# Cisco Stealthwatch

## Mehr Transparenz im gesamten Unternehmen

**Kenntnis von jedem Host**

**Aufzeichnung aller Gespräche**

**Ermittlung des Normalverhaltens**


**Warnmeldungen bei Änderungen**

**Schnelle Reaktion auf Bedrohungen**

## Mehr Transparenz als Voraussetzung für Sicherheit in digitalen Unternehmen

Das typische Unternehmensnetzwerk von heute wächst rasant und verbindet mehrere Zweigstellen, mobile Benutzer, die Cloud und Rechenzentren miteinander. Dabei kehren Unternehmen sich immer mehr ab von herkömmlichen IT-Infrastrukturen und wählen digitalisierungsfähige Netzwerkinfrastrukturen, um ihre Geschäftsabläufe von Grund auf zu verändern. Viele von ihnen profitieren erheblich von einer solchen Digitalisierung, sei es in Form von optimiertem Betrieb und Bestandsmanagement oder weil sie neue Services mit größerem Mehrwert anbieten können.

Die Transformation in ein digitales Unternehmen und die Implementierung neuer Prozesse und Technologien bedeuten aber auch eine Notwendigkeit für mehr Transparenz, um Sicherheit gewährleisten zu können.


76 % aller IT-Experten sagen, dass Transparenz die größte Herausforderung ist. Quelle: Ponemon Institute



## Vorteile

- **Transparenterer Überblick** über die gesamte Kommunikation im Netzwerk, einschließlich Ost-West- und Nord-Süd-Datenverkehr, zur Erkennung interner und externer Bedrohungen
- **Erweiterte Sicherheitsanalytik** und Erfassung detaillierter Kontextinformationen zur Erkennung verschiedenster ungewöhnlicher Verhaltensweisen, die auf einen Angriff hindeuten könnten
- **Schnellere und bessere Bedrohungserkennung**, Incident-Response und Forensik im gesamten Netzwerk, auch für verschlüsselten Datenverkehr
- **Tiefergehende forensische Untersuchungen** anhand von Audit-Historien zu Netzwerkaktivitäten
- **Einfachere** Netzwerksegmentierung, Leistungsüberwachung und Kapazitätsplanung
- **Gewährleistung von Unternehmens-Compliance** durch Ermittlung des Ausmaßes und der Qualität der Verschlüsselung im Netzwerk
- **Mehr Transparenz und bessere Anomalienerkennung** dank Korrelation von globalem und lokalem Datenverkehr
- **Identifizierung von Insiderbedrohungen** anhand von Kontextinformationen aus Cloud-Services

# Cisco Stealthwatch

Überwachen · Erkennen · Analysieren · Reagieren


Erweitertes Netzwerk


Rechenzentrum


Zweigstelle


Cloud

Cisco Stealthwatch ermöglicht eine kontinuierliche Echtzeitüberwachung des gesamten Netzwerkdatenverkehrs sowie detaillierte Einblicke in alle Netzwerkaktivitäten. Die Lösung verbessert die Transparenz in erweiterten Netzwerken drastisch und verkürzt die Reaktionszeiten bei verdächtigen Vorfällen. Sie erstellt eine Baseline, die das normale Web- und Netzwerkverhalten eines Netzwerkhosts abbildet, und erkennt mittels kontextsensitiver Analyse automatisch ungewöhnliches Verhalten. Stealthwatch kann eine breite Palette von Angriffstypen identifizieren, darunter Malware, Zero-Day-Angriffe, DDoS-Angriffe (Distributed Denial of Service), APTs (Advanced Persitent Threats) und Bedrohungen durch Insider.

Ergänzt um Cognitive Analytics, eine Cloud-basierte Lösung für Bedrohungserkennung und Bedrohungsanalytik, kann Cisco Stealthwatch jetzt außerdem zusätzliche Kontextinformationen abrufen und so neue sowie aufkommende Bedrohungen im gesamten erweiterten Netzwerk identifizieren und priorisieren. Stealthwatch mit Cognitive Analytics bietet noch mehr Transparenz für globalen und lokalen Datenverkehr inklusive zusätzlicher Kontextinformationen und nutzt maschinelles Lernen für kontinuierliche Analysen sowie die Erkennung von Command-and-Control-Datenverkehr. So können Sie jetzt auch Bedrohungen identifizieren, die Ihre Sicherheitskontrollen umgangen haben, und erkennen, wenn Daten ungewollt an eigentlich legitime Cloud-Services gesendet werden.

## Analyse von verschlüsseltem Datenverkehr für höhere Sicherheit

Verschlüsselung ist ein wichtiger Baustein für Sicherheit. Doch während Sie mithilfe von Verschlüsselung Ihre Daten und Ihre Privatsphäre schützen, nutzen Angreifer die Technologie, um Malware zu verbergen und der Erkennung durch Netzwerksicherheitsprodukte zu entgehen. Mit Cisco Stealthwatch und seinen erweiterten Analytikfunktionen können Sie leichter herausfinden, ob verschlüsselter Datenverkehr in Ihrem Netzwerk gefährlich ist. Stealthwatch nutzt maschinelles Lernen und statistische Modellierung zur Gewinnung von Intraflow-Metadaten oder Encrypted Traffic Analytics als Ergänzung zu NetFlow-Analysen. Cognitive Analytics kann selbstständig lernen und sich im Laufe der Zeit an sich verändernde Netzwerkverhalten anpassen.

Stealthwatch mit Cognitive Analytics zentralisiert das Management von Netzwerk- und Webdatenverkehr in der Management Console und erlaubt so detaillierte Einblicke in alle Datenverkehrsflüsse. Statt den Datenverkehr zu entschlüsseln, untersucht Stealthwatch mit Cognitive Analytics den verschlüsselten Datenverkehr auf gefährliche Muster. So kann die Lösung Bedrohungen identifizieren und schneller geeignete Gegenmaßnahmen einleiten.

Mithilfe von Encrypted Traffic Analytics stellt Stealthwatch außerdem sicher, dass Ihr Unternehmen mit kryptografischen Protokollen konform ist und jederzeit weiß, was im Netzwerk verschlüsselt wird und was nicht.

## Ausweitung der Transparenz auf die Cloud

Immer mehr Workloads werden von lokalen Umgebungen in Cloud-Umgebungen überführt. Zwar wird Ihr Unternehmen so flexibler; gleichzeitig haben Sie aber auch nur begrenzt Einblick in die Datenverkehrsflüsse in diesen virtuellen Instanzen. Mit Stealthwatch stehen Ihnen alle Funktionen für Netzwerktransparenz, Bedrohungserkennung und Analytik sowohl in öffentlichen als auch in privaten und hybriden Cloud-Umgebungen zur Verfügung. Sie haben in Echtzeit Zugriff auf Informationen zum Situationskontext und können die Sicherheit in Ihrer gesamten Infrastruktur verbessern.

## Ausweitung der Transparenz auf Endpunkte

In der vernetzten Welt von heute ist Mobilität das A und O. Immer mehr Benutzer verbinden sich mit Unternehmensnetzwerken, über immer mehr Geräte und von mehr verschiedenen Orten aus als jemals zuvor. Möchten Sicherheitsverantwortliche hier wirklich alle Netzwerkaktivitäten überwachen, müssen sie Einblick in sämtliche Anwendungen und Prozesse haben, vom Netzwerkrand bis hin zu einzelnen Remote-Geräten. Mit der Cisco Stealthwatch Endpoint-Lizenz kann Ihr Sicherheitsteam Benutzersysteme, die sich verdächtig verhalten, effizienter und unter Rückgriff auf mehr Kontextinformationen untersuchen, schneller auf Vorfälle reagieren und Richtlinienverstöße rasch korrigieren.

## Ausweitung der Transparenz auf Zweigstellen

Netzwerktransparenz in einem Zweigstellennetzwerk zu erreichen kann kompliziert und kostspielig sein, insbesondere wenn es sich um ein über mehrere Standorte verteiltes Zweigstellennetzwerk handelt. Die Cisco Stealthwatch Learning Network-Lizenz ist eine kosteneffiziente Lösung, mit der Sie Ihre Vorkehrungen für Netzwerksicherheit auf Zweigstellen- und Remote-Netzwerke ausweiten können. Sie können Ihre bereits vorhandene

**„Wenn ich mir in einem Unternehmen einen Überblick darüber verschaffen muss, was passiert ist oder was gerade passiert, dann ist Stealthwatch ideal. Die Lösung hat mich noch nie im Stich gelassen. [...] Für mein Team ist der wichtigste Vorteil von Stealthwatch die Rund-um-die-Uhr-Überwachung. Bedrohungen können uns entgehen – nicht jedoch Stealthwatch.“**

**Phil Agcaoili**
CISO, Elavon Weitere Informationen

Cisco Netzwerktechnologie nutzen und mithilfe der von Cisco Geräten generierten NetFlow-Daten die Netzwerktransparenz und die Netzwerksicherheit verbessern. Die Erkennung von Sicherheitsanomalien wird in die Netzwerkelemente selbst eingebettet, wobei Paketerfassung sowie intelligente Detektoren zum Einsatz kommen, um Bedrohungen zu identifizieren, einzudämmen und zu neutralisieren. Die Lösung ermöglicht Transparenz ohne Auswirkungen auf die Bandbreite. Interaktionen und Datenverschiebungen sind nur notwendig, wenn eine Maßnahme ergriffen werden muss.

## Ineinandergreifende Sicherheitslösungen

Cisco Stealthwatch nutzt Ihre bereits vorhandene Netzwerkinfrastruktur, um die Transparenz in Ihrem gesamten Unternehmen zu verbessern. Es extrahiert aus NetFlow-Daten Intelligence mit konkreten Handlungsempfehlungen und macht aus Ihrem Netzwerk einen Sensor. Sie gewinnen detaillierte Einblicke in den gesamten Netzwerkdatenverkehr und können potenzielle Netzwerkbedrohungen identifizieren.

Wenn Sie Stealthwatch mit anderen Security-Lösungen von Cisco integrieren, profitieren Sie von erweiterten Funktionen für Segmentierung, Bedrohungserkennung und Forensik in allen erweiterten Netzwerken, Zweigstellen, Rechenzentren und Clouds.

Die Integration von Cisco Stealthwatch mit der Cisco Identity Services Engine liefert Unternehmen einen vollständigen Überblick über ihr erweitertes Netzwerk. Sie können Ihr Netzwerk als Sensor nutzen und gewinnen so einen einzigartig detaillierten Einblick in Ihr Unternehmen. Zentralisierte Kontrolle und Richtliniendurchsetzung vereinfachen die Segmentierung. Bedrohungen lassen sich schneller neutralisieren, sowohl proaktiv mittels Bedrohungserkennung als auch im Nachhinein durch erweiterte forensische Untersuchungen.

Cisco hat jetzt den Funktionsumfang von NetFlow-Analysen und Paketanalysen kombiniert: Wir haben Cisco Stealthwatch mit Cisco Security Packet Analyzer integriert. Zwar sind beide Technologien eine Hilfe bei der Behebung von Sicherheits- und Netzwerkvorfällen. In der Vergangenheit wurde jedoch häufig jeweils einer der Vorzug gegeben – in der Regel aus Budgetgründen oder aufgrund eines Mangels an Ressourcen. Unser zielgerichteter Ansatz erlaubt es Ihnen, nur Pakete von Interesse zu speichern. Das reduziert die Speicherkosten und liefert gleichzeitig detailliertere Aufzeichnungen aller Netzwerkaktivitäten mit mehr Kontextinformationen. Die zusätzliche Transparenz und der zusätzliche Sicherheitskontext aus NetFlow werden kombiniert mit einer präziseren und kosteneffizienteren Methode zur Erfassung von Paketdaten, sodass Sie spezifische Probleme bei Bedarf eingehender untersuchen können.

## Nächste Schritte

Weitere Informationen finden Sie unter http://www.cisco.com/go/stealthwatch. Alternativ können Sie sich an Ihren Cisco Ansprechpartner vor Ort wenden.



# Cisco Stealthwatch

- Umfassender Überblick über den gesamten Netzwerkperimeter, das Netzwerk selbst, das Rechenzentrum sowie private und öffentliche Clouds, bis hinunter zum einzelnen Endpunkt
- Einfachere Ermittlung des normalen Netzwerkverhaltens und Definition einer Baseline mit NetFlow zur Identifizierung von ungewöhnlichem Verhalten
- Kontinuierliche Überwachung von Geräten, Anwendungen und Benutzern in allen verteilten Netzwerken
- Erweiterte Sicherheitsanalytik und erweiterte Intelligence zur Erkennung einer breiten Palette von Verhaltensvarianten, die auf einen Angriff hindeuten könnten
- Schnellere Reaktion auf Vorfälle dank Bedrohungserkennung in Echtzeit
- Überragend gründliche forensische Untersuchungen dank umfassender Netzwerk-Audit-Trails
- Einfachere Netzwerksegmentierung, Compliance-Validierung, Fehlerbehebung und Diagnose