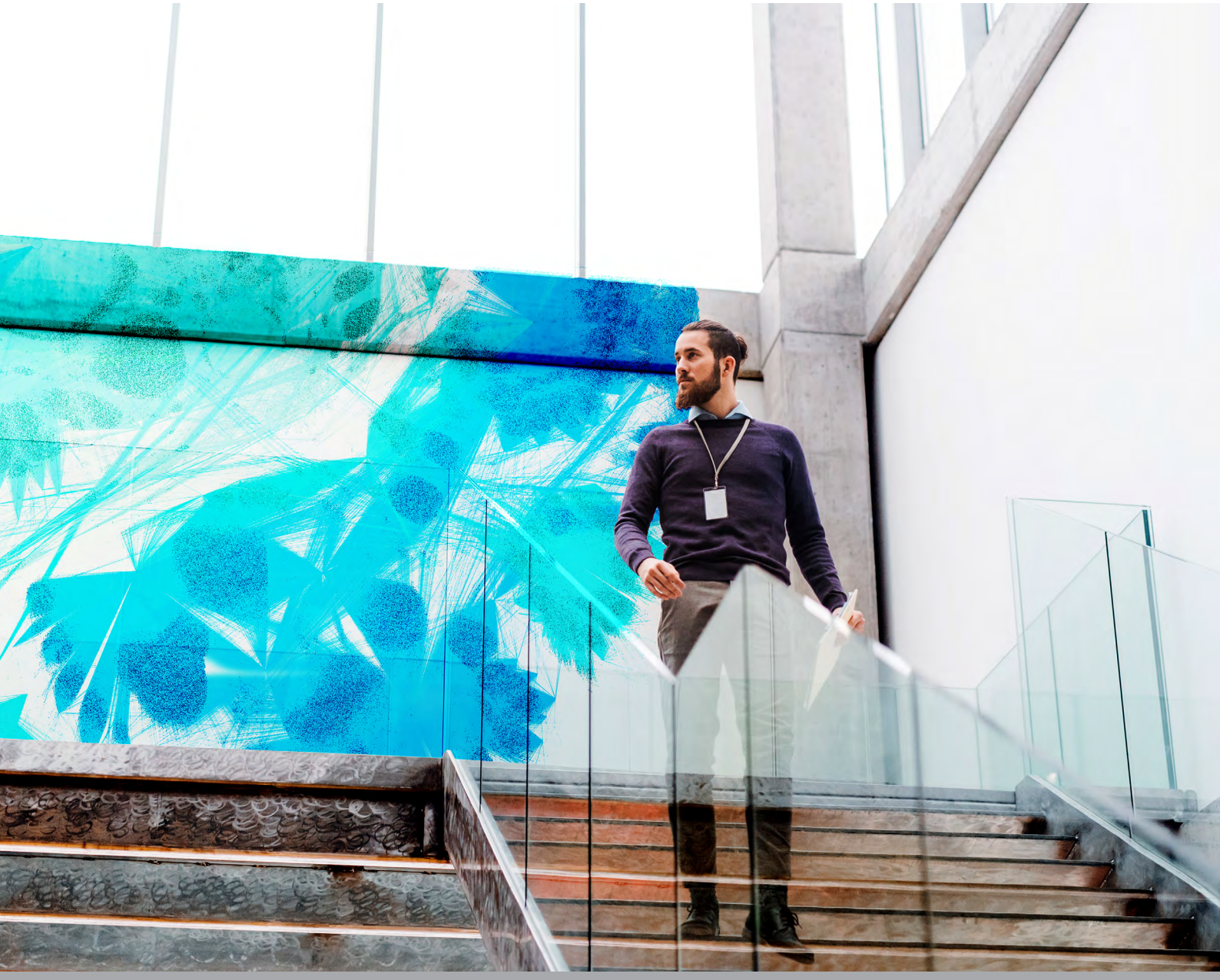
| Finanzdienstleistungen & Versicherungen

Cloud-Applikationen ganzheitlich absichern

Compliance von der DevOps-Entwicklung bis zur Produktion



KENNEN SIE DAS AUCH?

Als Versicherungsunternehmen möchten Sie Ihren Kunden besten Service bieten. Dazu gehört auch, neue digitale Anwendungen bereitzustellen – und das möglichst zeitnah. Denn wer will sich schon von Wettbewerbern abhängen lassen?

Die Fachabteilung lässt also einen neuen Service in der Cloud entwickeln. Nur leider werden Sie als IT Security-Verantwortlicher zu spät mit einbezogen. Die Cloud-Architekten haben bereits ein Konzept ausgearbeitet und dabei zwar auch an die Absicherung gedacht – aber eben nicht aus der richtigen Perspektive.

Jetzt stehen Sie da und sollen sich um die Einhaltung von Regularien wie PCI DSS, DSGVO und IT-Sicherheitsgesetz kümmern. Hier nachlässig zu sein, steht außer Frage. Nicht nur, weil sonst hohe Strafen drohen, sondern auch weil die Finanz- und Versicherungsbranche besonders häufig von Cyberangriffen betroffen ist.

LEICHTER GESAGT, ALS GETAN

Ganz oben auf Ihrer PCI-DSS-Checkliste steht: Sie brauchen eine Anti-Virus-Lösung. Aber ist es damit auch getan? Schnell erkennen Sie, dass Virenschutz eigentlich das kleinste Problem in der Cloud ist.

Denn damit können Sie raffinierten Cyber-Kriminellen heute nicht mehr die Stirn bieten. Zumal auch bei den besten Schutzmaßnahmen immer ein Restrisiko besteht, dass einmal ein Angriff erfolgreich ist. Mindestens genauso wichtig für die Compliance sind daher eine ganze Reihe von Anforderungen, die im IT-Sicherheitsgesetz etwas schwammig unter Sicherheit „nach Stand der Technik" zusammengefasst werden.

Dazu gehört zum Beispiel:

Sie brauchen ein Patch-Management.

Sie müssen eine Risikobetrachtung durchführen, Schwachstellen erkennen und schließen.

Sie müssen Logfiles auswerten, um verdächtige Vorkommnisse zu erkennen.

Sie müssen in der Lage sein, schnell auf einen Sicherheitsvorfall zu reagieren, um Schaden zu begrenzen und Ihrer Meldepflicht nachzukommen.

WAS JETZT?

„Alles kein Problem“, mag sich der eine oder andere jetzt denken. „Wir suchen uns einfach verschiedene Security-Lösungen, sodass alle Anforderungen abgehakt sind.“ Aber Sie wissen, dass das nicht so einfach ist. Denn wer soll diesen Flickenteppich am Ende noch managen?

Wenn Mitarbeiter zwischen verschiedenen Konsolen hin und her springen und Meldungen an verschiedenen Systemen auswerten müssen, ist das nicht nur zeitaufwändig, sondern auch gefährlich. Im Ernstfall können sie Zusammenhänge nicht richtig erkennen und nicht schnell genug reagieren. Was Sie brauchen, ist eine Lösung, die all Ihre Anforderungen mit einer einzigen Plattform abdeckt und sich über eine zentrale Konsole managen lässt.

Am besten sollte sich die Lösung sogar schon in die DevOps-Pipeline integrieren, damit neue Apps bereits von Grund auf sicher aufgesetzt werden.

Ein automatisierter Security Check prüft den Code während der Entwicklungs- und Bereitstellungsphase und weist auf mögliche Sicherheitskonflikte hin. So können Sie Probleme frühzeitig beheben – oder sich im Einzelfall gezielt entscheiden, überschaubare Risiken einzugehen, um schneller am Markt zu sein.

Ist die App dann online, helfen Techniken wie virtuelles Patch Management und Detection & Response, Risiken zu minimieren.

WIE MACHE ICH DAS AM BESTEN?

Wählen Sie eine Plattform-Lösung eines führenden Herstellers für Cloud Workload Security und lesen Sie dazu die Einschätzung von Analysten wie Forrester und Gartner. Im Idealfall kann die Lösung gleichermaßen On-Premises und als Cloud Service eingesetzt werden.

So gewinnen Sie maximale Security bei maximaler Flexibilität. Lesen Sie weitere Empfehlungen im kostenlosen Whitepaper „Wie die Hybrid Cloud die Spielregeln der Sicherheit verändert“.

DAS BRINGT'S

- Sie entdecken Sicherheitsprobleme schon während der DevOps-Entwicklung, können sie frühzeitig beheben und dadurch Zeit und Kosten sparen.
- Neue Applikationen sind von der Entwicklung bis in die Produktion ganzheitlich abgesichert. In jeder Phase greifen die passenden Security-Mechanismen, ohne dass Sie sich darüber den Kopf zerbrechen müssen.
- Sie decken mit einer Lösung alle Compliance-Anforderungen ab. Ihre Security-Mitarbeiter können alle Sicherheitsfunktionen von einer zentralen Konsole aus managen. Das reduziert Aufwand und spart Zeit.
- In der zentralen Konsole sehen Sie auf einen Blick, wenn etwas Verdächtiges passiert. Sie können sofort reagieren und Schaden minimieren.

DER PARTNER AN IHRER SEITE

Mit Cloud One Workload Security von Trend Micro erhalten Sie Best of Breed-Lösungen vereint aus einer Hand von einem Marktführer. Trend Micro wurde im Forrester Wave™: Cloud Workload Security als Leader genannt (4. Quartal 2019) und zählt laut Gartner zu den drei größten Anbietern von Cloud Workload Protection Platforms.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss."

TREND MICRO™
Securing Your Connected World