



Anwendungsbereitstellungs-Netzwerke:
das neue Muss für Sichtbarkeit, Beschleunigung und Sicherheit in der IT >



Anwendungsbereitstellungs-Netzwerke: das neue Muss für Sichtbarkeit, Beschleunigung und Sicherheit in der IT

Ihr Geschäft hängt wesentlich davon ab, dass Sie den richtigen Personen zum richtigen Zeitpunkt die richtigen Informationen übermitteln. Um Wettbewerbsvorteile zu erlangen, den Kundenservice zu verbessern und auf umfassendere geschäftliche Informationen zugreifen zu können, müssen Sie eine schnelle und reaktionsfähige Anwendungsbereitstellung für Nutzer an jedem Ort sicherstellen. Zugleich müssen Sie Nutzer, Systeme und Anwendungen vor Bedrohungen schützen, damit Mitarbeiter, Kunden und Partner sorgenfrei geschäftliche Transaktionen tätigen können, sei es mit Oracle, Salesforce.com oder VoIP.

Die wesentlichen Trends der heutigen Geschäftswelt – Zentralisierung, Mobilität und Globalisierung – machen es oft schwierig, wenn nicht geradezu unmöglich, eine bedarfsgesteuerte Anwendungsbereitstellung zu unterstützen. IT-Initiativen wie die Konsolidierung von Servern und die Konvergenz von Sprache, Video und Daten können den Netzwerkbetrieb stören. Ihre mobilen Anwendungen und Geräte können durch Sicherheitslücken und Datendiebstähle gefährdet sein. Außerdem enthalten globale IT-Infrastrukturen oft Dateninseln, die schwer zu durchdringen und zu verwalten sind und die die Sichtbarkeit Ihrer IT-Ressourcen verringern.

Wenn Sie nicht die Informationsbereitstellung unterstützen, die Ihr Geschäft erfordert, müssen Sie die Technologien überdenken, mit denen Sie die Anwendungsleistung überwachen, Ihr WAN optimieren und Ihr Web-Gateway sichern. Zusammen sind diese Funktionen unerlässlich, um die heutigen Geschäftsanforderungen zu erfüllen und sich auf die Notwendigkeiten von morgen vorzubereiten.

Die Verwaltung neuer Geschäftsfaktoren erfordert einen neuen Ansatz

Unternehmen, die eine größere Zentralisierung, Mobilität und Globalisierung der IT anstreben, müssen:

- > Ihre IT- und Geschäftsprozesse besser durchschauen.
 - > Informationsbereitstellung und Geschäftsergebnisse im gesamten Unternehmen beschleunigen.
 - > Sicherheit für Daten und Nutzer an beliebigen Orten bieten.
- Um diese Ziele zu erreichen, müssen Sie zuerst verstehen, wie sich diese Geschäftsfaktoren auf Ihre Infrastruktur auswirken.

Zentralisierung: die Herausforderung, größere Kontrolle und Flexibilität zu erreichen

Unternehmen wie Ihres suchen immer nach neuen Möglichkeiten, Ressourcen zu zentralisieren, um mehr Kontrolle über die IT zu erlangen und Verwaltungskosten zu senken. Je mehr Sie Ihre Infrastruktur erweitern, umso intensiver müssen Sie konsolidieren. Sie können:



- > Die Konsolidierung von Servern in Zweigniederlassungen ermöglichen.
- > Sicherstellen, dass auch bei schwerwiegenden IT-Ausfällen der Geschäftsbetrieb aufrechterhalten werden kann.
- > Backup- und Recovery-Vorgänge beschleunigen.
- > Mehr Kontrolle über WAN- und Internet-Gateway-Verbindungen erlangen.
- > Die Flexibilität für innovative Webtechnologien vergrößern.

Die Zügel Ihrer Informationsressourcen fester anzuziehen, kann jedoch auch Nachteile haben. Durch Zentralisierung kann die Anwendungsleistung für Mitarbeiter in Zweigniederlassungen verschlechtert werden, was die Beweglichkeit in einer veränderlichen Geschäftsumgebung verringert. Eine strenge Richtliniendurchsetzung kann gelegentlich dazu führen, dass Nutzer nicht auf Web 2.0-Anwendungen und -Mashups zugreifen können, die sie für legitime geschäftliche Zwecke verwenden möchten. Daher steht die IT vor der Herausforderung, eine zentrale Kontrolle zu erlangen und aufrechtzuerhalten und dennoch eine flexible Anwendungsbereitstellung im gesamten Unternehmen zu bieten.

Mobilität: Beschleunigung von Anwendungen und Daten jederzeit, an jedem Ort

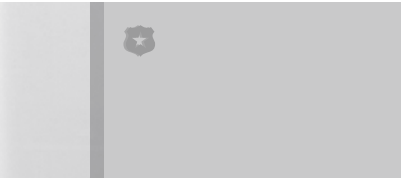
Jedes Unternehmen, das in der heutigen Wirtschaft wirklich wettbewerbsfähig sein möchte, muss sich auf eine geschäftliche Zukunft vorbereiten, die auf Konnektivität an jedem Ort und nahtlosem Zugriff auf Informationen beruht. Es reicht nicht, die Verwendung von Websites zu forcieren. Ihr Unternehmen muss Technologie intelligent und effektiv verwenden, um die Konnektivität von praktisch überall aus zu ermöglichen. Dabei muss die IT geschäftlichen Führungskräften darlegen, wie neue mobile Technologien Geschäftsziele direkt unterstützen können, wie z. B. die Erhöhung des Umsatzes und der Kundenzufriedenheit.

Letztlich sind die Ziele erhöhter Mobilität die Verbesserung der Unternehmensproduktivität und:

- > Die Beschleunigung von Geschäftsprozessen und Kommunikation.
- > Die Unterstützung wichtiger Unternehmensinitiativen, wie z. B. von Schulungsvideos, VoIP und der Einführung neuer Anwendungen.
- > Die Bereitstellung der gleichen Sicherheit und Leistung wie in der Hauptniederlassung an jedem beliebigen Arbeitsort.

Natürlich bedeutet eine beschleunigte Informationsübertragung in alle Teile der Welt bedeutende Sicherheitsrisiken. Um die bedarfsgesteuerte Informationsbereitstellung erfolgreich zu verwalten, müssen Sie die Möglichkeit haben, unternehmenswichtigen Datenverkehr von schädlichem zu unterscheiden, datenbezogene Sicherheitslücken zu verhindern und sicherzustellen, dass Ihr Unternehmen behördliche Vorschriften einhält. Sie müssen außerdem die zunehmende Belastung Ihres Netzwerks durch Web 2.0-Anwendungen, -Video-Sites und -Mashups verwalten.

Leider reicht es nicht aus, Datenverkehr zu fragwürdigen Sites und Inhalten zu blockieren. Sie benötigen effektive Möglichkeiten, die Bandbreitenanforderungen



zu steuern, die durch private Internetverwendung entstehen, ohne den Zugriff vollständig zu verwehren. Aufgabe der IT ist die Fähigkeit, mobile Technologien und Webanwendungen zu nutzen, um wichtige Unternehmensinitiativen zu unterstützen und zugleich die Sicherheit und die Integrität vertraulicher Geschäftsdaten zu wahren.

Globalisierung: Sichere Skalierung Ihres Geschäfts für neue Wachstumschancen

Die Globalisierung ist heute einer der wichtigsten Geschäftsfaktoren. Jedes Unternehmen, das weltweit erfolgreich sein möchte, benötigt die richtige Mischung aus taktischen und visionären IT-Führungsqualitäten, um alltägliche Verwaltungsprobleme zu lösen und sich zugleich strategisch auf zukünftige Wachstumschancen vorzubereiten. Je mehr sich Ihr Unternehmen weltweit ausdehnt, umso mehr muss Ihre IT-Abteilung:

- > Risiken mindern und die Einhaltung von Vorschriften sicherstellen, indem sie integrierte Kontrollmechanismen für die Netzwerksicherheit auf der Grundlage von Sichtbarkeit, Informationen und Richtlinien umsetzt.
- > Richtlinien bedarfsgesteuert ändern, um unmittelbar auf Weiterentwicklungen von Technologien, organisatorische Bedingungen und Realitäten der Märkte zu reagieren.
- > Datenlecks verhindern, indem sie zentralisierte, richtlinienbasierte Kontrollmechanismen für Netzwerkverwendung und -zugriff einrichtet.
- > Proaktiv auf Anforderungen an die Anwendungsleistung in einem wachsenden verteilten Unternehmen reagieren.

Beispielsweise hängen globale Transaktionen heute zunehmend von Software-as-a-Service (SaaS)-Anwendungen wie Salesforce.com sowie von vereinheitlichter Kommunikation wie Videokonferenzen und Instant Messaging ab. Außerdem werden in serviceorientierten Architekturen (SOA) Anwendungen und Daten aus mehreren Quellen kombiniert, sodass Ihre Infrastruktur erkennen muss, was unternehmenswichtig ist und was nicht. Sie müssen wichtige Anwendungen beschleunigen, unerwünschten oder gefährlichen Datenverkehr blockieren und alles dazwischen verwalten oder unter Kontrolle halten.

Zusätzlich zur Optimierung der täglichen Netzwerkleistung bereiten viele Unternehmen bereits die nächste Phase jederzeit und überall verfügbarer Geschäftsanwendungen vor, indem sie die Konvergenz von Sprach-, Video- und Datennetzwerken umsetzen. Die geschäftlichen Vorteile der Netzwerkkonvergenz liegen auf der Hand: schnelle, zuverlässige Kommunikation in Echtzeit, nie da gewesene Informationsmobilität und Mitarbeiterflexibilität sowie die Möglichkeit, Daten vieler Arten unmittelbar an so gut wie jedes Gerät weltweit zu übermitteln. Aber wie können Sie sicherstellen, dass diese neuen Modelle der Anwendungsbereitstellung die Sicherheitsrichtlinien Ihres Unternehmens umsetzen, Sicherheitsrisiken mindern und Ihnen helfen, Vorschriften einzuhalten?

Und noch wichtiger: Wie wird die Informationsübermittlung in wenigen Jahren aussehen, und wie sollten Sie sich jetzt darauf vorbereiten? Diese Fragen müssen



IT-Führungskräfte beantworten, um die Wettbewerbsfähigkeit ihres Unternehmens an den globalen Märkten aufrechtzuerhalten.

Die Zukunft der Anwendungsbereitstellung

Zwar sind die Herausforderungen der Konsolidierung und Mobilitätserhöhung globaler IT-Ressourcen alles andere als einfach; Sie können sie jedoch angehen, indem Sie herausfinden, wie Sie mehr Sichtbarkeit, Beschleunigung und Sicherheit für Anwendungen in Ihrer Infrastruktur erreichen.

Eines der größten Hindernisse für die Bereitstellung schneller, sicherer und zuverlässiger Anwendungsleistung liegt in der Verbindungsschicht. Zwar können Netzwerke Datenverkehr sehr effizient routen und Pakete übermitteln, aber die Verbindungsschicht kann nicht bestimmen, ob der Inhalt nützlich, schädlich oder sogar potenziell katastrophal ist. Um die Qualität von Netzwerktransaktionen, die Anwendungsleistung und die Nutzererfahrungen im gesamten Netzwerk hinreichend zu bewerten, benötigen Sie eine neue Schicht der IT-Kontrolle, auf der Sie zuverlässig Anwendungen und nicht nur Datenpakete übermitteln können.

Das Anwendungsbereitstellungs-Netzwerk: Eine neue Schicht intelligenter Kontrolle

Während viele Unternehmen die einzelnen Probleme verwalten können, die die Anwendungsleistung gefährden können, benötigt jedes Unternehmen eine kritische Schicht, die mehr bietet, als die Anwendungen am Laufen zu halten. Sie müssen die Möglichkeit haben, böswillige Aktivitäten zu blockieren und Anwendungen genau zum richtigen Zeitpunkt am richtigen Ort bereitzustellen. Jetzt und in Zukunft.

Das Anwendungsbereitstellungs-Netzwerk bietet genau das. Es erfüllt die Anforderung an größere Anwendungsmobilität und Sicherheit in einer stetem Wandel unterlegenen globalen Geschäftsumgebung. Das Anwendungsbereitstellungs-Netzwerk kombiniert drei wichtige Funktionen – die Überwachung der Anwendungsleistung, die WAN-Optimierung und Sicherheitstechnologien für das Webgateway – und ermöglicht Ihnen damit Folgendes:

- > Anzeigen von Anwendungen und Nutzern und ihrem Verhalten im Netzwerk sowie Behandlung von Leistungsproblemen.
- > Beschleunigen von unternehmenswichtigen Anwendungen, Streaming Video, SSL und anderen Unternehmensanwendungen.
- > Schutz vor Malware, Datenlecks und Leistungsver schlechterungen.
- > Ermöglichen einer hoch effizienten und produktiven Endnutzererfahrung zu jeder Zeit an jedem Ort.

Erstellen des Anwendungsbereitstellungs-Netzwerks

Um Ihnen den Einstieg zu erleichtern, beschreibt dieses Whitepaper die Komponenten und Prozesse, die Sie zur Einrichtung eines Anwendungsbereitstellungs-Netzwerks in Ihrer Infrastruktur benötigen.



Überwachung der Anwendungsleistung:

Identifizieren und beheben Sie die kritischen Faktoren, die die Anwendungsleistung beeinträchtigen.

Die Überwachung der Anwendungsleistung ist eine der schwierigsten und wichtigsten Aufgaben jeder IT-Abteilung. Sie umfasst folgende Aufgaben:

Sichtbarmachen des gesamten Datenverkehrs im Netzwerk.

Für diese Informationsbeschaffung sind Tools erforderlich, die jeden Tag automatisch Hunderte von Anwendungen in Ihrem Netzwerk identifizieren können. Um sie richtig zuordnen zu können, müssen Sie zwischen unternehmenswichtigen Inhalten, Malware und privatem Datenverkehr wie iTunes, YouTube und Peer-to-Peer (P2P)-Anwendungen unterscheiden können. Sie benötigen die Fähigkeit, komplexe Umgebungen in Unterklassen einzuteilen, einschließlich über das Web bereitgestellter Suiten wie Oracle und SAP, damit die wichtigsten Vorgänge und Nutzer innerhalb dieser Anwendungen die höchste Priorität bekommen.

Überwachen der Endnutzernerfahrung.

Wenn Ihre IT-Abteilung erfolgreich ist, wissen die Nutzer meist gar nicht, wie schwer Sie arbeiten, um Anwendungen am Laufen zu halten, die Datenintegrität zu wahren und Hardwareausfälle zu verhindern. Aber Vorbeugungsmaßnahmen sind nur so effektiv wie die Tools, über die Sie verfügen. Außerdem benötigen Sie die Möglichkeit, bestimmte Faktoren zu messen, die die Nutzernerfahrung beeinträchtigen, und die IT-Abteilung entsprechend zu benachrichtigen. Ein Beispiel hierfür sind P2P-Anwendungen, die Ihren kritischen Unternehmensanwendungen die Bandbreite wegnehmen.

Bestimmen der Ursache von Netzwerkproblemen.

Probleme bei der Anwendungsleistung können die unterschiedlichsten Ursachen haben. Daher müssen Sie eine Reihe von Aufgaben durchführen, um die Hauptprobleme schnell zu isolieren. Das kann eine Verzögerung zwischen dem Server und dem Netzwerk sein oder problematische Hosts, Server oder Anwendungen, die die größte Leistungsverschlechterung verursachen. Als Nächstes müssen Sie die Ursachen analysieren, um beispielsweise zu bestimmen, ob es sich um eine Spitzenlast in der Anwendungsnutzung oder um ein Protokollproblem handelt, und diese detaillierte Analyse verwenden, um Feineinstellungen für die Umgebung vorzunehmen und die Geschwindigkeit Ihrer Anwendungen wieder auf das gewünschte Niveau zu bringen.

Ermöglichen umfassender Sichtbarkeit.

Viele IT-Abteilungen führen diese Aufgaben bisher mithilfe einer Mischung von Verbindungsschicht-Tools unterschiedlicher Hersteller durch. Dies kann zu Kompatibilitätsproblemen führen. Eine vollständige, integrierte Lösung ist jedoch besser skalierbar und langfristig kosteneffektiver und kann sich schneller rentieren als eine Gruppe unterschiedlicher Tools, die integriert werden müssen.

Mit Beschleunigungs- und Steuerungstechnologien für Anwendungen werden



außerdem Maßzahlen und Statistiken auf Dienstebene zu umfassenden Berichten integriert, mit denen Sie die Nutzererfahrung verwalten können, indem Sie Probleme schnell identifizieren und lösen.

WAN-Optimierung:

Herausragende geschäftliche Leistungen hängen von schneller Anwendungsleistung ab.

Verwalten Sie die Nutzererfahrung in Ihrem gesamten verteilten Unternehmen.

In den meisten Unternehmensumgebungen werden heute zu jedem Zeitpunkt Hunderte von Anwendungen in jedem Teil des Netzwerks ausgeführt. Diese können unterschiedliche Verwaltungsprobleme aufweisen, je nach Anwendungstyp:

Interne Massenanwendungen

Anwendungen dieses Typs verwenden CIFS, MAPI, FTP oder TCP; sie umfassen Dateizugriff, Speicherkonsolidierung, E-Mail, Internet, Backups sowie Anwendungen, mit denen Updates, Patches und neue Firmware-Abbilder unternehmensweit verteilt werden.

Externe Anwendungen

Diese Anwendungen umfassen das gesamte Spektrum von unternehmenswichtig bis hin zu richtiggehend böswillig. Daher kann die Verwaltung externer Anwendungen die größte – und wichtigste – Herausforderung darstellen. Externe Anwendungen können alles von Schulungsvideos des Unternehmens und Salesforce.com bis hin zu den Hunderten von Anwendungen sein, auf die Nutzer von Ihrem Unternehmensnetzwerk aus zu privaten Zwecken zugreifen.

Den Zugriff auf erholungsorientierte Sites zu verwalten kann schwierig sein, da viele von ihnen, wie z. B. YouTube oder Instant Messaging, manchmal für geschäftliche Zwecke und nicht nur zur privaten Unterhaltung verwendet werden. Es ist also wesentlich, zwischen geschäftlicher und privater Nutzung zu unterscheiden, Ihre Netzwerkressourcen unter Kontrolle zu halten und den böswilligen Datenverkehr zu blockieren, der sich von überall huckepack in Ihr Netzwerk einschleichen kann.

Echtzeitanwendungen

Anwendungen wie VoIP, Videokonferenzen, Kreditkartentransaktionen, finanzieller Handel und Auftragsabwicklung sind häufig am empfindlichsten gegenüber Verzögerungen und am wichtigsten für das Unternehmen. Wie können Sie sie rund um die Uhr verfügbar halten?

Zentralisierte Verwaltung und Kontrolle vom Rechenzentrum bis hin zum Gerät.

Um für alle diese Anwendungstypen eine einheitliche Leistung sicherzustellen, müssen Sie geschäftliche Daten bis hin zur Geräteebene verwalten und schützen. Dafür benötigen Sie die Möglichkeit, Unternehmensrichtlinien durchzusetzen und Informationen gegen Diebstahl, Verlust und Malware-Infektionen zu schützen. So können Sie die Leistung aller Ihrer Client/Server-Anwendungen verbessern und



VPN-Nutzern, die ab und zu auch in der Niederlassung arbeiten, transparenten Zugriff ermöglichen.

Sicheres Web-Gateway:

Sie sollten Bedrohungen ihres Unternehmens an ihrem Eintrittspunkt vorhersehen und blockieren.

Sie müssen auf alles gefasst sein.

Sie können nie wissen, welche neue Art der Malware versuchen wird, Ihr Gateway zu durchqueren, um Finanzdaten, persönliche Informationen, Kundenunterlagen und mehr zu entwenden oder zu manipulieren. Deshalb müssen Sie Ihre Technologie-Strategie ständig weiterentwickeln und auf potenzielle physische und digitale Bedrohungen reagieren. Große Unternehmen stehen vor der Herausforderung, ihre globale Sicherheit aufrechtzuerhalten, ohne ihre globale Beweglichkeit zu gefährden. Um Ihr gesamtes Unternehmen zu sichern, müssen Sie alle Eintrittspunkte schützen – die Geräte und auch die Mitarbeiter.

Jede IT-Strategie muss die folgenden vier wichtigen Sicherheitsanforderungen berücksichtigen:

Schutz vor Malware. Technologien von führenden Malwareschutz-Anbietern wie Kaspersky, Sophos, Panda und McAfee können Malware-Infektionen verhindern, indem sie eingehenden und ausgehenden Web-Datenverkehr in Echtzeit filtern und Ihre Angreifbarkeit für böswillige Webinhalte reduzieren.

Wahrung der Mitarbeiterproduktivität. Nicht alle erholungsorientierten Anwendungen schaden der Produktivität Ihres Unternehmens. Sie benötigen die richtigen Tools, um herauszufinden, wann eine private Nutzung einen Verlust von Bandbreite und Mitarbeiterproduktivität bedeutet, damit Sie sie auf der Grundlage Ihrer Unternehmensrichtlinien und Geschäftsanforderungen steuern können.

Verhinderung von Informationslecks. Stellen Sie sicher, dass Ihr Schutz vor Datenlecks Funktionen für Überwachung, Warnungen und Verhinderung von Informationsdiebstahl aus Datenbanken und anderen anfälligen Ressourcen in Ihrem gesamten Unternehmen bietet. Erwägen Sie die Verwendung von Tools, die in Lösungen von Symantec/Vontu, RSA/Tablus, Code Green Networks und anderen führenden Anbietern integriert werden können.

Überprüfung von Vertrauensstellungen. Letztlich müssen Sie Ihr Unternehmen innen und außen sichern, da geschäftliche Verluste viele Formen annehmen können: Informationsdiebstahl, Ausfallzeiten, verringerte Produktivität, versehentliche oder absichtliche Datenbeschädigung und andere. Angesichts aller dieser Bedrohungen fragen Sie sich vielleicht, ob Sie jemals genug Sicherheitsmaßnahmen zum Schutz Ihres Unternehmens umsetzen können. Indem Sie jedoch umfangreiche Funktionen für die URL-Filterung, die Verhinderung von Datenlecks, den Malwareschutz, die Richtlinienverwaltung und die Identitätsauthentifizierung in Ihre Netzwerkverwaltung integrieren, können Sie Ihren Sicherheitsansatz insgesamt drastisch verbessern.

**Blue Coat bietet die intelligente Kontrolle, die Sie benötigen**

Sie sehen sich mit einer Reihe konvergenter Geschäftsfaktoren konfrontiert – Zentralisierung, Mobilität und Globalisierung. Zwar bieten viele Unternehmen Tools für die Verwaltung unterschiedlicher Aspekte dieser geschäftlichen Herausforderungen, aber nur Blue Coat hilft Ihnen, sie mit Lösungen für das Anwendungsbereitstellungs-Netzwerk umfassend anzugehen. Unsere zentralen Technologien – die Überwachung der Anwendungsleistung, die WAN-Optimierung und das sichere Web-Gateway – bieten Ihnen die Sichtbarkeit und die Kontrolle, die Sie benötigen, um Anwendungen besser als je zuvor zu analysieren, zu sichern und zu beschleunigen.

Sichtbarkeit

Blue Coat-Lösungen für das Anwendungsbereitstellungs-Netzwerk ermöglichen die Identifizierung und Klassifizierung von Anwendungen und Nutzern im gesamten Netzwerk. Mit unseren Funktionen können Sie den gesamten Anwendungs-Datenverkehr erkennen, die Nutzererfahrung überwachen, Leistungsprobleme behandeln und Probleme lösen, bevor sie die Nutzererfahrung beeinträchtigen. Insbesondere ermöglichen wir Ihnen Folgendes:

- > Automatische Erkennung von über 600 Anwendungen
- > Identifizierung von P2P-, erholungsorientierten oder Streaming-basierten Anwendungen über beliebige Ports
- > Detailliertere Klassifizierung komplexer Anwendungen wie SAP, Oracle, Citrix, Web, CIFS, MAPI und DCOM
- > Erkennung von URLs und externen Sites innerhalb von HTTP
- > Identifizierung problematischer Hosts, Server und Anwendungen

Beschleunigung

Mit Blue Coat können Sie für jeden Nutzer und an jedem Ort unternehmenswichtige Anwendungen beschleunigen, einschließlich interner und externer Anwendungen sowie Echtzeitanwendungen. Zugleich stellen wir sicher, dass Ihre Nutzer, ganz gleich an welchem Ort sie sich befinden, die gleiche Nutzererfahrung haben, als wären sie in der Hauptniederlassung. Wir bieten folgende Beschleunigungstechnologien:

- > Objekt- und Byte-Caching
- > Kompression und grundlegende Quality-of-Service (QoS)-Funktionen
- > Externe Web-/SSL-Beschleunigung
- > Protokollbeschleunigung für TCP, CIFS/NFS, MAPI, HTTP und mehr
- > Erweiterte Verwaltung von Webrichtlinien und Bandbreite
- > Fortschrittliche Anwendungs-ID-Technologie



Sicherheit

Blue Coat sichert Ihr Internet-Gateway, um Nutzer vor böswilligen Inhalten und Anwendungen zu schützen. Wir bieten folgende Sicherheitsfunktionen:

- > Prüfung auf Viren und Malware
- > Filterung von URLs und Webinhalten
- > Zentral verwaltetes verteiltes Gateway
- > Detaillierte Richtlinienverwaltung mit über 500 Variablen, einschließlich Variablen für Nutzer, Gruppen, Anwendungen, Quellen, Inhaltstypen und Transaktionen.
- > Protokollierung, Statistiken und SNMP-Unterstützung

Blue Coat-Lösungen für das Anwendungsbereitstellungs-Netzwerk bieten die intelligente Kontrolle, die Sie für die Zentralisierung, Mobilität und Globalisierung Ihrer gesamten IT-Infrastruktur benötigen. Mit Blue Coat können Sie die Anwendungs- und Netzwerkleistung für jeden Nutzer an jedem Ort in einem verteilten Unternehmen optimieren. Machen Sie Ihre IT-Abteilung zur treibenden Kraft für größere geschäftliche Effizienz, Effektivität und Wettbewerbsfähigkeit. Erfahren Sie, wie die Einführung eines Anwendungsbereitstellungs-Netzwerks Ihnen helfen kann, sich auf die nächste Phase konvergenter IT- und Geschäftsherausforderungen vorzubereiten. Sehen Sie unter www.bluecoat.com, wie es gemacht wird.



Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direkt
+1.408.220.2250 Fax • www.bluecoat.com



Copyright © 2008 Blue Coat Systems, Inc. Alle Rechte weltweit vorbehalten. Dieses Dokument darf ohne die vorherige schriftliche Einwilligung von Blue Coat Systems, Inc. weder ganz noch teilweise reproduziert noch auf ein elektronisches Medium übertragen werden. Technische Daten können ohne vorherige Ankündigung geändert werden. Die in diesem Dokument enthaltenen Informationen sind als genau und zuverlässig zu betrachten, Blue Coat Systems, Inc. übernimmt jedoch keinerlei Haftung für ihre Verwendung. Blue Coat ist in den Vereinigten Staaten und weltweit ein eingetragenes Markenzeichen von Blue Coat Systems, Inc. Alle anderen in diesem Dokument erwähnten Marken sind Eigentum ihrer jeweiligen Inhaber.