Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

11.08. 2022

Fortinet unterstützt aktives Cloud-Risikomanagement mit neuem Cloud-native-Angebot

Von PPS

(Zürich)(PPS) **Fortinet®, ein weltweit führender Anbieter von umfassenden, integrierten und automatisierten Cybersecurity-Lösungen, stellt FortiCNP vor. Das neue «Built-in-the-Cloud»-Angebot referenziert Security-Erkenntnisse aus allen in einer Cloud-Umgebung gesammelten Daten eines Unternehmens, um einen reibungslosen Cloud-Security-Betrieb zu ermöglichen.**

FortiCNPs patentierte Resource Risk Insights (RRI)-Technologie liefert kontextbezogene Handlungsempfehlungen. Diese helfen Teams dabei zu priorisieren, welche Bedrohungen für die Sicherheit der Cloud-Workloads am gefährlichsten sind und daher als erstes abgewehrt werden müssen. Und das, ohne dabei den Betrieb zu verlangsamen.

Bekannt gegeben wurde ausserdem, dass Fortinet ein Amazon Web Services (AWS) Launch-Partner für Amazon GuardDuty Malware Protection ist. Die Lösung bietet agentenlose Malware-Erkennungsfunktionen für AWS-Datenspeicher, Festplattenlaufwerke und Workload-Images. FortiCNP unterstützt Amazon GuardDuty Malware Protection und bietet Bedrohungsschutz nahezu in Echtzeit mit Zero-Permission-Funktionen zum aktiven Scannen laufender Workloads ohne negative Auswirkungen auf den Betrieb.

Die wachsende Geschwindigkeit der Cloud-Nutzung als Teil hybrider IT-Architekturen ermöglicht Unternehmen kürzere Markteinführungszeiten und ein besseres

Reaktionsvermögen auf Kundenbedürfnisse. Die Cloud kann jedoch das allgemeine Sicherheitsrisiko erhöhen. Eine Gegenmassnahme ist üblicherweise, die bestehende Infrastruktur eines Unternehmens, um neue Security-Lösungen zu erweitern. Jede dieser Lösungen bringt eine ganze Reihe von Warnmeldungen mit sich, die oft eine manuelle Analyse erfordern und so schnell einen hohen Aufwand verursachen.

«Ohne die richtigen Tools müssen die Security-Experten täglich Hunderte, wenn nicht gar Tausende von Benachrichtigungen manuell überprüfen», erklärt Doug Cahill, Vice President, Analyst Services and Senior Analyst bei der Enterprise Strategy Group (ESG). «Teams, die mit Warnungen überschwemmt werden, müssen mit verminderter Produktivität, ineffizienten Arbeitsabläufen und Security-Risiken rechnen, die schneller anfallen, als sie behoben werden können. FortiCNP hilft den Teams dabei, auf einen Blick die wichtigsten Benachrichtigungen zu sehen.»

Kunden profitieren bereits von den Vorteilen des FortiCNP-Ansatzes für Cloud-natives Risikomanagement:

«FortiCNP bietet uns eine umfassende Cloud-Transparenz mit einem intuitiven Dashboard, mit dem wir das Risikomanagement über einen längeren Zeitraum verfolgen können», so Caio Hyppolito, Chief Technology Officer (CTO) der BK Bank. «Am wichtigsten ist es, dass sich unser Team darauf fokussieren kann, unsere wichtigen Ressourcen zu sichern – ohne sich durch Listen von Warnmeldungen wühlen zu müssen. Die Integration mit den bereits vorhandenen Produkten bietet uns einen noch grösseren Nutzen: umfassendere Transparenz sowie ein einfacheres, aktiveres Cloud-Security-Management.»

Auch Partner nutzen FortiCNP, um ihr Angebot zu erweitern:

«Als AWS Level 1 MSSP Competency Partner legt Observian Wert darauf, dass unsere Serviceangebote Kunden beim Aufbau skalierbarer, sicherer Cloud-Implementierungen unterstützen. Observian freut sich, einen neuen Service anbieten zu können, der Fortinets neue Cloud-Native Protection-Lösung FortiCNP mit Observians bewährten Managed Detection- und Response-Services verbindet», sagt Scott Plamondon, Mitbegründer und VP of Architecture bei Observian. «FortiCNP ermöglicht es Kunden, die nativen Cloud-Security-Services von AWS einfach zu integrieren, schneller in Betrieb zu nehmen und sofort von ihnen zu profitieren. Mit gezielteren und handlungsbezogenen Benachrichtigungen, die auf ihre Bedürfnisse abgestimmt sind. Unsere Kunden, die sich auf das Security-Operations-Team von

Observian verlassen, werden von unserer Fähigkeit profitieren, diese Benachrichtigungen noch besser zu sortieren und rund um die Uhr Berichte zu erstellen.»

Eine Kernfunktion von FortiCNP ist die Integration mit Security-Produkten und -Services von AWS sowie der Fortinet Security Fabric. Die ermöglicht Unternehmen, ihre Cloud-Umgebungen effektiver abzusichern und den Nutzen ihrer Cloud-Security-Investitionen zu maximieren.

«Bei AWS stellen wir unseren Kunden intelligentere Tools zur Verfügung, mit denen sie einfach Massnahmen ergreifen und Risiken schneller eindämmen können», sagt Jon Ramsey, Vice President (VP) AWS Security. «Dank Security-Partnern wie Fortinet mit ihrem FortiCNP-Angebot, das auf AWS aufgebaut und in unsere Security-Services wie Amazon GuardDuty integriert ist, können Kunden ihre Cloud-Reise mit Cloud-nativen Security-Services vereinfachen und beschleunigen.»

FortiCNP bietet die folgenden Funktionen, mit denen Security-Teams Cloud-Risiken effektiver verwalten können:

- FortiCNP Resource Risk Insights (RRI)TM nutzt einen patentierten Risikobewertungsalgorithmus, um sicherheitsrelevante Informationen von Fortinet Cloud Security-Lösungen und AWS-Produkten und -Services in einen Zusammenhang zu bringen. So kann die Anwendung den Teams priorisierte, kontextreiche Handlungsempfehlungen darüber zukommen lassen, welche Ressourcen das höchste Risiko darstellen und sofortige Aufmerksamkeit erfordern.
- Durch die Analyse, Korrelation und Kontextualisierung von sicherheitsrelevanten Informationen aus AWS Cloud-Security-Services mit FortiCNP können Kunden den Wert ihrer Security-Lösungen maximieren. Sie profitieren von den einfachen Funktionen zur Bereitstellung von Amazon GuardDuty Malware Protection, Amazon Inspector, AWS Security Hub, AWS CloudTrail und AWS Organizations.
- Integrationen mit Amazon GuardDuty Malware Protection verwenden einen agentenlosen Zero-Permission Ansatz, um durch Scannen von Cloud-Speichern, Festplattenspeichern und Workload-Images Malware in der gesamten Datenlieferkette zu erkennen.
- Durch die Integration mit digitalen Workflow-Lösungen werden FortiCNP RRIs zu unmittelbar umsetzbaren Workflow-Aufgaben als Teil des Lebenszyklus der

Cloud-Infrastruktur.

- Bei Kunden, die Fortinet Cloud Security-Lösungen wie FortiGate-VM und FortiWeb nutzen, können RRIs Remediation-Massnahmen auslösen, um hochgefährliche Bedrohungen zu blockieren.
- FortiCNP scannt und überwacht Änderungen an Cloud-Daten kontinuierlich mit branchenführender Threat Intelligence und durch die FortiGuard Labs ermöglichtes Content Scanning.

ortiCNP wird kontinuierlich weiterentwickelt, um noch mehr Arten von Cloud-Security-Informationen verarbeiten zu können und diese über mehr Cloud-Workloads mit einem noch umfangreicheren Kontext zu versehen. Konsistente Workflows, die die Sicherheit in Public Clouds skalieren, helfen Teams, die Security-Abdeckung, Produktivität und Risikoabwehr zu verbessern – und das in Cloud-Geschwindigkeit. Cloud-native Integrationen reduzieren die Reibungsverluste von der Bereitstellung bis zum Betrieb. Mit konsistenten Workflows, die Cloud-native Services über mehrere Clouds hinweg nutzen, müssen Security-Teams nicht mehr die Feinheiten des Security-Service-Betriebsmodells jeder einzelnen Cloud-Plattformen beherrschen. So können Security-Teams ihre Produktivität steigern, indem sie den Backlog bei der Cloud-Security effektiv aufholen, Risiken abwehren und die Cloud-Security messbar verbessern.

«FortiCNP demonstriert wieder einmal Fortinets Bestreben, Fabric-Lösungen zu entwickeln, die die Unternehmenssicherheit mit Cloud-nativen Integrationen erweitern», betont John Maddison, EVP of Products und CMO bei Fortinet. «Wir freuen uns, weiterhin Lösungen anzubieten, mit denen Security-Experten von zeitaufwändiger Triage und manuellen Analyseprozessen zu einer aktiven Sicherung ihrer Cloud-Workloads übergehen und so ihr Cloud-Security-Risiko einfach nachvollziehen können.»

Die Ankündigung fusst auf der Beziehung zwischen Fortinet und AWS, die gemeinsam Kunden bei ihrer Reise zu AWS zu unterstützen. Fortinet wurde ausserdem zum AWS Security Competency Partner ernannt.

FortiCNP ist das jüngste Beispiel dafür, wie Fortinet zweckmässige Cloud-Security-Lösungen entwickelt, die mit AWS-Produkten und -Lösungen integriert werden können. Fortinet bietet eine sehr grosse Auswahl an Anwendungsfällen mit umfassender Sicherheit für AWS-Workloads, einschliesslich Firewall, Security Gateway, Intrusion Prevention und Web Application Security. Mit flexiblen

Beschaffungsoptionen im AWS Marketplace, einschliesslich Vertrags- und Verbrauchsangeboten, und einer Reihe von verfügbaren Formfaktoren, einschliesslich Software-as-a-Service (SaaS), virtueller Maschinen (VM), Containern und API-basiertem Schutz, können Kunden eine breite Palette von AWS-Sicherheits- und Beschaffungsanforderungen zum Schutz ihrer AWS-Arbeitslasten erfüllen.

Über die Organisation:

Über Fortinet
Fortinet (NASDAQ: FTNT) schafft durch seine Mission, Menschen, Geräte und Daten jederzeit zu schützen, eine digitale Welt, der wir immer vertrauen können. Aus diesem Grund entscheiden sich viele der weltweit grössten Unternehmen, Service Provider und Behörden für Fortinet, um ihre digitale Transformation sicher voranzutreiben. Die Fortinet Security Fabric-Plattform bietet umfassenden, integrierten und automatisierten Schutz über die gesamte digitale Angriffsfläche hinweg und sichert kritische Geräte, Daten, Anwendungen und Verbindungen vom Rechenzentrum über die Cloud bis hin zum Homeoffice. Als die Nummer 1, was die am häufigsten ausgelieferten Security Appliances angeht, vertrauen mehr als 580.000 Kunden Fortinet den Schutz ihrer Marke an. Fortinets Network Security Expert (NSE) Training Institute, eine Initiative der Fortinet Training Advancement Agenda (TAA), verfügt über eines der grössten und umfangreichsten Cybersecurity-Schulungsprogramme der Branche. Cybersecurity-Kurse und neue Karrieremöglichkeiten werden somit jedem zugänglich gemacht. Weitere Informationen dazu auf fortinet.com/de, auf dem Fortinet Blog oder bei den FortiGuard Labs.

Pressekontakt:

BCW Zürich
Hardturmstrasse 133
8037 Zürich

BCW im Auftrag von Fortinet
silja elmiger | account executive
+41.44.455.84.24

Kategorie
IT & Software & Neue Medien

---

unterstuetzt-aktives-cloud-risikomanagement-neuem-cloud-native-angebot