Trend Micro™

INTERSCAN™ WEB SECURITY

Bester Schutz vor Internetbedrohungen und Kontrolle über ungeschützte Nutzung des Internets

Herkömmliche Sicherheitslösungen für Internet-Gateways, die auf regelmäßigen Updates gegen Cyberbedrohungen beruhen, können mit den sich rasant entwickelnden Internetbedrohungen von heute nicht mehr Schritt halten. Sicherheitsadministratoren müssen nicht nur bösartigen Code, gezielte Angriffe und den Zugriff auf unangemessene Webseiten verhindern. Ihnen obliegt darüber hinaus die Verantwortung, den zunehmenden Einsatz von Web 2.0 und cloudbasierten Anwendungen dauerhaft zu gewährleisten und gleichzeitig Kosten für die Verwaltung und Bandbreite zu senken.

Trend Micro™ InterScan™ Web Security bietet umfassenden Schutz vor Cyberbedrohungen am Internet-Gateway. Angesichts der wachsenden Nutzung cloudbasierter Consumer-Anwendungen am Arbeitsplatz ist Applikationstransparenz ein wesentlicher Faktor bei der Erkennung von Netzwerkrisiken. Durch die Integration von Anwendungssteuerung, Suche nach Zero-Day-Exploits und Malware, Erkennung zielgerichteter Angriffe, Web Reputation in Echtzeit, URL-Filtern und Botnetzerkennung schützt InterScan Web Security Ihr Netzwerk optimal vor komplexen Bedrohungen. Durch die optionale Integration von **Deep Discovery Advisor** können zudem Sandbox-Analysen von verdächtigen Dateien durchgeführt werden. Das sorgt für mehr Transparenz und bietet Schutz vor komplexen, zielgerichteten Bedrohungen aus dem Internet, wie beispielsweise Watering-Hole-Angriffe.

Mit dem integrierten Schutz vor Datenverlust (DLP) für InterScan Web Security können Sie zudem verhindern, dass vertrauliche Daten Ihr Unternehmen verlassen. Das optionale Data Loss Prevention Modul filtert mithilfe von anpassbaren Vorlagen Daten, um Sie bei der Einhaltung von Compliance-Richtlinien und dem Datenschutz zu unterstützen. Mit dem integrierten Schutz vor Datenverlust am Internet-Gateway haben Sie folgende Möglichkeiten:

- Durchsuchen des ausgehenden Datenverkehrs auf sensible Daten
- Erstellen von Richtlinien anhand vordefinierter Vorlagen, um die Einhaltung gesetzlicher Datenschutzbestimmungen in unterschiedlichen Ländern durch Filtern von personenbezogenen Daten zu verbessern
- Erstellen von Reports zu DLP-Richtlinienverletzungen bestimmter Anwender
- Bereitstellen von Audit-Funktionen, mit denen sich die Wirksamkeit von DLP-Richtlinien beurteilen lässt

SICHERHEIT FÜR INTERNET-GATEWAYS

Geschützte Punkte

- Internet-Gateway

Schutz vor Bedrohungen

- Cloudbasierte Anwendungen
- Web 2.0-Anwendungen
- Komplexe, zielgerichtete Angriffe
- Zero-Day-Exploits
- Malware
- Datenverlust
- Viren und Würmer
- Bots und Callbacks zu C&C-Servern
- Spyware und Keylogger
- Bösartiger mobiler Code
- Rootkits
- Phishing-Angriffe
- Content-Bedrohungen

Integrierbar in:

- LDAP
- Active Directory™
- SNMP

WESENTLICHE VORTEILE

Bester Schutz

- Entlastet Endpunkt-Sicherheitslösungen und stoppt mehr Bedrohungen am Gateway durch die integrierte Suche nach Zero-Day-Exploits und Malware, Erkennung von komplexen, zielgerichteten Angriffen mit Web Reputation, URL-Filtern sowie Schutz vor Java Applet und ActiveX Code.
- Gewährleistet sicheren und angemessenen Zugriff auf Webinhalte durch die Überwachung des Internetverkehrs auf bösartige Inhalte
- Wehrt neue Bedrohungen umgehend ab
- Bietet schnelle Updates für sofortigen Schutz

Transparenz und Kontrolle

- Zentrale Verwaltung mehrerer Instanzen und Standorte in Echtzeit
- Überwacht die Internetnutzung in Echtzeit, was ein sofortiges Eingreifen ermöglicht
- Verwaltungs- und Reporting-Funktionen für über 1000 Internetprotokolle und -anwendungen
- Ermöglicht die Erstellung detaillierter Richtlinien zur Kontrolle aller Internetaktivitäten, einschließlich der Nutzungszeit

Weniger Verwaltungsaufwand und -kosten

- Verbessert die Auslastung vorhandener Server, verringert Wildwuchs und Energiekosten
- Wird als virtuelle Appliance oder Software-Appliance zur Konsolidierung und Standardisierung von Rechenzentren eingesetzt
- Zentralisiert die Verwaltung von verteilten Internet-Gateways im gesamten WAN
- Erhöht die Sicherheitsstufe durch die schnelle Bereitstellung neuer Funktionen
- Beschleunigt die Wiederherstellung nach Netzwerkausfällen durch native Ausfallsicherheit und Redundanz
- Vereinfacht Betriebssystem- und Sicherheitsupdates, Versionskontrollen und Tests

WICHTIGSTE FUNKTIONEN

Transparenz und Kontrolle von Anwendungen

- Überwachungs- und Reporting-Funktionen für über 1000 Internetprotokolle und -anwendungen, darunter Instant Messaging, Peer-to-Peer, soziale Netzwerke und Streaming Media
- Anwender können auf cloudbasierte Anwendungen zugreifen, während die Durchsetzung zulässiger Richtlinien für die Eindämmung von Risiken und die Einsparung von Ressourcen sorgt
- Ermöglicht die Erstellung detaillierter Richtlinien zur Kontrolle aller Internet-aktivitäten und der Nutzungszeit von Anwendern

Mehrfach ausgezeichneter Gateway-Schutz vor Viren und Spyware

- Durchsucht ein- und ausgehenden Daten-verkehr nach Malware
- Stoppt Malware, bevor sie in Ihr Netzwerk eindringt und entlastet so die Endpunkt-Sicherheitslösung
- Verhindert Viren- und Spyware-Downloads, Botnetze, Malware-Callback-Versuche sowie den Aufbau von Tunnels durch Malware
- Schließt die HTTPS-Sicherheitslücke durch die Entschlüsselung und Prüfung von ver-schlüsselten Inhalten
- Bietet Unternehmen die Möglichkeit, den HTTPS-Verkehr wahlweise zu entschlüsseln, um Content Security und den Schutz der Privatsphäre von Anwendern in die Balance zu bringen

Web Reputation mit korrelierten Bedrohungsdaten

Die Web-Reputation-Technologie des Trend Micro™ Smart Protection Network™ blockiert den Zugriff auf Webseiten mit bösartigen Aktivitäten

- Schützt in Echtzeit vor neuen Bedrohungen und verdächtigen Aktivitäten
- Erkennt und blockiert Botnetze und gezielte Angriffe durch Command-and-Control-Kommunikation (C&C) mithilfe globaler und lokaler Informationen über Bedrohungen

Leistungsstarke und flexible URL-Filter und Filterfunktionen für aktiven Code

- Identifiziert Webseiten mit bösartigen oder unangemessenen Inhalten mit Hilfe von URL-Kategorisierung und -Reputation in Echtzeit
- Bietet sechs verschiedene Richtlinien-aktionen für die Internetzugriffskontrolle einschließlich Überwachen, Zulassen, Warnen, Blockieren, Blockieren mit Kenn-wortzurücksetzung und Durchsetzen von Zeitkontingenten
- Unterstützt das Blockieren auf Objektebene innerhalb dynamischer Webseiten wie Web 2.0 Mashups
- Stoppt „Drive-by-Downloads" und blockiert den Zugriff auf Spyware- und Phishing-Webseiten

Erkennung komplexer Bedrohungen

Der optionale Deep Discovery Advisor wendet zusätzliche Bedrohungsdaten an, indem Sandbox-Analysen zur Offline-Inspektion verdächtiger Dateien durchgeführt werden.

- Löst Dateien in benutzerdefinierbaren Sandbox-Umgebungen aus und überwacht diese auf gefährliche Verhaltensweisen
- Korreliert umfassende forensische Analysen mit Trend Micro Bedrohungs-daten, um Informationen zum Angriff und Angreifer bereitzustellen
- Nutzt adaptive Sicherheitsupdates, um neue C&C-Server zu sperren, die während der Analyse gefunden wurden
- Identifiziert Angriffe mittels regelmäßig aktualisierter Erkennungsdaten und Korrelationsregeln vom Smart Protection Network und dedizierter Bedrohungs-forschung

Echtzeit-Reporting und zentrale Verwaltung

Zentralisiert Protokollierung, Reporting, Konfigurationsverwaltung und Richtlinien-synchronisierung auf mehreren InterScan Web Security Servern unabhängig vom geografischen Standort. Über eine einzige Konsole können Administratoren die Internet-nutzung ihres Unternehmens effektiver überwachen, verwalten und schützen.

- Bietet unübertroffene Transparenz durch Überwachung der Internetaktivitäten in Echtzeit
- Macht das Reporting zu einem proaktiven Mittel zur Entscheidungsfindung und ermöglicht sofortiges Eingreifen
- Zentralisiert die Konfiguration und das Reporting mehrerer Instanzen der virtuellen Software-Appliance
- Unterstützt die Erstellung benutzer-definierter Reports
- Unterstützt anonymes Protokollieren und Reporting, um persönliche Daten von End-benutzern zu schützen
- Entlastet einzelne Server beim Reporting und bei der Protokollierung und erlaubt dadurch einen höheren Datendurchsatz, niedrigere Latenzzeiten sowie Verlaufs-reports

Data Loss Prevention Add-on-Modul

Erweitern Sie Ihre bestehende Sicherheit, um Compliance-Richtlinien einzuhalten und Datenverluste zu verhindern. Die in InterScan Web Security integrierte DLP-Funktion ist mit einem einzigen Klick aktiviert und ermöglicht Transparenz und Kontrolle über Daten während der Übertragung.

- Verfolgt und dokumentiert vertrauliche Daten, die durch Netzwerk-Austrittspunkte fließen
- Erkennt riskante Geschäftsprozesse und verbessert Richtlinien zur Nutzung von Unternehmensdaten
- Erkennt und stoppt die unzulässige Nutzung von Daten basierend auf Schlüsselwörtern, regulären Ausdrücken und Dateiattributen
- Reduziert den Verwaltungsaufwand durch die zentrale Verwaltung mit dem Trend Micro Control Manager zusammen mit anderen Endpunkt- und E-Mail-DLP-Modulen
- Vereinfacht die Implementierung durch ein Add-on-Modul, ohne dass zusätzliche Hardware oder Software erforderlich wären

DLP-Vorlagen (Data Loss Prevention) für Compliance-Richtlinien

Über 100 direkt nutzbare DLP-Vorlagen schützen vertrauliche und personenbezogene Daten und erfüllen die wichtigsten Compliance-Richtlinien

Regulatorische Compliance

- PCI/DSS – Internationaler Datensicherheits-standard für Kreditkarten
- IBAN – International Bank Account Number (Internationale Kontonummer)
- US HIPAA – Legt Standards für alle Gesund-heitsorganisationen in den USA fest
- US Gramm-Leach-Bliley Act (GLBA) – Legt Datenschutzrichtlinien für Banken, Versicherungen und Investment-unternehmen fest
- US SB-1386 – Bezieht sich auf Gesetze zu Datensicherheitsverstößen
- UK NHS Number – Dient zur Identifizierung von Patienten im Vereinigten Königreich und zur Lokalisierung von Gesundheits-daten

Personenbezogene Daten

- Bank- und Finanzdaten
- Daten von Karteninhabern

Andere

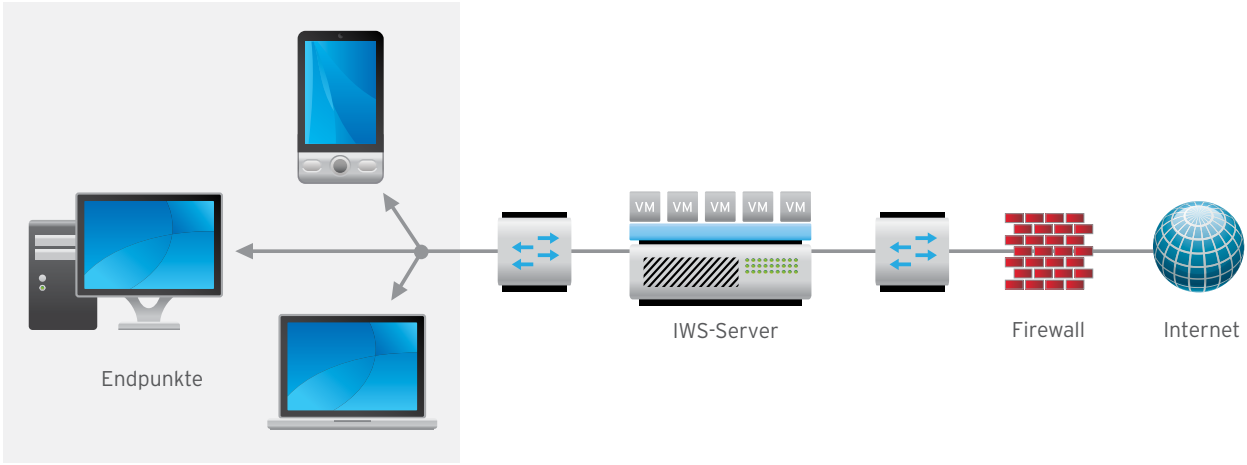
- Quellcode-Identifikatoren
- Ausführbare Dateien
- Über 170 verschiedene Dateitypen, ein-schließlich MS Office-, Datenbank-, Multi-media- und komprimierter Dateien
- Und vieles mehr

MEHRERE INSTALLATIONSMODI

InterScan Web Security (IWS) wurde entwickelt, um Ihre speziellen Bedürfnisse zu erfüllen. Die Lösung bietet verschiedene Installationsoptionen in Netzwerken an, darunter den transparenten Bridge-Modus, ICAP, WCCP, Forward Proxy oder Reverse Proxy.

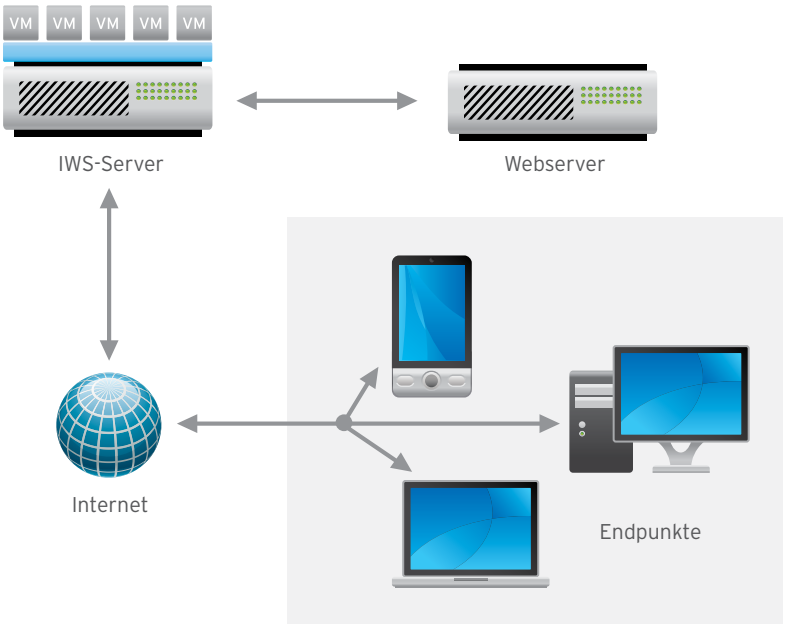
Transparenter Bridge-Modus

In diesem Modus agiert IWS als Brücke zwischen zwei Netzwerksegmenten und durchsucht auf transparente Weise den gesamten Verkehr, zusätzlich zum HTTP(s)- und FTP-Verkehr. Der transparente Bridge-Modus ist die einfachste Möglichkeit, um die Lösung in eine vorhandene Netzwerktopologie zu implementieren und erfordert keine Änderungen an Clients, Routern oder Switches. IWS agiert hier als "bump in the wire", ist dem Netzwerk also vorgelagert, und bietet gleichzeitig alle Content Security-Funktionen der Lösung.



Reverse Proxy

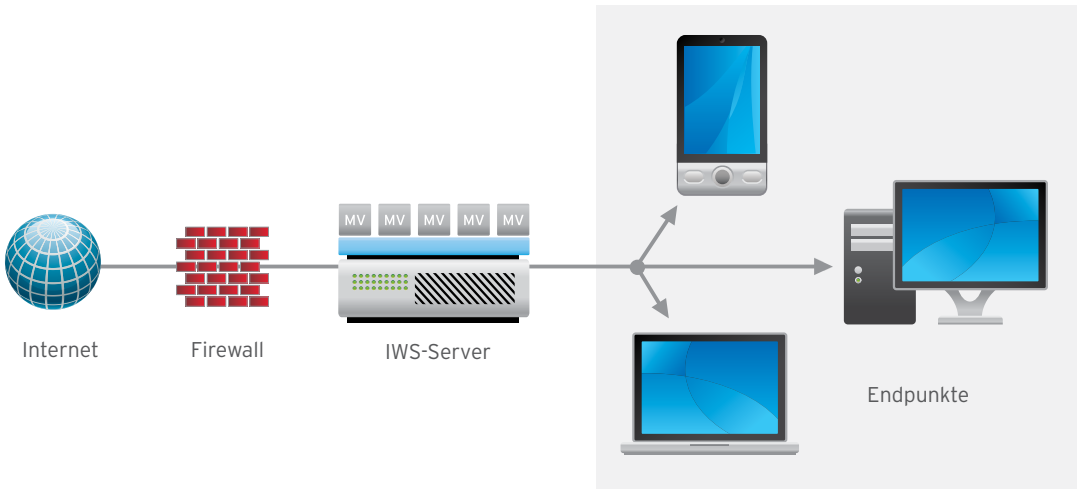
IWS kann als Reverse Proxy installiert werden, um einen Webserver vor Malware-Uploads zu schützen. Im Reverse Proxy-Modus wird die Lösung vor dem zu schützenden Webserver installiert. Dieser Modus ist sinnvoll, wenn der Webserver Dateiuploads von Clients akzeptiert. xSPs können die Lösung als HTTP-Proxy nutzen, um hochgeladene Daten für Kunden mit interaktiven Webseiten zu schützen und zu überwachen.



MEHRERE INSTALLATIONSMODI (FORTS.)

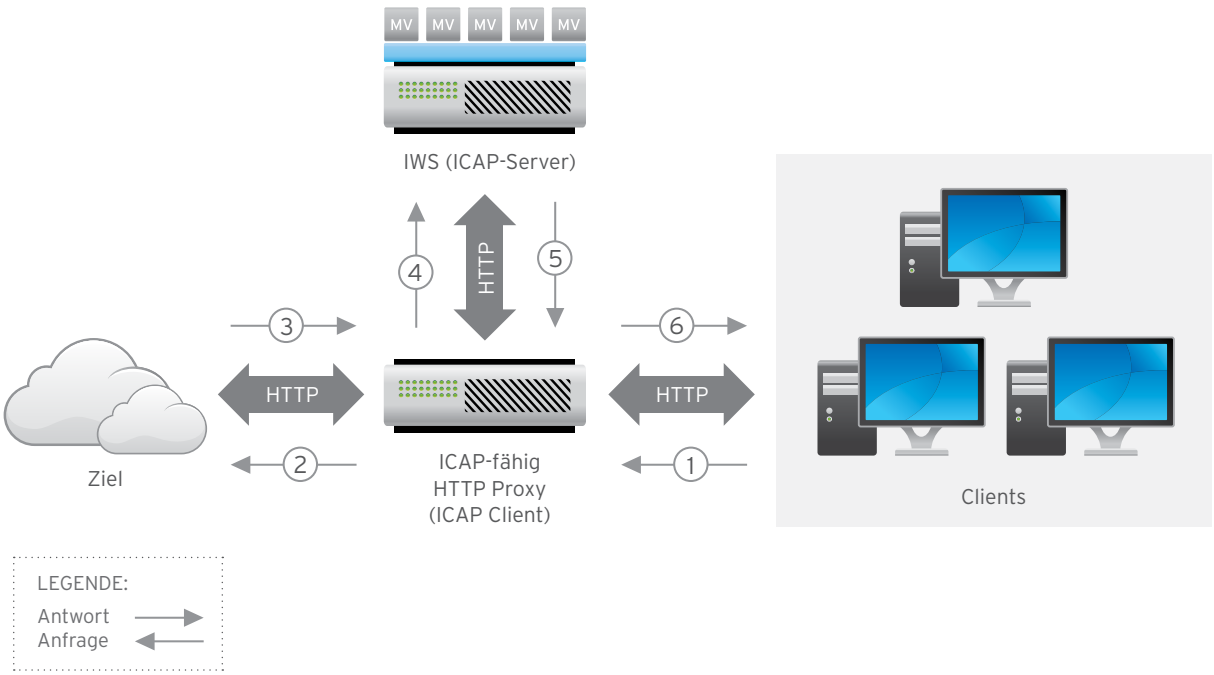
Forward Proxy

IWS kann als dedizierter Proxy für Netzwerk-Clients installiert werden. Sowohl explizite als auch transparente Proxy-Implementierungen sind je nach vorhandener Proxy-Infrastruktur möglich. ICAP und WCCP werden auch für Netzwerke unterstützt, die ein selektives Routing des Internetverkehrs von einem vorhandenen Proxy oder anderen Netzwerkgerät erfordern.



Internet Content Adaption Protocol (ICAP)

IWS unterstützt die Integration von externen Cache-, Proxy- und Storage-Servern über die ICAP v1.0 Schnittstelle, wie beispielsweise Blue Coat Proxy, EMC Isilon Scale-Out Network-Attached Storage (NAS), NetApp NetCache und Cisco Content Engines. Bei der ICAP-Installation lässt IWS ICAP-Verbindungen von einem ICAP v1.0-Server zu und schützt alle Inhalte, die auf den Server und anschließend dem Anwender zurückgegeben werden.



INSTALLATIONSOPTIONEN

Software-Appliance

- „Bare-Metal"-Installation mit optimiertem, robustem Betriebssystem
- **Von Trend Micro zertifiziert:** In ausführlichen Tests und Prüfungen zertifiziert Trend Micro Hardwareplattformen hinsichtlich der Kompatibilität mit Trend Micro Software-Appliances. Von Trend Micro zertifizierte Serverplattformen finden Sie unter: www.trendmicro.com/go/certified

Virtuelle Appliance

- Virtualisierte Bereitstellung über Hypervisor-Technologien
- Microsoft® Hyper-V™ Virtual Appliance
- VMware Ready-zertifizierte virtuelle Appliance: Gründlich getestet und geprüft von VMware; ausgezeichnet durch VMware Ready-Zertifizierung. Unterstützung von VMware ESX oder ESXi v3.5 (oder höher) und vSphere

MINDESTSYSTEMVORAUSSETZUNGEN

Server-Plattform-Kompatibilität

Virtuelle Appliances:

- VMware ESX/ESXi v3.5 und höher; Microsoft Hyper-V Windows 2008 SP1 oder Windows 2008 R2
- Windows Server 2012 Hyper-V

Software-Appliances:

- Die neuesten, von Trend Micro zertifizierten Plattformen finden Sie unter www.trendmicro.com/go/certified

Prozessor

Mindestvoraussetzungen:

- 2,0 GHz Intel™ Core2Duo™ Einzelprozessor (64 Bit) mit Unterstützung für Intel VT™ oder vergleichbarer Prozessor

Empfohlen:

- Für bis zu 4000 Anwender: 2,8 GHz Intel Core2Duo Dual-Prozessor (64 Bit) oder vergleichbarer Prozessor
- Für bis zu 9500 Anwender: 3,16 GHz Intel QuadCore™ Dual-Prozessor (64 Bit) oder vergleichbarer Prozessor

Arbeitsspeicher

Mindestvoraussetzungen:

- 4 GB Arbeitsspeicher

Empfohlen:

- Für bis zu 4000 Anwender: 6 GB Arbeitsspeicher
- Für bis zu 9500 Anwender: 24 GB Arbeitsspeicher
- Für bis zu 15.000 Anwender: 32 GB Arbeitsspeicher

Festplattenspeicher

Mindestvoraussetzungen:

- 20 GB Festplattenspeicher

Empfohlen:

- 300 GB Festplattenspeicher (partitioniert den erkannten Festplattenspeicher automatisch wie erforderlich)

TREND MICRO™

Securing Your Journey to the Cloud