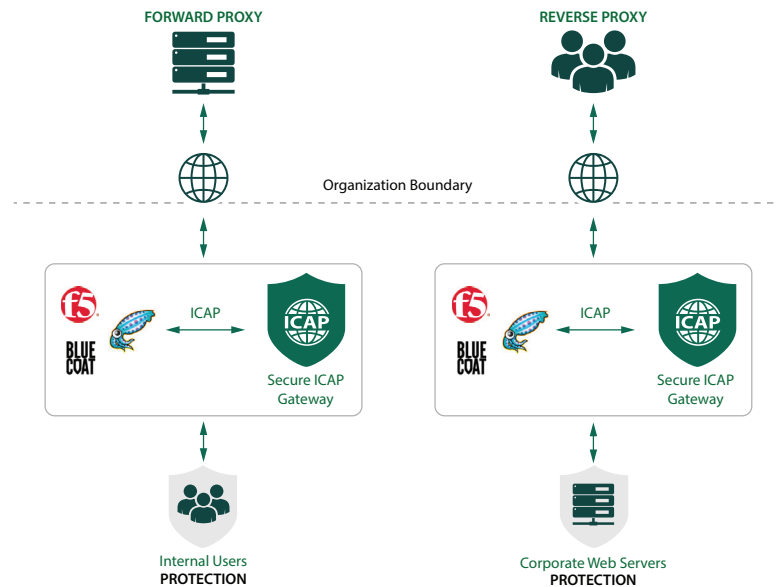
- Public Cloud-Bereitstellung in Microsoft Azure oder Amazon Web Services
- Virtuelle VMware-Umgebung
- Software-Image auf eigener oder Clearswift-Hardware

Bereitstellung Für Den Echtbetrieb

Die Verwaltung und Bereitstellung einiger DLP-Tools ist komplex und führt zu einer hohen Anzahl von Richtlinienverstößen. Das Secure ICAP Gateway verwaltet diese betrieblichen Probleme mit erweiterten, bidirektionalen Funktionen, die den Austausch nicht autorisierter Daten einschränken und gleichzeitig die False Positives minimieren, die die Unternehmensproduktivität einschränken können. Die Verbindung zu externen Datenquellen und lexikalische Abfragekriterien ermöglichen dem Secure ICAP Gateway die präzise Bestimmung realer Datenverlustrisiken, bevor es zu Verstößen kommt.

Flexible und granulare Richtlinien erlauben die Ausführung unterschiedlicher Workflows abhängig vom jeweiligen Verstoß. Inhalte können in Echtzeit dynamisch modifiziert werden, um eine kontinuierliche und konforme Zusammenarbeit zu ermöglichen. Integrierte Compliance-Wörterbücher und mehr als 200 vordefinierte PCI- und PII-Tokens erleichtern die Definition von Richtlinien sowie die Aufrechterhaltung der Compliance.

Das Secure ICAP Gateway arbeitet sowohl im Forward- als auch im Reverse-Proxy-Modus und bietet so einen umfassenden Schutz für ein- und ausgehende Aktivitäten



Deep Content-Inspektion

Eine Engine zur tiefgreifenden Inhaltsuntersuchung (Deep Content Inspection - DCI) führt eine vollständige Aufgliederung des Kommunikationsflusses in Echtzeit durch und wendet, abhängig vom Inhalt, Kontext sowie den gesetzlichen Vorschriften, die entsprechende Richtlinie an. Eine kontextsensitive Scan-Funktion unterstützt das Erkennen und Vermeiden von Szenarien, in denen Benutzer versuchen, Dokumente hochzuladen, die geistiges Eigentum enthalten, beispielsweise auf Schatten-IT-Websites oder über Cloud-Filesharing-Anwendungen wie Dropbox.

Die DCI-Engine bietet darüber hinaus eine Erkennung der tatsächlichen Dateitypen sowie die Verifizierung der Dateistruktur, um das Herunterladen ausführbarer Dateien zu verhindern.

Adaptive Redaktion

Statt durch das Secure ICAP Gateway geleitete Inhalte lediglich zu blockieren, ermöglicht Adaptive Redaction eine Bereinigung sensibler oder kritischer Daten in Microsoft Office-, Open Office-, PDF- und Bilddateien in Echtzeit und gewährleistet so deren Sicherheit.

Data Redaction – Sensible Daten oder kritische Informationen werden automatisch aus Dokumenten und Bildern entfernt. OCR (Optical Character Recognition) erkennt in Bildern verborgenen Text.

Document and Image Sanitization – Metadaten, Änderungsverläufe und Eigenschaften werden aus den Dateien entfernt.

Structural Sanitization – Aktiver Code (Makros, Skripte und ActiveX-Elemente) wird aus gängigen Dokumentformaten entfernt.

Advanced Threat Protection

Das Secure ICAP Gateway ist mit Avira-, Kaspersky- oder Sophos-Anti-Malware-Produkten erhältlich, die automatisch aktualisiert werden, damit sie stets aktuellen Schutz bieten. Diese Technologien werden durch Structural Sanitization ergänzt, mit dessen Hilfe aktive Inhalte aus Dokumenten und Websites in Echtzeit und ohne jegliche Verzögerungen entfernt werden.

Benutzer werden am Zugriff auf unzulässige Websites gehindert, die in einer URL-Datenbank mit Millionen von Websites und Milliarden von Unterseiten enthalten sind. Die Datenbank enthält Details zu Sicherheits-Risikokategorien, einschließlich Malware- und Phishing-Kategorien und wird kontinuierlich aktualisiert, um zusätzlichen Schutz zu bieten. Mehr als 50 Millionen neuer Websites werden jährlich hinzugefügt, von denen einige jedoch nicht kategorisiert werden. In diesem Fall erkennt eine Echtzeitkategorisierung die Merkmale risikobehafteter Websites und verhindert den Zugriff darauf.

Kontrolle Des Zugriffs Auf Web 2.0

Das Definieren von Richtlinien für den Zugriff auf die Websites beliebter sozialer Medien ist einfach. Verschiedene Zugriffsregeln können auf individueller oder Abteilungsebene definiert werden und jeder Route werden bereits vordefinierte Inhaltsregeln zugeordnet. So kann beispielsweise der Zugriff auf YouTube gestattet, der auf unangemessene Inhalte jedoch eingeschränkt werden.

The screenshot shows the 'Routes' configuration window. At the top, there is a toolbar with icons for New, Identify, Edit, Delete, Copy, Color, Disable, and Show rules. Below the toolbar, it states '6 Routes defined (applied in the order shown)'. The main area contains a table with the following data:

	Action	From	To	Rules
1.	Allow	Everyone	Trusted Sites	
2.	Block	Everyone	Security Risk	7
3.	Block	Everyone	Inappropriate sites	7
4.	Allow	Everyone	YouTube	11
5.	Allow	Everyone	Web Mail & Chat	10
6.	Allow	traffic that does not match another route		9

Below the table, a flowchart displays 10 security rules in a sequence:

1. Block Virus
2. Block Encrypted Data
3. Strip Active Content
4. Block Spyware Call Home
5. Block Executables
6. Track Uploading PCI Content
7. Redact outgoing PII information
8. Remove Tracking Cookie
9. Block uploading of Profanity
10. Processing of request or response fails ...

Lassen Sie Uns Starten

Sehen Sie sich das Secure ICAP Gateway in Aktion an: Besuchen Sie uns unter www.clearswift.de und wir vereinbaren eine Produktdemo.

FORTRA

Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.