RSA NetWitness® Endpoint

Schnellere Erkennung von Bedrohungen. Verkürzte Verweildauer. Automatisierte Reaktion.

Hauptmerkmale

- *EDR, NDR, SIEM, UEBA, O&A in einer kompletten Plattform*
- *Prozessvisualisierung*
- *Fortlaufende bedrohungssensitive Authentifizierung*
- *Einzelner manipulationssicherer Agent für Protokolle, Endpunkt-Kernel und Metadatenerfassung*
- *Erste integrierte endpunktbasierte UEBA*
- *Breites Spektrum an Erkennungsalgorithmen für Verhaltensanalysen*
- *Innovative und anpassbare Engine für Risikobewertung*

In einer Ära ständig wachsender Angriffsflächen ist der Schutz vor Bedrohungsakteuren – von Commodity-Malware über Insiderbedrohungen und Crimeware bis hin zu staatlich tolerierten Angriffen, Hacktivisten und Terroristen – zu einer immer komplexeren Aktivität geworden. Nicht alle Bedrohungen werden auf die gleiche Weise erstellt; und dennoch sind die getrennten Silos der Präventions-, Monitoring- und Ermittlungstechnologien nach wie vor nicht in der Lage, die SOCs (Security Operations Centers) so zu unterstützen, dass falsch positive Ergebnisse schnell erkannt und zielgerichtete Indikatoren bereitgestellt werden (im Gegensatz zu offenen Silo-Warnmeldungen). Eine umfassende und kooperative Lösung ist erforderlich, mit der Sicherheitsanalysten die für ihr Unternehmen wichtigsten Bedrohungen erkennen und darauf reagieren können.

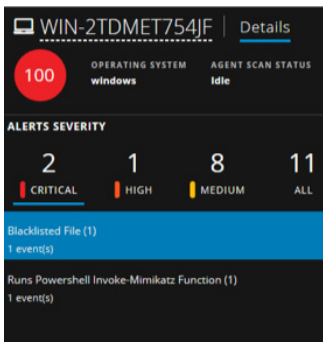
Angesichts der mobilen Mitarbeiter von heute, die zunehmend extern in nicht vertrauenswürdigen Netzwerken eingesetzt werden und anschließend wieder in vertrauenswürdigen Umgebungen angemeldet sind, bleiben Endpunkte – jetzt mehr denn je – der am stärksten gefährdete Angriffsvektor.

RSA NetWitness® Endpoint ist eine vollständig integrierte Lösung für die Erkennung und Abwehr von Endpunktbedrohungen, ein zentrales Produktangebot innerhalb der RSA NetWitness Platform, das ein fortlaufendes Monitoring von Endpunkten ermöglicht, um Sicherheitsanalysten umfassende Einblicke in sowie die leistungsstarke Analyse von allen Bedrohungen auf den Endpunkten eines Unternehmens zu bieten. Anstelle von Signaturen oder Regeln nutzt die IT ein einzigartiges kontinuierliches Monitoring des Verhaltens sowie erweitertes maschinelles Lernen, um die Endpunkte besser zu analysieren. Auf diese Weise werden Zero-Day-Angriffe sowie versteckte und Non-Malware-Angriffe identifiziert, die andere Endpunktsicherheitslösungen völlig übersehen.

Unglaublich leicht. Kein durchschnittlicher Agent.

RSA NetWitness Endpoint bietet einen einzigen, skalierbaren und schnellen manipulationssicheren Agent, der sofortige Einblicke, Reaktionen und Metadatenerfassung sowohl von Windows-Protokollen als auch von den Kernprozessen der Endpunkte liefert. Dieses Maß an Sichtbarkeit und umsetzbaren Einblicken sorgt für eine unternehmensweite Ansicht aller Endpunkte mit einem vollständigen Angriffslebenszyklus sowie Incident-Response-Untersuchungen auf Windows-, macOS- und Linux-Betriebssystemen.

Umfassende Analyse von Nutzer- und Entitätsverhalten



Die RSA NetWitness Platform bietet Modelle für maschinelles Lernen, die auf Deep-Endpoint-Prozessdaten basieren, um Anomalien im Nutzer- und Maschinenverhalten schnell zu erkennen – und das alles auf einer einzigen, vollständigen Plattform. RSA NetWitness Endpoint und RSA NetWitness UEBA, die wichtigsten Produktangebote der RSA NetWitness Platform, liefern umfassende Sichtbarkeit, die die Erkennungs- und Reaktionsfähigkeit von Sicherheitsanalysten steigert, und zwar unabhängig davon, auf welchem Gebiet die Angreifer tätig werden. Missbräuchliche Nutzung/Missbrauch von PowerShell, bösartiges Scripting, Prozess- und Kernel-Hooks, Registrierungsangriffe, Speicherexfiltration, dateilose Angriffe und vieles mehr werden schnell erkannt, da die RSA NetWitness Platform in der Lage ist, Millionen von Ereignissen zu korrelieren, ohne dass eine manuelle Analyse oder Anpassung von Regeln und Signaturen erforderlich ist.

Mit der RSA NetWitness Platform erhalten SOC- und IT-Teams einen netzwerk- und endpunktübergreifenden Überblick über den gesamten Angriffsumfang sowie umsetzbare Informationen, die Sicherheitsanalysten für eine optimierte Bedrohungsanalyse und -reaktion benötigen.

RSA

Hauptvorteile

- *Verringerte durchschnittliche Zeit für Erkennung, Untersuchung und Reaktion*
- *Schnellere Incident Response und kürzere Verweildauer*
- *Einzigartige Sichtbarkeit in Verhaltensanomalien von Endpunkten gewährleistet frühzeitige Bedrohungserkennung*
- *Bedrohungssensitive Authentifizierung identifiziert verdächtige Nutzer und kompromittierte Konten*
- *Schnellere Ursachenanalyse*
- *Netzwerk- und endpunktübergreifender Überblick über den gesamten Angriffsumfang*

Verbesserte Reaktionszeit. Weniger Auswirkungen einer Sicherheitsverletzung.

Ein wichtiger Aspekt der effektiven Problembehebung ist, zu verstehen, wie weit sich ein zielgerichteter Angriff im Netzwerk ausgebreitet hat. RSA NetWitness Endpoint bietet diese umfassende Bedrohungssichtbarkeit und stärkt Sicherheitsteams mit zielgerichteten Reaktionsfähigkeiten, sodass Incidents auf allen Endpunkten im Unternehmen rasch behoben werden können. RSA NetWitness Endpoint erfasst schnell die entscheidenden Daten, die für eine effektive forensische Untersuchung benötigt werden, und ermittelt sofort alle infizierten Endpunkte. Damit lassen sich den Umfang und Ausmaß eines Angriffs unmittelbar nachvollziehen.

Sicherheitsteams können einen Endpunkt im Netzwerk isolieren, die Kommunikation des Angreifers und eine laterale Bewegung der Bedrohung verhindern sowie Bedrohungen über alle infizierten Endgeräte hinweg blockieren und isolieren. Umfassende Untersuchungen und Metadatenintegrationen mit der RSA NetWitness Platform ermöglichen es Unternehmen, den vollen Umfang eines Angriffs über Netzwerk- und Endpunkttelemetrie zu erkennen und so die Security-Operations-Reaktion zu optimieren.

Die RSA NetWitness Platform

Mit mehr als 30 Jahren Erfahrung im Sicherheitsbereich ist RSA mit innovativen Lösungen für die größten Herausforderungen bei Security Operations weltweit der Branchenführer. Das neue eingebettete Produkt RSA NetWitness Endpoint erweitert die RSA NetWitness Platform und die Angebote für fortschrittliches SIEM und Threat Defense und bietet so umfassende Sichtbarkeit über Protokolle, Netzwerke und Endpunkte hinweg.

Informationen über RSA

Mit den Lösungen von RSA® Business-Driven Security™ können Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. Dank der Lösungen für schnelle Erkennung und Reaktion, Nutzerzugriffskontrolle, Verbraucherschutz und integriertes Risikomanagement können RSA-Kunden erfolgreich sein und sich kontinuierlich an Transformationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com/de-de.