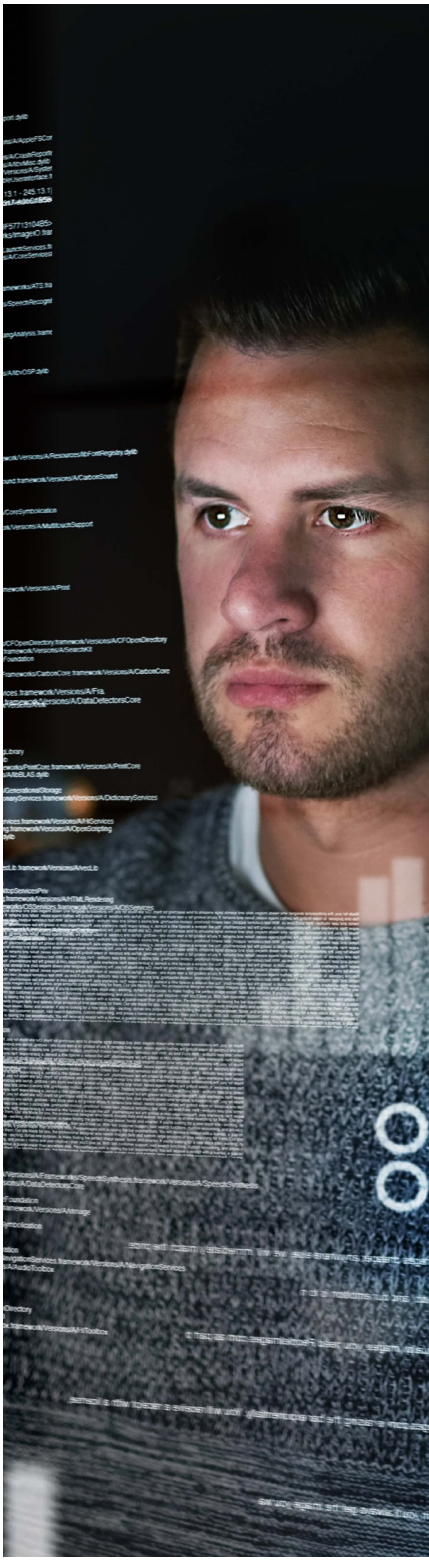
NETWITNESS
An RSA Business

SOCWISE
POWERED BY EURO ONE

NetWitness® Plattform

Beschleunigte Erkennung von Bedrohungen und Reaktion vom Endpunkt bis zur Cloud



Um bei einer zunehmenden Zahl ausgefeilter neuer Bedrohungen immer einen Schritt voraus zu sein, müssen Unternehmen heute Wege finden, um sich einen Überblick zu verschaffen, Vorfälle effektiv zu untersuchen und gleichzeitig falsch positive Ergebnisse, die Zeit kosten, zu vermeiden.
In der Vergangenheit mussten Unternehmen Daten aus verschiedenen Systemen, die oft in Silos arbeiteten, in Beziehung zueinander setzen. Dadurch wurde Arbeitszeit verbraucht, die für Alltagsaufgaben hätten aufgewendet werden können, was zu Überlastung von Sicherheitsanalysten führte oder potenzielle Bedrohungen unbeachtet ließ. Unternehmen müssen vollständige Transparenz anstreben und Analysen mit Geschäftskontext und Bedrohungsdaten in Beziehung setzen, um die wesentlichen Bedrohungen zu erkennen und auf sie zu reagieren. Sie müssen über ein effizientes, organisiertes Verfahren verfügen, das sich der Aufgabenautomatisierung bedient, damit Probleme schnell und konsequent gelöst werden können.

Kampf gegen die ständig wachsende Vielfalt immer heimtückischerer Bedrohungen

Sicherheitsteams müssen sich ständig weiterbilden, um Angreifern und neuesten Bedrohungen immer einen Schritt voraus zu sein. In den letzten Jahren ist dies jedoch noch schwieriger geworden. Denn auch die Angreifer entwickeln sich weiter und verwenden ausgefeilte Techniken, um Unternehmen zu infiltrieren, die heute über keine klar definierten Grenzen mehr verfügen. Angreifer wenden erhebliche Ressourcen für die Aufklärung auf, um mehr über Unternehmen zu erfahren und Techniken zu entwickeln, die speziell auf die Umgehung von Sicherheitstools bestimmter Unternehmen ausgerichtet sind.
Raffiniertes Agieren und die immer größer werdenden Angriffsflächen machen es für die ohnehin schon überlasteten Sicherheitsteams fast unmöglich, das gesamte Ausmaß von Bedrohungen schnell genug zu erkennen sowie zu verstehen und dann noch zu reagieren, bevor sich die Bedrohungen negativ auf das Unternehmen auswirken.
Die fortgeschrittene und ständig wachsende Angriffsfläche moderner IT-Infrastrukturen übersteigt mittlerweile die Möglichkeiten herkömmlicher SIEM-Systeme (Security Information and Event Management). Sicherheitsteams müssen in der Lage sein, Gefährdungen schnell zu erkennen und ihr gesamtes Ausmaß zu verstehen, damit sie entsprechend reagieren können, bevor sich die Bedrohungen auf das Unternehmen auswirken.
Angreifer verschaffen sich Zugang zur Infrastruktur eines Unternehmens - in der Regel innerhalb von Minuten – und extrahieren sensible Daten innerhalb weniger Tage. Es kann Monate dauern, bis diese Sicherheitslücken entdeckt werden, und sie werden oft von externen Behörden und nicht von internen Sicherheitssystemen entdeckt.

Unternehmen haben Schwierigkeiten, Sicherheitslücken schnell zu erkennen und darauf zu reagieren. Gründe dafür sind:

- Unverhältnismäßiges Vertrauen in präventive Kontrollen und protokollzentriertes SIEM.
- Blinde Flecken im gesamten Netzwerk, am Endpunkt und in der virtuellen und der Cloud-Infrastruktur.
- Isolierte Datenquellen ohne Korrelation oder Analyse über mehrere Datensätze hinweg.
- Fehlen von Bedrohungsdaten und Vermischung der Sicherheitsdaten mit Geschäftsinformationen.

Die Bedrohungslandschaft wird immer vielfältiger:

- Da Anwendungen, Daten und alltägliche Datenverarbeitung in die Cloud verlagert werden, ist die Sichtbarkeit von Ereignissen unterschiedlich.
- Die Angreifer sind gut ausgestattet, gehen zielgerichtet vor und kennen die blinden Flecken der Unternehmen.
- Angreifer müssen nur einmal richtig liegen, Sicherheitsteams müssen jedes Mal richtig liegen.

Die Sicherheitsteams bemühen sich stets um eine effiziente und effektive Erkennung und Reaktion, aber:

- Technische Experten haben Mühe, die Flut von Warnmeldungen ohne Priorisierung rechtzeitig auszuwerten.
- Sicherheitsanalysten sind oft auf manuelle Korrelation, Erkennung und Untersuchung angewiesen.
- Es ist außerdem zeitaufwendig zu verstehen, wie sich Sicherheitsvorfälle auf das Unternehmen auswirken.

Die NetWitness Plattform bedient sich fortschrittlichster Technologie, um Bedrohungen in einem Bruchteil der Zeit, die andere Sicherheitsprodukte benötigen, zu erkennen, zu priorisieren und zu untersuchen.

Die Transparenz, die Sie benötigen, um effektiv auf bekannte und unbekannte Bedrohungen zu reagieren

Durch eine einzigartige Kombination aus Verhaltensanalyse, Data-Science-Techniken und Bedrohungsanalyse erkennt sie bekannte und unbekannte Angriffe. Sie zeigt das gesamte Ausmaß eines Angriffs auf, indem Vorfälle über einen längeren Zeitraum miteinander verbunden, Vorfälle schnell priorisiert und tiefere Einblicke durch Automatisierung und maschinelles Lernen geliefert werden.

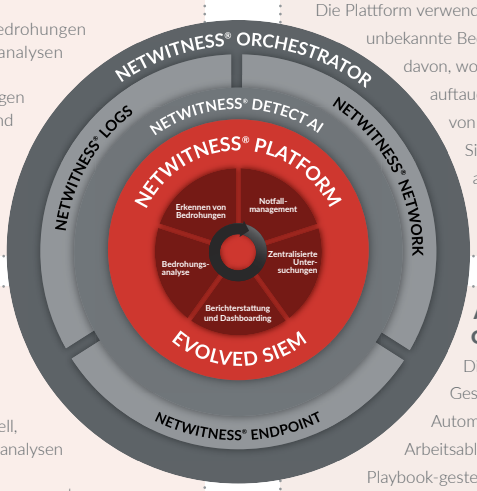
Die NetWitness Plattform vereint die Lösungen Evolved SIEM und XDR, die als Herzstück des Security Operations Center (SOC) unübertroffene Transparenz, Analysen und automatische Reaktionsmöglichkeiten garantieren. Sie ermöglicht den Sicherheitsteams, bekannte und unbekannte Angriffe zu erkennen und abzuwehren.

- Sie bietet Einblick wie kein anderes System in Protokolle, Netzwerk, Endgeräte, Benutzerverhalten und NetFlow-Daten, angereichert mit Geschäftskontext und Bedrohungsinformationen.
- Sie ermöglicht Abstimmung des Geschäftskontexts mit den Sicherheitsrisiken, um sicherzustellen, dass die IT-Sicherheit zur Unterstützung der strategischen Ziele des Unternehmens optimiert wird.
- Sie identifiziert neue, zielgerichtete und unbekannte Bedrohungen mit Data-Science-Analysen und durch maschinelles Lernen in Echtzeit, um wirklich jeden Angriff zu erkennen.

- Sie ermöglicht es Sicherheitsteams, die Nachforschungen zu beschleunigen, indem sie anhand von Protokollen nach neu erstellten Sitzungen sucht, um zu ermitteln, was passiert ist.
- Sie ermöglicht ein sofortiges Verständnis des gesamten Umfangs eines Angriffs und versetzt SOC-Teams in die Lage, dreimal effizienter zu erkennen und effektiver zu reagieren, indem Bedrohungsdaten besser mit dem Kontext verschränkt werden.
- Sie ist skalierbar von der kleinsten bis zur größten Organisation.

FORTSCHRITTLICHES ERKENNEN VON BEDROHUNGEN
Die Plattform erkennt und identifiziert Bedrohungen mithilfe ausgefeilter Regeln, Bedrohungsanalysen und Malware-Analysen. Hochentwickelte Algorithmen zur Erkennung von Bedrohungen arbeiten über verschiedene Datentypen und -quellen hinweg und ermöglichen eine schnelle Identifizierung und Korrelierung von Kompromissindikatoren (IOCs) sowie eine Echtzeit-Priorisierung von wirklichen Bedrohungen.

VERHALTENSANALYSE
Die Plattform verwendet unüberwachtes maschinelles Lernen, um unbekannte Bedrohungen schnell zu erkennen, unabhängig davon, wo sie im Lebenszyklus eines Angriffs auftauchen. Durch die zuverlässige Erkennung von Unregelmäßigkeiten kann Ihr bestehendes Sicherheitsteam effizienter und effektiver arbeiten, ohne die Algorithmen manuell feinabstimmen zu müssen.



UMFASSENDE TRANSPARENZ
Die Plattform bietet unübertroffene Transparenz über Protokolle, Pakete, Endpunkte und NetFlow-Daten hinweg und das in lokalen, virtuellen und Cloud-Umgebungen. Ein einheitliches Datenmodell, das mit Geschäftskontext und Bedrohungsanalysen angereichert ist, ermöglicht es Analysten, Unregelmäßigkeiten miteinander in Beziehung zu setzen, wo immer sie auch auftreten, und bietet so einen schnellen Einblick in das gesamte Ausmaß eines Angriffs.

AUTOMATISIERUNG UND ORCHESTRIERUNG
Die Plattform erhöht die Effizienz und Geschwindigkeit des SOC durch die Automatisierung von Sicherheitsaufgaben und Arbeitsabläufen. NetWitness Orchestrator bietet Playbook-gesteuerte, automatisierte Maßnahmen und maschinelles Lernen, wobei Ihr gesamtes Sicherheitsarsenal berücksichtigt wird.

GESCHÄFTSBEZOGENE SICHERHEIT
In dem Maße, in dem Unternehmen eine Veränderung ins Digitale durchmachen, wird das digitale Risiko auch zum Geschäftsrisiko. Die NetWitness Plattform gleicht Geschäfts- und Sicherheitsrisiken ab, integriert Risikofaktoren wie die Kritikalität von Anlagen und die Identität von Benutzern und koordiniert schließlich die Maßnahmen auf Vorfälle in Ihrem Unternehmen.

Fortschrittliches Erkennen von Bedrohungen

Die Plattform erkennt und identifiziert Bedrohungen mithilfe ausgefeilter Regeln, Bedrohungsanalysen und Malware-Analysen sowie Verhaltensanalysen. Hochentwickelte Algorithmen zur Erkennung von Bedrohungen arbeiten über verschiedene Datentypen und -quellen hinweg und ermöglichen eine schnelle Identifizierung und Korrelierung von Kompromissindikatoren (IOCs) sowie eine Echtzeit-Priorisierung von wirklichen Bedrohungen.

Verhaltensanalyse

Eine Lösung zur Verhaltensanalyse von Benutzern und Unternehmenseinheiten ist ein zentraler Bestandteil der NetWitness Plattform. NetWitness Detect AI ist eine Cloud-native, Big-Data-gesteuerte Lösung für erweiterte Analysen und maschinelles Lernen, die als zentraler Bestandteil in die NetWitness-Plattform integriert ist. Sie bedient sich der unüberwachten statistischen Anomalieerkennung und Data Science, um eine umfassende Erkennung unbekannter Bedrohungen zu ermöglichen.

Umfassende Transparenz

Die Plattform bietet unübertroffene Transparenz über Protokolle, Netzwerk, Endpunkte und NetFlow-Daten in Cloud-, virtuellen und lokalen Umgebungen hinweg. Ein gemeinsames Datenmodell, das mit Geschäftskontext und Bedrohungsanalyse angereichert ist, ermöglicht es Analysten, Anomalien miteinander in Verbindung zu setzen, wo immer sie auftreten, und so einen schnellen Einblick in das gesamte Ausmaß eines Angriffs zu erhalten.

Automatisierung und Orchestrierung

Die Plattform ermöglicht es dem gesamten Sicherheitsteam, potenziellen Bedrohungen schnell und effizient zu begegnen, indem Menschen und Technologien in einen gemeinsamen Strategieplan integriert werden. Sicherheitsmaßnahmen können leicht zusammen durchgeführt und teamübergreifend koordiniert werden, wobei die Automatisierung zur Ausführung sich wiederholender Aufgaben genutzt wird. Deshalb kann die Zeit der Analysten konsequent für wichtige Aufgaben genutzt werden und Doppelgleisigkeiten oder verpasste Aufgaben während einer Untersuchung werden minimiert. Durch die Zusammenführung aller relevanten Informationen und Erkenntnisse im Verlauf einer Untersuchung können die Entscheidungsträger den Beteiligten das Risiko leicht vermitteln und rasche Maßnahmen setzen.

Geschäftsbezogene Sicherheit

In dem Maße, in dem Unternehmen eine Veränderung ins Digitale durchmachen, wird das digitale Risiko auch zum Geschäftsrisiko. Die NetWitness Plattform gleicht Geschäfts- und Sicherheitsrisiken ab, integriert Risikofaktoren wie die Kritikalität von Anlagen und die Identität von Benutzern und koordiniert schließlich die Maßnahmen in Reaktion auf Vorfälle in Ihrem Unternehmen.

Flexible und skalierbare Plattform

Die NetWitness Plattform ist eine modulare Lösung, das Herzstück eines fortschrittlichen Sicherheitskonzepts, zur Erkennung von und Reaktion auf Bedrohungen. Es reichert die Daten zum Erfassungszeitpunkt an und erstellt Metadaten, um Alarmierung und Analyse drastisch zu beschleunigen und das gesamte Ausmaß eines Angriffs schnell zu erkennen. Zu den Kernfunktionen der NetWitness Plattform gehören ein einheitliches Datenmodell, radikale Skalierbarkeit und die flexiblen Einsatzmöglichkeiten sowie die ausgefeilten Analyse-Tools, die forensischen Funktionen und die Reporting-Engine.

Durch die Zusammenführung aller relevanten Informationen und Erkenntnisse im Verlauf einer Untersuchung können die Entscheidungsträger den Beteiligten das Risiko leicht vermitteln und rasche Maßnahmen setzen.

NetWitness Logs

NetWitness Logs bietet grundlegenden Einblick in alle relevanten Protokollquellen, einschließlich verschiedener branchenführender Netzwerk- und Sicherheitsgeräte, gängiger Anwendungen und Betriebssysteme, um sich gegen eine breite Bedrohungslandschaft zu schützen. NetWitness Logs ist eine Sicherheitsüberwachungslösung, die Protokolldaten aus einer Vielzahl von Quellen sammelt, analysiert, auswertet und speichert, um Bedrohungen schneller zu erkennen und Initiativen zur Einhaltung von Sicherheitsrichtlinien und Vorschriften zu unterstützen.

NetWitness Network

NetWitness Network sammelt und analysiert Netzwerkdaten in Echtzeit, um die Möglichkeiten eines Sicherheitsteams zur Erkennung von und Reaktion auf moderne Bedrohungen zu vermehren. Die Lösung indiziert Netzwerkpaketdaten, reichert sie gleich zum Erfassungszeitpunkt an und setzt sie in Beziehung zueinander, um sofort umfassende Transparenz zu ermöglichen. NetWitness Network bietet umfangreiche forensische Funktionen wie die Sitzungsrekonstruktion, sodass Analysten eine E-Mail aus Netzwerkdaten rekonstruieren können, um Bedrohungen auf eine Weise aufzudecken, wie präventive Lösungen dazu nicht imstande sind.

NetWitness Endpunkt

Kontinuierliche Überwachung und Reaktion am Endpunkt – darunter versteht man z. B. Laptops, Desktops, Server und virtuelle Maschinen – für umfassende Transparenz und leistungsstarke Analyse aller Bedrohungen an den Endpunkten eines Unternehmens. NetWitness Endpunkt nutzt die einzigartige, kontinuierliche Überwachung des Endpunktverhaltens und umfangreiche Reaktionskomponenten, um tiefer einzutauchen und neue, gezielte, unbekannte und sogar dateilose Angriffe genauer und schneller zu identifizieren, die von anderen Endpunktsicherheitslösungen vollständig unbeachtet bleiben.

NetWitness Orchestrator

Gehen Sie Bedrohungen schnell und konsequent an, indem Sie Menschen und Technologien in einem gemeinsamen Strategieplan vereinen. Arbeiten Sie gemeinsam und reagieren Sie koordiniert, indem Sie wiederkehrende Aufgaben schnell und konsequent automatisieren. Entscheidungsträger können Risiken einfach kommunizieren und können durch relevante Einblicke rasch handeln, außerdem werden Untersuchungen durch kontextbezogene Bedrohungsanalysen im Herzen der Lösung verbessert. Dies stellt sicher, dass die Sicherheitsteams sofort einen Überblick über alle verbundenen Indikatoren haben, die aus massiven Datenmengen aus verschiedenen Quellen erstellt werden, um rascher Entscheidungen treffen zu können.

NetWitness Detect AI

Die künstliche Intelligenz von NetWitness verbessert die Arbeit Ihres bestehenden Sicherheitsteams durch die schnelle Erkennung unbekannter Bedrohungen und ungewöhnlicher Verhaltensweisen in jeder Phase des Angriffslebenszyklus. Die leistungsstarke Engine für maschinelles Lernen ermöglicht eine zuverlässige Erkennung von Bedrohungen in zahlreichen Anwendungsfällen. NetWitness führt kontinuierlich eine Feinabstimmung der Algorithmen für maschinelles Lernen durch, damit Sie das nicht tun müssen und damit NetWitness Detect AI in dem Moment, in dem Sie es einschalten, bereit ist, ungewöhnliches Verhalten schnell und genau zu erkennen.

Professionelle Dienstleistungen

NetWitness bietet Mehrwertdienste an, die sich bewährter Beratungspraktiken unserer Global Services-Organisation bedienen, um die Bemühungen der Kunden im Bereich der Cybersicherheit in den folgenden Bereichen zu unterstützen:

- Der Bereich Incident Response (IR – Reaktion auf Vorfälle) unterstützt Unternehmen bei der Erkennung und Eindämmung von Cyberangriffen auf ihre digitalen Geschäftssysteme. Ein Pool erfahrener Mitarbeiter kann schnell und weltweit eingesetzt werden, um Cyberbedrohungen zu erkennen, zu entschärfen und zu beseitigen. IR-Dienste können als „Retainer" oder „Rapid Deployment" in Anspruch genommen werden.
- Die Planungs-, Design-, Implementierungs-, Verwaltungs- und Integrationsdienstleistungen ergänzen die kundeneigenen Bereitstellungs- und Entwicklungskapazitäten und sorgen für eine schnellstmögliche Inbetriebnahme der NetWitness Plattform sowie für die Überbrückung laufender Sicherheitsprogramme zur Verbesserung der laufenden Effektivität von SOC/CIRT.
- Unser Schulungsteam bietet Kurse für Administration und Analyse an, die vom Anfänger- bis zum Expertenniveau reichen und verschiedene Modalitäten abdecken.

Mehr über die NetWitness Plattform erfahren Sie unter rsa.com.
Über die NetWitness Plattform erfahren Sie mehr auch auf unserer YouTube Playlist oder auf unserem Blog.

Sicherheitsteams bedienen sich der NetWitness Plattform, um neuen und aufkommenden Bedrohungen jeweils einen Schritt voraus zu sein, da es sich um eine weiterentwickelte SIEM- und Bedrohungsabwehrlösung handelt, die Sicherheitsteams in die Lage versetzt, das gesamte Ausmaß einer Gefährdung schnell zu erkennen und zu verstehen.
Die Plattform gleicht den Geschäftskontext mit den Sicherheitsrisiken ab, um die Lücken von reinen Technologielösungen zu schließen und sicherzustellen, dass die IT-Sicherheit zur Unterstützung der strategischen Ziele eines Unternehmens optimiert wird.
Die NetWitness Plattform bietet die umfassendste Transparenz, integriert Protokolle, Netzwerkdaten und Endpunkte und nutzt Bedrohungs- und Verhaltensanalysen, um Bedrohungen zu analysieren, zu priorisieren, zu untersuchen und die Reaktion zu automatisieren. Diese unübertroffene Breite an Einblicken und die Technologietiefe machen Sicherheitsanalysten effektiver und effizienter.

- Sie können sicher sein, dass sie alle Systeme im Blick haben, um Bedrohungen zu erkennen, bevor sie dem Unternehmen schaden können.
- Eine Anpassung des Unternehmenskontextes an die Sicherheitsrisiken ist Standard, um die Lücken von reinen Technologielösungen zu schließen.
- Sie können darauf vertrauen, das ganze Ausmaß der Bedrohung richtig einschätzen zu können.
- Schaffen Sie ein effizienteres und effektiveres Sicherheitsteam – ohne zusätzliches Personal.

Über die NetWitness Plattform

NetWitness, ein RSA®-Unternehmen, bietet umfassende und hoch skalierbare Ressourcen zur Erkennung von Bedrohungen und zu entsprechender Maßnahmensetzung für Unternehmen in aller Welt. Die NetWitness Plattform bietet umfassende Transparenz in Kombination mit angewandter Bedrohungsanalyse und Analyse des Benutzerverhaltens, um Bedrohungen zu erkennen, zu priorisieren, zu untersuchen und die Maßnahmen dagegen zu automatisieren. Sie ermöglicht Sicherheitsanalysten, effizienter zu arbeiten und geschäftsrelevanten Bedrohungen stets einen Schritt voraus zu sein. Weiterführende Informationen finden Sie unter netwitness.com.

NETWITNESS
An RSA Business

©2021 RSA Security LLC oder seine verbundenen Unternehmen. Alle Rechte vorbehalten. RSA, das RSA-Logo und NetWitness sind eingetragene Markenzeichen oder Marken der RSA Security LLC oder ihrer Tochtergesellschaften in den Vereinigten Staaten und anderen Ländern.
Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. RSA ist überzeugt, dass die Informationen in diesem Dokument korrekt sind. Änderungen vorbehalten. 3/21 Solution Brief H18492-4 W448314

SOCWISE
POWERED BY EURO ONE

Für weitere Informationen wenden Sie sich an **socwise.eu** oder kontaktieren Sie:
Gergely Lesku, Head of Business Development bei SOCWISE via E-Mail:
lesku.gergely@socwise.eu oder Telefon: +36309627597
Mehr über die NetWitness Plattform erfahren Sie unter **rsa.com**