Tripwire Enterprise 8.8

Erkennung. Reaktion. Prävention.

Tripwire schützt führende Organisationen auf der ganzen Welt vor ruf- und betriebsschädigenden Cyberangriffen.

Und weil Hacker immer raffinierter werden, haben auch wir unsere Technologien in den letzten 20 Jahren immer weiter entwickelt.

Tripwire® Enterprise ist eine Suite vollständig integrierter SCM-Lösungen (Security Configuration Management) für die Verwaltung von Richtlinien, Dateiintegrität und Bedrohungsabwehr. Kunden können diese Lösungen zu einem einzigen, umfassenden SCM-Paket kombinieren oder die Tools zur Überwachung der Dateiintegrität (File Integrity Monitoring, FIM) und für die Richtlinienverwaltung als Punktlösungen nutzen. Ganz gleich, für welche Variante Sie sich entscheiden: Mit Enterprise sind Sie bestens ausgestattet, um die heutigen und auch zukünftige Herausforderungen im Bereich Sicherheit und Compliance erfolgreich zu meistern.

Unsere SCM-Suite unterstützt Sicherheits-, Compliance- und Betriebsteams dabei, die grundlegende Sicherheitsinfrastruktur zu stärken und geschäftskritische Ressourcen unter anderem in On-Premises-, Cloud- und industriellen Umgebungen zu schützen, indem sie die Angriffsfläche reduziert, die Systemintegrität verbessert und die Einhaltung von Branchenstandards fördert. Außerdem lässt sich Tripwire Enterprise mit verschiedenen Unternehmensanwendungen integrieren. Dadurch können Workflows automatisiert, weitere Sicherheitslösungen wie SIEM- und Change-Management-Tools hinzugefügt und die Betriebseffizienz gesteigert werden, und Organisationen erhalten einen umfassenderen Überblick über ihre Sicherheitsinfrastruktur.

Tripwire Enterprise dient als leistungsstarkes Fundament für eine effektive Bedrohungserkennung, -abwehr und -prävention in IT-Umgebungen und bietet dazu die folgenden Services:

- **Erkennung:** Sicherheitsteams werden durch die Bereitstellung von Gefahrenindikatoren frühzeitig auf Cyberbedrohungen und etwaige schädliche Aktivitäten aufmerksam gemacht.
- **Reaktion:** Bei tatsächlichen Sicherheitsvorfällen oder Cyberbedrohungen werden Warnmeldungen generiert und zusammen mit Empfehlungen zur Systemwiederherstellung an die Verantwortlichen geschickt.
- **Prävention:** Indem Risiken und verdächtige Aktivitäten nach Priorität geordnet werden, können sich Teams einen besseren Überblick über den Sicherheitsstatus sämtlicher Geräte und Systeme verschaffen.

So unterstützen wir unsere Kunden: Eng miteinander verzahnte Tools

Der Leistungsumfang von Tripwire Enterprise umfasst miteinander integrierte Tools, die gemeinsam eine SCM-Lösungssuite der Enterpriseklasse bilden:

- **Tripwire File Integrity Manager** ist eine führende Lösung zur Überwachung der Dateiintegrität, mit der sich große, heterogene IT-Umgebungen auf Bedrohungen überprüfen, Erkenntnisse über Konfigurationsschwachstellen in Echtzeit bereitstellen, die Anzahl von Konfigurationsabweichungen und unautorisierten Änderungen reduzieren und die Betriebseffizienz steigern lassen. Tripwire FIM stellt detaillierte Bedrohungsdaten von Endpunkten zur Verfügung, um Sicherheitsbeauftragte mit wichtigen Einblicken in den Sicherheits- und Compliance-Status dieser

Geräte und Systeme zu versorgen. In Kombination mit Tripwire Policy Manager werden zudem bei Änderungen Konfigurationsprüfungen gestartet, die nützliche Informationen liefern. Dieser dynamische, kontinuierliche Bewertungsansatz ermöglicht die sofortige Reaktion auf schädliche Fehlkonfigurationen und eine Stärkung der Sicherheitsrichtlinien in sämtlichen IT-Umgebungen.

» **Tripwire Policy Manager** ist sowohl im agentbasierten als auch im agentlosen Bereitstellungsmodell verfügbar und bietet kontinuierliche Konfigurations- und Compliance-Prüfungen gegen mehr als 1000 verschiedene Plattformen, Sicherheitsrichtlinien, Standards, Verordnungen und Anbietervorgaben. Hinzu kommen Funktionen zur Anpassung und Erlassung von Richtlinien, zur Verwaltung von Ausnahmefällen und zur automatisierten, priorisierten Fehlerbehebung anhand von überschrittenen Grenzwerten und dem Schweregrad der Fehlkonfiguration. Gleichzeitig stellt Policy Manager Compliance-Berichte für Betriebsprüfungen sowie Statusinformationen sämtlicher vorhandener Richtlinien bereit.

» **Remediation Manager** ergänzt Tripwire Policy Manager und unterstützt IT-Sicherheits- und Compliance-Teams bei der Wiederherstellung falsch ausgerichteter Konfigurationen. Dabei wird jedem Mitarbeiter eine bestimmte Rolle zugewiesen und jeder Schritt bei der Fehlerbehebung muss von der verantwortlichen Person abgesegnet werden. Diese Informationen werden teamübergreifend zugänglich gemacht. So wissen alle Betroffenen, welche Fehler wo identifiziert wurden, ob sie sich noch in Arbeit befinden und wie sie sich beheben lassen.

» **Mit Funktionen für die Ursachenermittlung und -analyse** können Sicherheits- und Betriebsteams schnell und effektiv auf Vorfälle reagieren. Personalwechsel, die Anpassung von Betriebsprozessen oder die Einführung neuer Technologien haben allesamt Auswirkungen auf die IT-Umgebungen und -Systeme einer Organisation. Tripwire Enterprise sorgt durch detaillierte Analysen, Statusvergleiche vor und nach einem Vorfall und historische Daten zum Normalzustand des Systems dafür, dass Teams die nötigen Informationen für ihre Untersuchungen zur Verfügung stehen: Was hat sich wie und wann verändert? Wer war dafür verantwortlich? Wie oft wurden Änderungen vorgenommen?

Branchenführende Sicherheit und Compliance

Wir ergänzen Tripwire Enterprise kontinuierlich um weitere Funktionen, um Organisationen bei der Einhaltung moderner Sicherheits- und Compliance-Anforderungen zu unterstützen. Zu diesen neuen Leistungen zählen die Überwachung von Cloud-Ressourcen, der Schutz von industriellen Geräten und am MITRE ATT&CK-Framework orientierte Tools zur Aufdeckung verdächtiger oder schädlicher Aktivitäten in Ihren IT-Umgebungen.

» **Cloud Management Assessor:** Die überwiegende Mehrheit der Sicherheitsvorfälle in Public-Cloud-Services wird durch Konfigurationsfehler verursacht. Mit dem Cloud Management Assessor bietet Ihnen Tripwire ein leistungsstarkes Tool, das Amazon Web Services, Microsoft Azure, Google Cloud-Plattformen und SaaS-Konten bei Anbietern wie Salesforce durchsucht und Sie auf unautorisierte oder unerwartete Konfigurationsänderungen aufmerksam macht. Außerdem wird anhand von Best Practices wie dem CIS AWS Foundations Benchmark Version 1.1.0 geprüft, ob Ihr Konto für das Public-Cloud-Management sicher konfiguriert wurde.

» Die Speicherung von Dateien mit cloudbasierten Speicherdiensten wie AWS S3-Buckets oder Azure Storage ist nicht ohne Risiko, denn oft reicht nur eine einfache Änderung an der Sicherheitskonfiguration, um sensible Daten offenzulegen. Um dies zu verhindern, generiert der Cloud Management Assessor zudem Warnmeldungen, falls unerwartete Änderungen an Dateiattributen wie Zugriffsrechten vorgenommen werden, sodass Sie zeitnah darauf reagieren können.

» **Tripwire Connect:** Mit Tripwire Connect können CISOs, Sicherheits- und Compliance-Teams sicherheitsrelevante und Geschäftsziele besser aufeinander abstimmen – unter anderem indem sie sich wichtige Fragen stellen, darunter: Wie steht es um unseren Sicherheitsstatus? Sind unsere Schutzmaßnahmen noch zeitgemäß? Wie lassen sich unsere Ziele zur Risikominimierung am besten umsetzen? Tripwire Connect ermöglicht Ihnen historische und aktuelle Einblicke in Ihre Cybersicherheit und Geschäftsrisiken und stellt diese Daten als Gesamtüberblick der Organisation oder nach einzelnen Abteilungen oder Teams geordnet bereit. Anschließend können solche Einblicke in praxistauglichen Berichten zusammengefasst werden, die CISOs und IT-Sicherheitsmanager mit den Informationen versorgen, die sie benötigen, um die Angriffsfläche zu reduzieren, die Systemintegrität zu schützen und somit ihren gesetzlichen Compliance-Pflichten nachzukommen.

» **MITRE ATT&CK-Framework:** Anhand des von MITRE entwickelten Frameworks können Angreiferverhalten und -taktiken analysiert und entsprechende Gegenmaßnahmen empfohlen werden, um das Geschäftsrisiko zu senken und die Cybersicherheit zu verbessern. Indem wir Erkenntnisse aus dem ATT&CK-Framework in Tripwire Enterprise einfließen lassen, erweitern wir die Bedrohungserkennungskapazitäten unserer Kunden und stärken ihren Sicherheitsstatus.

Tripwire Enterprise baut auf unserem ursprünglichen hostbasierten Tool zur Erkennung von Änderungen an Dateien und Ordnern auf und erweitert dessen Leistungsumfang um zuverlässige FIM-Funktionen. Durch die Analyse von Dateien, Verzeichnissen, Konfigurationsparametern, DLLs, Ports, Services, Protokollen oder der Systemregistrierung ermöglicht Enterprise eine granulare Überwachung der gesamten Systemintegrität. Zusätzliche Integrationen bieten detaillierte Bedrohungsdaten von Endpunkten, die zu einer schnelleren Risikoerkennung und besseren Compliance beitragen. Tripwire Enterprise ist das Ergebnis jahrelanger Verfeinerungen. Die aktuelle Lösungssuite ist integrationsfreundlich und punktet zudem mit leistungsstarken Erkennungsfunktionen für das Change Management sowie mit effektiver Risikoeinschätzung und Richtlinienpriorisierung und informiert Sicherheitsbeauftragte mit sorgfältig gefilterten Warnmeldungen über Cybersicherheitsrisiken. Somit ist Enterprise bestens ausgestattet, um selbst großen Organisationen die Verwaltung der Integrität, Sicherheit und Compliance ihrer Systemkonfigurationen zu erleichtern.

Integration mit Active Directory

Viele Administratoren nutzen Active Directory (AD) für die Verwaltung von Benutzergruppen und Zugriffsrechten. Mit Tripwire Enterprise haben Sie die Möglichkeit, Ihre Active Directory-Gruppen und organisationsspezifischen Richtlinien zu integrieren und entsprechende Rollen in Enterprise zuzuweisen. Dadurch entfällt der überflüssige manuelle Aufwand, Nutzer in Enterprise hinzuzufügen, die bereits in AD existieren.

Automatisiertes On- und Offboarding von Cloud-Ressourcen

Damit geschäftskritische Ressourcen in dynamischen Cloud-Umgebungen effektiv überwacht werden können, müssen sie getaggt und gescannt werden. Mithilfe des automatisierten Onboarding erfasst Enterprise den Normalzustand Ihrer Cloud-Umgebungen, erkennt, wenn neue Ressourcen hinzukommen und scannt sie. Somit behalten Sie den Überblick über sämtliche Cloud-Ressourcen, ganz gleich, ob sie kurz- oder langfristig bereitgestellt werden. Mit der automatisierten Offboarding-Funktion können Sie bestimmen, wie lange Daten in kurzlebigen Ressourcen von Tripwire Enterprise gespeichert werden.

Tripwire als Multitalent

Tripwire Enterprise ist im agentbasierten und agentlosen Bereitstellungsmodell verfügbar und unterstützt:

- **Alle gängigen Betriebssysteme:** Windows, Red Hat, CentOS, Ubuntu, SUSE und Debian
- **Viele anbieterspezifische Betriebssysteme:** AIX, Solaris, HP-UX u. a.
- **Verzeichnisdienste:** Active Directory, LDAP u. a.
- **Netzwerkgeräte:** Firewalls, IPS- und IDS-Systeme, Router u. a.
- **Datenbanken:** Oracle, MS SQL, Db2 und PostgreSQL
- **Industrielle Geräte:** Datenerfassungs-Controller, Mensch-Maschine-Schnittstellen (HMIs), speicherprogrammierbare Steuerung (PLCs), Relays, Remote Terminal Units (RTUs) u. a.

Umfassende Unterstützung des gesamten IT-Stacks

Ob Sie nur bestimmte, geschäftskritische Server oder die ganze IT-Infrastruktur (inklusive cloudbasierter und virtualisierter Umgebungen, Anwendungen und industrieller Geräte) im Auge behalten wollen: Mit Tripwire Enterprise stehen Ihnen die richtigen Tools zur Verfügung, um sämtliche Sicherheitsrichtlinien zu überprüfen und durchzusetzen und Konfigurationsänderungen rechtzeitig zu identifizieren.

Fordern Sie eine Demo an

Erleben Sie Tripwire Enterprise in einer Demo in Aktion und stellen Sie uns Ihre Fragen. Näheres erfahren Sie unter **tripwire.com/contact/request-demo**

Tripwire Enterprise: Support für den gesamten Service-Stack

Anwendungen	Tripwire Enterprise bietet Kunden die Tools, die sie zur Verwaltung von Compliance-Richtlinien und zur Überwachung der Dateiintegrität und korrekten Konfigurationen ihrer Anwendungen benötigen, um somit für die bestmögliche Sicherheit, Leistung und Verfügbarkeit zu sorgen.
Verzeichnisdienste	Mit Tripwire Enterprise können Kunden überprüfen, ob ihre LDAP Server-Objekte und -Attribute wie LDAP-Verzeichnisschemata, Passworteinstellungen, Nutzerberechtigungen, Netzwerkressourcen, Gruppenaktualisierungen und Sicherheitsrichtlinien die einschlägigen Compliance-Anforderungen erfüllen.
Datenbanken	Enterprise lässt sich mit den Dateisystemen von Tripwire kombinieren, um Organisationen beim Schutz ihrer Oracle-, Microsoft- und IBM-Datenbankserver und bei der Leistungssteigerung zu unterstützen.
Dateisysteme und Desktops	Tripwire Enterprise überprüft die Konfigurationen der physischen und virtuellen Server und Desktop-Dateisysteme, unter anderem mit Fokus auf Sicherheit, Konfigurationsparameter und Berechtigungen.
Kassen- und Bezahlsysteme (Point-of-Sale, POS)	Enterprise schützt POS-Geräte vor Cyberbedrohungen, unterstützt die Verwaltung von Sicherheits- und Compliance-Richtlinien und stellt IT-Betriebsteams Warnmeldungen, Benachrichtigungen und Empfehlungen zur Reaktion auf mögliche Gefahrenindikatoren zur Verfügung.
Virtuelle Umgebungen	Tripwire Enterprise kann in virtuellen Umgebungen in privaten, öffentlichen und Hybrid-Clouds und als virtuelle Maschine eingesetzt werden. In einem agentbasierten Bereitstellungsmodell können zusätzliche virtuelle Endpunkte überwacht und verwaltet werden. Somit können virtuelle und Cloud-Umgebungen vor Cyberbedrohungen geschützt, die Systemintegrität geprüft, Richtlinien konsistent durchgesetzt, Dashboards und Berichte erstellt und Warnmeldungen sowie Benachrichtigungen in Echtzeit generiert werden.
VMware	Mit Tripwire Enterprise erhalten Kunden einen Überblick über ihre auf VMware basierte virtuelle Infrastruktur, wodurch sie die Konfigurationen in diesen Umgebungen stets im Auge und im Griff behalten.
Netzwerkgeräte	Mit Enterprise können Kunden die Konfigurationseinstellungen vieler verschiedener Netzwerkgeräte analysieren und bewerten lassen, darunter Geräte mit einem POSIX-konformen Betriebssystem.
Industrielle Geräte	Tripwire Enterprise ermöglicht die Überwachung industrieller Geräte über unterschiedliche Protokolle wie Modbus TCP, Ethernet/IP CIP und SNMP. Das Scannen industrieller Windows- oder Linux-Systeme wird auch in der agentlosen Bereitstellung unterstützt. Durch die Integration mit Rockwell Automation FactoryTalk AssetCentre, MDT AutoSave und Kepware KEPServerEX lassen sich auch für Geräte, die nicht direkt mit Enterprise gescannt werden können, Konfigurationsdaten erfassen. Eine weitere Möglichkeit ist hier der Einsatz von Web Retriever, der entsprechende Konfigurationsdaten aus Websites zusammenträgt.

Tripwire Enterprise: Features und Vorteile

Leistungsfähige Datenerfassungs- und Kommunikationsplattform	Mit Tripwire Axon von Tripwire Enterprise, einer anpassbaren, erweiterbaren und leistungsfähigen Kommunikationsplattform, steht Kunden ein erstklassiges Tool zur Datenerfassung an Endpunkten zur Verfügung. Sie dient der Stärkung der Cybersicherheit, Überwachung der Datei- und Systemintegrität und der Verwaltung von Konfigurationen und Compliance. Nutzer profitieren von beispielloser Transparenz und Cybersicherheit und können gleichzeitig den Betrieb straffen und die Reaktionsfähigkeit der IT-Teams verbessern.
Unterstützung für Hybrid-Umgebungen	Tripwire Enterprise überprüft On-Premises- und Cloud-Umgebungen auf Sicherheit und Compliance und ermöglicht es Kunden, Kosten zu reduzieren und sich einen klaren Überblick über sämtliche Ressourcen, Systeme und Richtlinien zu verschaffen.
Zentralisierte Kontrolle sämtlicher IT-Konfigurationen	Mit Enterprise kann die gesamte physische und virtuelle IT-Infrastruktur einer Organisation – darunter Server, Geräte, Anwendungen, Plattformen und Betriebssysteme – von einer zentralen Konsole aus gesteuert werden.
Erweiterte Integration über REST-APIs	Funktionsreiche REST-APIs ermöglichen die wertschöpfende Integration zusätzlicher Anwendungen mit Tripwire Enterprise. Zum Beispiel können über diese REST-APIs Befehle an Anwendungen weitergeleitet oder Daten aus Tripwire Enterprise extrahiert werden. Und mithilfe von Administrations-APIs können Aufgaben wie die Echtzeitüberwachung oder die Durchsetzung von Richtlinien automatisiert werden.
Netzwerküberwachung in OT-Umgebungen	Werden Tripwire Enterprise und der Tripwire Data Collector kombiniert, können Kunden ihre industriellen Netzwerke auf Konfigurationsänderungen und Compliance-Verstöße überprüfen. Dadurch stärken sie ihre Cybersicherheit, ohne den Betrieb zu stören.
Umfassende Tagging-Funktionen mit Asset View	Die Asset View-Funktionen von Tripwire Enterprise ermöglichen die tagbasierte Klassifizierung von Ressourcen nach Risiko, Priorität, geografischem Standort, Richtlinien und weiteren Kategorien. Ressourcen können selbst in großen Mengen mit Tags versehen und bereitgestellt werden. Außerdem lassen sich getaggte Ressourcen aus Tripwire IP360 importieren, sodass Kunden einen klaren Überblick über das Geschäftsrisiko in der gesamten Organisation haben.
Workflow-Tools zur Verwaltung von Fehlkonfigurationen	Der Remediation Manager dient der rollenbasierten Bereitstellung von Workflow-Tools für die Zulassung, Zurückweisung, Verschiebung und Wiederherstellung von Konfigurationen.
Integration mit Change Management-Systemen (CMS)	Mit Tripwire integrierte CMS-Lösungen versetzen Enterprise in die Lage, Änderungen in Echtzeit zu erkennen und automatisch mit erstellten Tickets oder Änderungsanforderungen abzugleichen.
Schnellere, einfachere Vorbereitung auf Betriebsprüfungen	Dank der kontinuierlichen Bereitstellung von Baseline-Werten, Echtzeitdaten zu Konfigurationsänderungen und integrierten Bedrohungsdaten können Kunden mit Tripwire Enterprise die (potenziellen) Auswirkungen solcher Änderungen präziser einschätzen und sich besser auf Betriebsprüfungen vorbereiten.
Stärkere Sicherheit und Compliance	Tripwire Enterprise kombiniert detaillierte Konfigurationsprüfungen mit Funktionen zur Überwachung der Dateiintegrität (FIM) in Echtzeit, um sämtliche Änderungen in IT-Umgebungen schnell zu erkennen und zu analysieren und die Ergebnisse an die Sicherheits- und Compliance-Teams zu übermitteln. Dadurch lassen sich Vorfälle zeitnah bearbeiten und Probleme beheben, um Organisationen vor schwerwiegenden Sicherheitsverletzungen, Compliance-Verstößen, längeren Ausfällen und möglichen Geldstrafen zu bewahren.
Automatisierte Compliance mit Branchenstandards	Tripwire Enterprise automatisiert die Durchsetzung von Compliance-Richtlinien und passt sie an einschlägige Branchenstandards wie PCI, NERC, SOX, FISMA und DISA an.
Automatisiertes On- und Offboarding von Ressourcen	Mithilfe der Onboarding-Funktion können kurzlebige Ressourcen aus dynamischen Cloud-Umgebungen mit Tags versehen, automatisch mit Tripwire Enterprise bereitgestellt und auf Compliance und Änderungen geprüft werden. Und mit der Offboarding-Funktion können Ressourcen automatisch wieder entfernt werden.
Integration mit Active Directory	Die Integrationsfreundlichkeit von Tripwire Enterprise ermöglicht eine enge Verzahnung mit Active Directory. Dank der automatisierten Erstellung und Zuweisung von Nutzern, Gruppen und Rollen können Administrationsaufwand und durch Mitarbeiter verursachte Fehler reduziert werden und die Verwaltung von Anmeldedaten wird gestrafft und geschützt.

tripwire®

Tripwire stellt Kunden branchenführende Produkte zur Stärkung ihrer Cybersicherheit zur Verfügung. Wir schützen prominente Unternehmen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere für Ihre Systeme. **Weitere Informationen erhalten Sie unter tripwire.com.**

***The State of Security*: Aktuelles, Trends und interessante Einblicke finden Sie unter tripwire.com/blog**
Folgen Sie uns auf LinkedIn, Twitter und Facebook

TEDS88b 2002