| eBook

Präventiver Cloud-Schutz: 5 Wege für eine sichere Migration

Cloud-Sicherheit für den Finanzsektor

Inhalt

Präventive Cloud-Sicherheit für den Finanzsektor

Cloud-Technologien verändern den Finanzsektor. Durch Lösungen für intensivere Kundenbeziehungen, verbesserte Risikomodellierung und agilere Infrastrukturen können sich Banken und andere Finanzdienstleister heute erfolgreich differenzieren und an einen veränderten Markt anpassen. Die Mehrzahl der Unternehmen hat daher bereits mit dem Einsatz von Cloud-Technologien begonnen:

Rund 78 Prozent der deutschen Banken nutzen heute Cloud-Lösungen – ein Anstieg von 25 Prozent im Vergleich zu 2018. Etwas mehr als die Hälfte der Banken, die bislang keine Cloud verwenden, planen absehbar eine Umstellung. Bei 73 Prozent aller Banken ist die Cloud-Nutzung zudem bereits fester Bestandteil der Strategie (Quelle: PwC, Cloud Computing im Bankensektor 2021). Die Wahrung der Sicherheit sensibler Unternehmens- und Kundendaten sowie die Einhaltung der Compliance bleiben dabei die größten Herausforderungen des Cloud Computing in der Finanzbranche.

Von Beginn an sicher

Cloud-Sicherheit ist heute keine separate, nachträglich integrierbare Funktion mehr, sondern lässt sich nur erreichen, wenn umfassender Schutz von Beginn an als integraler Bestandteil aller Cloud-Projekte verstanden wird. Durch eine zentrale Plattform für Sicherheitsservices kann die Cloud-Nutzung in allen Phasen geschützt werden, von der Migration über die Applikationsentwicklung bis zum laufenden Betrieb – und das zentralisiert über die gesamte Hybrid-, Multi-Cloud- und On-Premises-Infrastruktur hinweg.

Wahr oder falsch?

Aus allgemeinen Unternehmensumfragen ergibt sich ein klares Bild des Betriebsalltags nach der Migration: Einrichtung und Wartung von Policies (34 Prozent), Patch- und Schwachstellen-Management (32 Prozent) sowie Fehlkonfigurationen (32 Prozent) haben negative Auswirkungen auf die Cloud Workloads von Unternehmen. Rund 43 Prozent der befragten Unternehmen haben seit der Migration einen höheren Kapitalaufwand und zahlen mehr für die Auslagerung von Services. Außerdem geben 39 Prozent mehr Geld aus für Betrieb und Trainings. Diese Organisationen haben wahrscheinlich den Schritt in die Cloud vollzogen, ohne zu prüfen, was bereits im Vorfeld für den Schutz und die Stabilität der Cloud-Umgebung getan werden muss.

Darüber hinaus hat sich gezeigt, dass sich bei vielen Unternehmen, die noch keine signifikante Migration vollzogen haben, hartnäckige Mythen über die Cloud halten. Dazu gehört zum Beispiel die Annahme, dass eine Cloud-Migration unweigerlich die Compliance mit regulatorischen Auflagen gefährdet oder Regulierungsbehörden zwingend ein On-Premises-Rechenzentrum verlangen. Viele befragte Unternehmen (43 Prozent) glauben auch, dass ein Mangel an Know-how und qualifizierten Fachkräften eine unüberwindliche Hürde für die Cloud-Migration darstellt. Diese falschen Annahmen führen zu einer Zögerlichkeit, die angesichts der Realität moderner Bedrohungen gefährlich werden kann.

Weltweit
130.000
Ransomware-Angriffe
auf den Finanzsektor im ersten HJ 2021

Die Realität der Cyberbedrohungen

Cyberangriffe sind eine sehr reale Bedrohung für Banken und Finanzdienstleister. Zusätzlich zu Malware-Angriffen verzeichneten Trend Micro Sensoren allein im ersten Halbjahr 2021 weltweit rund 130.000 Ransomware-Angriffe auf den Finanzsektor. Das Ziel ist in jedem Fall die Verschlüsselung sensibler Daten und die anschließende Lösegelderpressung. Ein Teil dieser Bedrohungen wird weiterhin durch Mitarbeiter in die Organisation eingeschleppt, zum Beispiel durch einen unbedachten Download oder Austausch infizierter Dateien. In anderen Fällen dringt Malware oder Ransomware über Schwachstellen der Infrastruktur ein. Oftmals geschieht dies in einem vorsichtigen, mehrstufigen Prozess der zusätzlich getarnt werden kann, was die Identifikation immens erschwert.

Diese unterschiedlichen Angriffsmethoden und Techniken erfordern umfassende Sicherheit, die sowohl vor unbedachten Mitarbeiteraktionen wie auch vor komplexen und zielgerichteten Bedrohungen schützt. Angreifer nutzen jede technische Schwachstelle und jede Gelegenheit zum Social Engineering. So wurden zum Beispiel in den letzten Jahren die Angst und Unsicherheit während der COVID-Pandemie sehr erfolgreich ausgenutzt, um Mitarbeiter dazu zu verleiten, dubiose Email-Anhänge zu öffnen, bösartige Dateien herunterzuladen und Informationen im Internet preiszugeben.

Sicherheit muss daher von Beginn an integraler Bestandteil der Cloud-Migration sein, denn nur so lassen sich Cyberbedrohungen sowie operative und regulatorische Herausforderungen gleichermaßen adressieren. Die zentralen Faktoren sind dabei: 1. Sichtbarkeit herstellen, 2. Permanente Kontrolle gewährleisten, 3. Compliance sichern, 4. Performance steigern und 5. Kollaboration und DevSecOps ermöglichen.

1. Das Unsichtbare sichtbar machen

Das Unsichtbare kann nicht kontrolliert werden, deshalb erfordert Cloud-Sicherheit einen ganzheitlichen Ansatz. Voraussetzung dafür ist ein vollständiges Inventar aller Arten von Workloads, Umgebungen, Plattformen und Betriebssysteme, die während der Migration verwendet werden. Eine Sicherheitslösung, die speziell für die Cloud konzipiert wurde, kann mit einer visuellen Timeline alle blinden Flecken beseitigen. So können Bedrohungsmuster erkannt und Risiken für Systeme, Mitarbeiter und Kunden über alle Geräte und Organisationsgruppen hinweg identifiziert werden, um Sicherheitsschwachstellen gezielt zu schließen. Und das ist erst der Anfang.

Informationssilos finden und auflösen

Informationssilos finden sich in allen Organisationen, auch bei Banken und Finanzdienstleistern. Wenn Sie beim Aufbau Ihrer Cloud-Infrastruktur die Sicherheit in den Vordergrund stellen, haben Sie aber die Möglichkeit, diese Silos aufzulösen und den freien Fluss sicherheitsrelevanter Informationen zu gewährleisten, zum Beispiel zwischen IT-Abteilung, Software-Entwicklung und Security Operations Center. Unternehmen sollten daher Sicherheitslösungen in Betracht ziehen, die automatisierte Bestandsaufnahmen und Schutz für alle Public-, Private- und Virtual-Cloud-Umgebungen und die Netzwerkebene bieten. Durch integrierte Integritätsüberwachung, Applikationskontrollen, Log Inspection, fortschrittliche Anti-Malware, Verhaltensanalysen und Machine Learning können Sicherheitslösungen darüber hinaus die Sichtbarkeit von Bedrohungen weiter verbessern und Fehlkonfigurationen vermeiden helfen.

„Mit einem einzigen, zentralen Management für alle Funktionen hat Trend Micro den Sicherheitsbetrieb vereinfacht."

Shiju Rawther
Assistant Vice President of Technology
Credit Information Bureau (India) Ltd.

Verbesserte Sichtbarkeit durch Korrelation

Eine zu große Zahl isolierter Punktlösungen auf den verschiedenen Ebenen der Sicherheitsarchitektur führt zu einer Flut redundanter Alarme, verursacht repetitive Administrationsaufgaben und verhindert einen Gesamtblick auf die Cloud-Landschaft. Stattdessen benötigen Unternehmen eine einzige Cloud-Sicherheitslösung, die automatisch alle verfügbaren Daten zu Vorfällen korreliert und mit externen Bedrohungs- und Schwachstelleninformationen in Beziehung setzt.
Ganzheitliche Sichtbarkeit muss sich dabei auf alle Endpunkte, Email, Server, Cloud Workloads und Netzwerke erstrecken. Deshalb muss die Sicherheitslösung in der Lage sein, all diese Komponenten zu einem Gesamtbild zu verbinden und unternehmensweite Ereignisketten darzustellen. Das ermöglicht Ihnen effektive Nachforschungen und die Einleitung angepasster Reaktionen an einer zentralen Stelle.

2. Permanente Kontrolle gewährleisten

Viele Unternehmen glauben, dass hybride oder On-Premises-Infrastrukturen mit eiserner Faust regiert werden müssen und jede Veränderung am Rechenzentrum automatisch einen Kontrollverlust bedeutet. Andere sind überzeugt, dass ohne On-Premises-Implementierungen schlicht keine Compliance mit DSGVO, PCI DSS etc. möglich ist. Tatsächlich ist das Gegenteil der Fall: Durch eine Cloud-Migration mit entsprechender Sicherheit erhalten Unternehmen mehr Kontrolle, nicht weniger. Schutz und Sichtbarkeit erstrecken sich über die gesamte Umgebung, sodass Bedrohungsakteure effektiv blockiert werden.

„Trend Micro hat uns geholfen, eine robuste Verteidigung aufzubauen, die nicht nur Schwachstellen identifiziert und abschirmt, sondern auch vollständigen Netzwerkschutz bietet.“

Upendra Singh
Director Global IT
Eli Global Financial Services Group

Daten und Applikationen überwachen

Durch die Planung und Umsetzung eines proaktiven Sicherheitsansatzes als Teil der Migration können viele Risiken von Beginn an vermieden werden. Eine Migration, die durch einen proaktiven Plan unterstützt wird, ermöglicht denselben unveränderten Zugriff auf Daten und Applikationen wie zuvor. Sie kontrollieren weiterhin die verwendeten Applikationen und bestimmen, wie auf Daten zugegriffen werden kann – ohne die Compliance zu behindern oder zusätzliches Personal einstellen zu müssen.

Konsistente Umsetzung sicherstellen

Mit einer Sicherheitslösung für Cloud-Implementierungen erzielen Sie im Vergleich zu vorher mehr Kontrolle und Sichtbarkeit für die gesamte Umgebung. Informationssilos werden aufgelöst und sicherheitsrelevante Daten stehen unternehmensweit zur Verfügung. Über eine einzige Lösung erhalten Sie einen umfassenden Überblick zu allem, was geschützt werden muss. Umsetzung und Kontrolle erfolgen konsistent über alle Ihre Clouds hinweg. Sie profitieren von einer Zentralisierung des Managements und der Orchestrierung, automatisierbarem Betrieb, Nahtlosigkeit bei der gemeinsamen Nutzung der Sicherheitskontrollen und Schutz vor lateralen Ausbreitungen.

Patches und Updates

müssen geprüft und verteilt werden, ohne Betrieb oder Compliance zu gefährden.

Virtual Patching für alte und neue Schwachstellen

Die Angriffsoberfläche von Unternehmen verändert sich ständig. Permanent werden neue Schwachstellen und potenzielle Angriffspunkte entdeckt, während oftmals noch nicht alle alten Sicherheitslücken geschlossen werden konnten. Patches und Updates müssen geprüft und verteilt werden, ohne Betrieb oder Compliance zu gefährden. Mit herkömmlichen Mitteln ist es daher kaum möglich, der aktuellen Bedrohungslage einen Schritt voraus zu sein. Eine ganzheitliche Cloud-Sicherheitslösung nutzt hingegen fortschrittliche Techniken wie Machine Learning und Virtual Patching, um Ihre Workloads vor Schwachstellen, Malware und nicht autorisierten Änderungen zu schützen – auch, wenn Sie gar nichts davon mitbekommen. Riskantes Notfall-Patching gehört der Vergangenheit an und selbst Legacy-Betriebssysteme und Applikationen können geschützt werden, obwohl vielleicht kein Hersteller-Patch verfügbar ist.

3. Compliance herstellen und erhalten

Compliance-Konformität ist ein ständiges Thema in der Finanzbranche. Dazu kommen die Sorgen der Kunden um die Sicherheit ihrer Daten und sensiblen Informationen, die durch immer neue Nachrichten zu Datenschutzverletzungen bestärkt werden. In dieser Situation gehen einige Banken und Finanzdienstleister davon aus, dass die Cloud sorgfältig ausgearbeitete Compliance-Pläne destabilisieren könnte. Tatsächlich ist das Gegenteil der Fall: Richtig durchgeführte Cloud-Migrationen haben das Potenzial, die Datensicherheit im Vergleich zu lokalen Rechenzentren zu steigern.

Compliance-Auflagen umfassend adressieren

Spezielle Regulierungen der Finanzaufsicht bilden nur die Spitze des Eisbergs, denn Banken und Finanzdienstleister unterliegen auch einer ganzen Reihe weiterer Datenschutzgesetze und Standards. Wenn die Sicherheit von Beginn an ein integraler Bestandteil aller Cloud-Projekte ist, kann auch die Compliance mit DSGVO (persönliche Daten) und PCI-DSS (Zahlungsverkehr per Kreditkarte) von Grund auf integriert werden. On-Premises Rechenzentren werden für die Einhaltung der Compliance nicht benötigt, die Cloud kann allen Anforderungen gerecht werden.

Konformität automatisieren

Umfassende Cloud-Sicherheit liefert kontinuierliche Gewissheit, dass die Cloud-Umgebung sicher, optimiert und Compliance-konform ist und alle Konfigurationsstandards eingehalten werden. Dies adressiert nicht nur die eigenen Bedenken der Finanzinstitute, sondern auch die Befürchtungen von Kunden, die ihre sensiblen Informationen durch virtuelle Speicherung, Datenfernzugriffe und Cyberangreifer bedroht sehen. Wie bei einem Gesundheitscheck sorgt die Cloud-Sicherheit automatisch dafür, dass die Einhaltung von Standards und Vorschriften durch Applikationen gewährleistet ist. Falls erforderlich, unterstützt sie zudem bei der Schritt-für-Schritt-Behebung von Problemen.

„Trend Micro bietet uns die richtige, proaktive Sicherheit für unsere virtuelle Infrastruktur und minimiert gleichzeitig Auswirkungen auf die System-Performance.“

Mr. Du Xuan Vu
CIO
Orient Commercial Bsnk (OCB)

4. Performance steigern

Finanzunternehmen äußern manchmal die Befürchtung, dass es durch eine Cloud-Migration zu Betriebsstörungen, Ausfallzeiten und verlangsamten Anwendungsreaktionen kommt, die sich negativ auf die Qualität des Kundenservice auswirken könnten. Wieder ist das genaue Gegenteil der Fall.

Geschäftsabläufe beschleunigen

Die richtige Cloud-Sicherheitslösung belastet Sie nicht mit unnötigen Verzögerungen, sondern sorgt dafür, dass Ihr Geschäftsabläufe nach der Migration mindestens so schnell sind wie vorher. Eine hochgradig dynamische Umgebung schützt Workloads und Infrastruktur. Automatisierte, Host-basierte Sicherheit ermöglicht nahtloses Auto-Scaling. Schlanke Agenten liefern spezifische Funktionalitäten für Server und Cloud Workloads. Intrusion Prevention (IPS), virtuelles Patching und eine eingebaute Firewall bieten proaktiven Schutz vor Netzwerkbedrohungen.

„Durch Implementierung der vielseitigen Lösung von Trend Micro haben wir die Sichtbarkeit unserer Umgebung gesteigert und können verdächtige Aktivitäten besser erkennen."

Ayman Al-Shafai
Head of Security Operations Center
The Saudi Investment Bank

Unerwünschte Änderungen erkennen

Mittels Applikationskontrollen, Integritätsüberwachung und Log Inspection informieren Cloud-Sicherheitslösungen über ungeplante Systemänderungen, die sich auf die Performance auswirken könnten. Applikationskontrollen sorgen dafür, dass nur genehmigte Applikationen ausgeführt werden. Log Inspection entdeckt Änderungen an Berechtigungen, Konfigurationen und mehr. Log Inspection alarmiert bei sicherheitsrelevanten Events in Logs. Die Erkennung und Reaktion auf Probleme kann zudem auf Endpunkte ausgedehnt werden, um auch dort Verzögerungen zu vermeiden.

Fintech-Anbieter steigert Wachstum durch Compliance und Transparenz der Cloud

Vindi ist ein brasilianisches Technologieunternehmen, das sich auf Finanzen und Zahlungen konzentriert. Zum umfangreichen Angebot gehören Lösungen für die Verwaltung von Abonnements, die Verarbeitung von Kreditkartentransaktionen, die Integration von Zahlungssystemen und mehr.

Die Erlangung der PCI DSS-Zertifizierung ist kein einfacher oder günstiger Prozess, der für Vindi aber Voraussetzung war. Als Industriestandard für Kreditkartenzahlungen bringt PCI DSS eine Reihe von Verfahrens- und Sicherheitsanforderungen mit sich, deren Einhaltung jedes Jahr geprüft wird.

Da die IT-Sicherheit ein entscheidender Teil der PCI DSS-Zertifizierung ist, suchte Vindi nach einer Lösung, die einerseits die Anforderungen erfüllte und andererseits das schnelle Wachstum des Unternehmens unterstützen konnte. Vindi verfolgt einen fast unbegrenzt skalierbaren „Cloud-first"-Ansatz, sodass entsprechend fortschrittliche Cloud-Sicherheit eingesetzt werden musste.

„Die Sichtbarkeit mit Trend Micro Cloud One™ – Workload Security war entscheidend für unserer PCI DSS-Compliance und ist für unser Management von zentraler Bedeutung."

Teógenes Panella
CISO
Vindi

Trend Micro Cloud One™ – Workload Security liefert nicht nur schnelle Antworten für jedes Problem, sondern entlastet das interne Teams von Vindi auch durch verbesserte Konsolidierung: Sicherheitsrelevante Informationen werden für die gesamte Cloud-Umgebung über ein einziges Dashboard bereitgestellt.

Aufgrund der gemachten Erfahrungen plant Vindi, die Partnerschaft mit Trend Micro auszubauen und weitere Cloud One Services hinzuzufügen, um Transaktionen zu schützen und die Unternehmensentwicklung voranzutreiben.

„Die Cloud ist die Zukunft. Die Entwicklung in der Cloud wird immer schneller und agiler, und die Sicherheit muss mit diesem Tempo Schritt halten."

Teógenes Panella
CISO
Vind

5. Kollaboration und DevSecOps fördern

Cloud-Migrationen sind Projekte des gesamten Unternehmens und öffnen Chancen für positive Veränderungen. Support und Zusammenarbeit sind die Schlüssel für den Erfolg.

Alle Beteiligten einbinden

Eine Cloud-Migration erfordert die Zusammenarbeit fast aller Teams eines Unternehmens. Besonders wichtig ist aber die Kollaboration von IT, IT-Sicherheit und DevOps (DevSecOps). Durch die Bereitstellung von Unterstützung durch DevSecOps wird gewährleistet, dass die Ziele der Cloud-Migration erreicht und gleichzeitig auch die Bedürfnisse der beteiligten Teams adressiert werden.

„Shift Left" umsetzen

DevSecOps erlaubt Sicherheitsteams den „Shift Left" – also die Integration der Sicherheit zu einem frühen Zeitpunkt in der Entwicklungspipeline, noch bevor Workloads in Produktivumgebungen überführt werden. Die enge Zusammenarbeit von Entwicklern und Management ermöglicht die Umsetzung agilerer und DevOps-fokussierter Prozesse. Dazu gehören zum Beispiel Continuous Integration und Continuous Deployment (CI/CD) Pipelines, die Entwicklungszyklen beschleunigen.

API-basierte Sicherheit nutzen

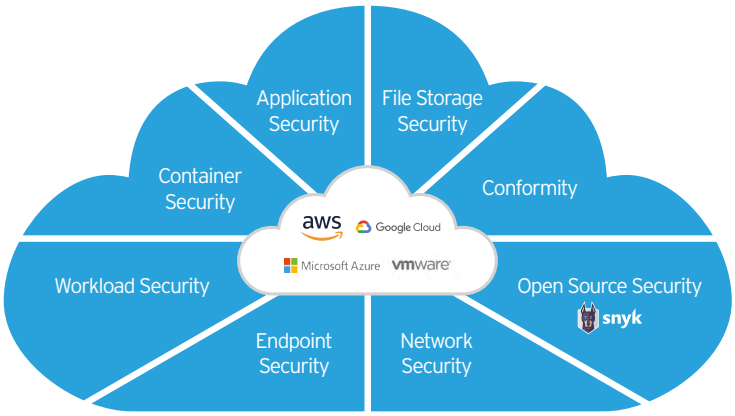
Durch den „Shift Left", der durch API-first-Entwicklung und API-basierte Sicherheit unterstützt wird, können Sicherheitslösungen sowohl Schwachstellen wie auch Malware früher und effizienter erkennen. Das Ergebnis ist eine sichere Cloud-Infrastruktur, die nahtlose Funktionalität für das gesamte Unternehmen bereitstellt.

Zentrale Sicherheit für alle Anforderungen der Cloud-Migration

Trend Micro ist der richtige Partner für alle Banken und Finanzdienstleister, die sich auf dem Weg in die Cloud befinden oder ihre Cloud-Nutzung weiter ausbauen wollen. Unsere zentralisierte Cloud-Sicherheit integriert ein breites Spektrum von Funktionalitäten, reduziert Kosten, steigert die Produktivität und schützt selbst komplexeste Umgebungen.

Trend Micro Cloud One™

Die Trend Micro Cloud One™ Services automatisieren die Identifikation und den Schutz von Private und Public Clouds. Die Trend Micro Cloud One™ Services für Workload Security, Network Security, File Storage Security, Application Security, Container Security, Endpoint Security, Open Source Security und Conformity bieten Ihnen mehr Flexibilität und vereinfachen den Schutz Ihres Unternehmens in allen Phasen der Cloud-Nutzung, von Migration bis Ausbau.



Trend Micro Vision One™

Die Trend Micro Vision One™ Plattform bietet erweiterte Detection & Response (XDR). Auf allen Ebenen der Infrastruktur werden detaillierte Daten gesammelt und miteinander korreliert – über Email, Endpunkte, Server, Cloud Workloads und Netzwerke hinweg. Das ermöglicht hochgradig effiziente Bedrohungserkennung und Nachforschung auf einem Niveau, das mit SIEMs, EDR oder spezialisierten Punktlösungen allein nicht erreicht werden kann.

Sicherheitskontrollen und Integration

Vollständige Sicherheitskontrollen und die nahtlose Integration mit vorhandenen Toolsets für Entwicklung und Betrieb steigern die Sichtbarkeit. Sicherheit wird über die gesamte hybride oder Multi-Cloud-Umgebung hinweg konsistent gewährleistet.

„Wir haben alle am Markt verfügbaren Optionen geprüft. Trend Micro war der einzige Anbieter, der eine ganze Security-Suite in einem virtuellen Paket bereitstellen konnte. Die Trend Micro Cloud One™ Plattform verwendet ein einziges Dashboard, bietet umfassenden Schutz für unsere Cloud-Datenbank und liefert zu jedem Zeitpunkt aktuelle Compliance-Reports. Das machte uns die Entscheidung einfach.“

Chaitanya Pinnamaneni
Chief Technology Officer
Sandstone Technology (Banken-IT-Dienstleister)

Entdecken Sie führende Cloud-Sicherheit für Ihre IT-Umgebung

Ist Ihre Cloud-Infrastruktur sicher und Compliance-konform? Trend Micro bietet einen kostenlosen, automatisierten Checkup Ihrer Cloud-Infrastruktur in Bezug auf Sicherheit, Governance und Compliance. In einem virtuellen Meeting mit unseren Cloud Engineers erhalten Sie eine persönliche Bewertung Ihrer individuellen Cloud-Risiken und -Schwachstellen sowie Empfehlungen zur Problembehebung. Neben Einblicken durch informative Reports und Dashboards erhalten Sie darüber hinaus Zugang zu einem kostenfreien Test von Trend Micro Cloud One™ - Conformity.

Wichtiger Hinweis: Während des Checkups erhalten wir keinen Zugriff auf Ihre sensiblen Unternehmensdaten.

Alle Details finden Sie hier ›