splunk> turn data into doing™

CASE STUDY

Imprivata verwaltet und schützt containerisierte Umgebungen mit Splunk Cloud

Zentrale Herausforderungen

Zur Entlastung des DevOps-Teams benötigte Imprivata sichere, zentrale Logging- und Ad-hoc-Abfragefunktionen in seinen hochgradig verteilten, containerisierten Produktions- und Entwicklungsumgebungen.

Wichtige Ergebnisse

Durch den Wechsel zu Splunk® Cloud konnte Imprivata die Kosten für die Wartung der lokalen Infrastruktur senken, die Sicherheits-Compliance optimieren und die DevOps-Mitarbeiter entlasten, sodass ihnen mehr Zeit für wertschöpfendere Aufgaben bleibt.

imprivata®

Branche: Gesundheitswesen

Lösungen: IT Operations, Security

Sichere digitale Identitäten sind heute wichtiger denn je.

Imprivata ist ein Unternehmen für IT-Sicherheitslösungen im Gesundheitswesen und bietet in dieser Branche agierenden Unternehmen weltweit eine Sicherheits- und Identitätsplattform mit ortsunabhängigem Zugriff, Identitätsmanagement und Multifaktor-Authentifizierung. Imprivata schützt das Gesundheitswesen, indem es Vertrauen zwischen Menschen, Technologien und Informationen schafft, um kritische Compliance- und Sicherheitsanforderungen zu bewältigen sowie die Produktivität und Patientenerfahrung zu verbessern.

Daten werden zu Geschäftsergebnissen

- NOC-Mitarbeiter meistern dank Automatisierung und Runbooks 100 % der Produktions-Incidents ohne Eskalation an DevOps
- Einfachere Compliance mit HIPAA, SOC 2 Type II und DSGVO
- Wegfall der Kosten für die lokale Infrastruktur und weniger Verwaltungsaufwand

Einblicke in die gesamte Cloud-Umgebung

Imprivatas DevOps- und Entwicklungsteams arbeiten bei der Wartung der Tooling- und Automatisierungsinfrastruktur des Unternehmens zusammen und setzen dabei auf Best Practices, um auch bei Spitzenbelastung maximale Leistung sicherzustellen. Dabei verlassen sich die Teams schon lange auf Splunk Enterprise, wenn es um Benachrichtigungen, die Erstellung von Dashboards, das Reporting zu Service Level Agreements und das Troubleshooting geht.

„Glücklicherweise arbeiten wir schon immer mit Splunk. Unsere Systemlogs, Amazon Web Services, Firewall- und Sicherheitslogs werden alle in Splunk eingespeist“, sagt ein Manager im Cloud Plattform-Team von Imprivata.

Splunk ist für die Transparenz und Stabilität von Imprivatas operativer Umgebung von großer Bedeutung, in der sowohl Docker- und Kubernetes-Containerisierung als auch Python-Automatisierungsteuerung für das Monitoring von in Amazon Web Services bereitgestellten Ressourcen eingesetzt wird. Imprivata-Entwickler nutzen Docker auf ihren Laptops und anstatt Logs lokal zu speichern, übertragen sie diese an Splunk Cloud, damit sie leichter analysiert werden können.

„Unsere hochgradig verteilte, Cloud-basierte Architektur umfasst viele Services und Container – das sind viele verschiedene Einzelteile. Sie könnten sich eine Logdatei ansehen, aber Sie wüssten nie, mit welcher Sie anfangen müssten. Ohne Splunk hätten wir keine Informationen, was gerade vor sich geht“, erklärt der Manager.

„Bei Imprivata sammeln wir sämtliche Logs für Cloud-Infrastruktur, Anwendungen und lokale Installationen an einem zentralen Ort, sodass das Troubleshooting der Anwendung, der Infrastruktur und des Cloud-Systems ebenfalls zentral erfolgt: und zwar in Splunk“. „Splunk-Dashboards helfen dem Produktmanagement-Team und den Engineering-Managern, Service Level Agreements festzulegen und von Anfang an zu messen – so wird mit dem Beginn der Datenaufnahme für Messbarkeit und ein gemeinsames Produktverständnis gesorgt.“

Kosteneffiziente Skalierbarkeit dank Splunk Cloud

Skalierungsbedarf und der Plan des Unternehmens, lokale Lösungen in die Cloud zu verlagern, waren der Auslöser für Imprivatas Migration von Splunk Enterprise zu Splunk Cloud. In der Regel schleust das Unternehmen pro Tag etwa 150 GB an Daten durch Splunk, in Ausnahmen sogar bis zu 500 GB. Splunk Cloud ermöglicht Imprivata, wichtige Erkenntnisse aus Maschinendaten zu gewinnen, ohne eine Infrastruktur verwalten zu müssen. „Splunk Cloud senkt die Betriebskosten unserer Infrastruktur und gibt unseren IT-Fachleuten gleichzeitig mehr Zeit für wertschöpfendere Aufgaben", sagt der Manager.

> Dank Splunk Cloud kann ich meinen Schwerpunkt von administrativen Aufgaben auf die Unterstützung meines Teams und anderer Personen im gesamten Unternehmen verlagern, geschäftliche und Kernursachenanalysen durchführen und konkrete Ergebnisse anvisieren."
>
> **Manager,** Cloud Platform Team, Imprivata

Optimierung von Compliance und Auditing

Mit Splunk Cloud wird auch die Compliance mit HIPAA (Health Insurance Portability and Accountability Act) und weiteren gesetzlichen Vorgaben (darunter SOC 2 Typ II und die DSGVO) zum Kinderspiel. Imprivata kann Maschinendaten aus beliebigen Quellen – einschließlich elektronischer Patientenakten (EPA) und vernetzter medizinischer Geräte – sicher analysieren, visualisieren und überwachen, um komplexe Anwendungsumgebungen zu monitoren und Audit-Funktionen zu optimieren. Der Splunk Cloud-Vertrag des Unternehmens beinhaltet ein Business Associate Agreement (BAA, Geschäftspartnervereinbarung), sodass persönliche Gesundheitsdaten (PHI) durch HIPAA-Richtlinien geschützt sind.

> Wir verwenden eine HIPAA-konforme Version von Splunk, die eine Geschäfts-partnervereinbarung beinhaltet, die für unsere Zusammenarbeit mit Anbietern sehr vorteilhaft und wichtig ist. Wenn ein Report nicht mehr läuft oder der Scheduler langsamer wird, müssen nicht mehr wir herausfinden, warum, sondern die Experten bei Splunk."
>
> **Manager,** Cloud Platform Team, Imprivata

„Als Sicherheitsunternehmen im Gesundheitswesen arbeiten wir auf einem viel höheren Sicherheitsniveau. Deswegen verwenden wir Splunk. Hier haben wir ein BAA, das definiert, wann ein Verstoß vorliegt, und die Verantwortlichkeiten festlegt", erklärt der Manager. „Für uns ist das eine Grundvoraussetzung für die Zusammenarbeit mit Anbietern."

Höhere Leistung, größerer Business Value

Nach Schätzungen des Managers interagieren etwa 100 Imprivata-Mitarbeiter in irgendeiner Weise mit Splunk Cloud; darunter ca. 25 Entwicklungsingenieure, die Cloud-Anwendungen erstellen, und etwa 10 „Splunk-Ninjas", die die anspruchsvollsten Suchen in Minuten- oder Sekundenschnelle ausführen. Imprivata verzeichnete kürzlich den ersten Monat, in dem die Mitarbeiter der Ebenen 1 und 2 des rund um die Uhr verfügbaren Network Operations Center (NOC) dank Automatisierung und Runbooks 100 Prozent aller Produktions-Incidents ohne Eskalation an DevOps meisterten. Dabei wurde die Mean-Time-to-Repair (MTTR) erheblich verbessert und Auswirkungen auf den Service wurden durch eine proaktive Problembehebung verhindert.

Durch diese Effizienz – und durch Outsourcing des Infrastrukturmanagements und der administrativen Aufgaben in die Splunk Cloud – haben die hochqualifizierten Ingenieure von Imprivata nun Zeit, Aufgaben nachzugehen, die das Unternehmen wirklich voranbringen. Sie können ihre wertvolle Zeit für das Troubleshooting, die Arbeit mit Leistungsmetriken und Kernursachenanalysen nutzen.

„Wenn mir jemand eine Frage stellt, kann ich ihm zeigen, wie er Splunk Cloud optimal einsetzt, um aussagekräftige Erkenntnisse zu gewinnen", erklärt der Manager. „Wir verwalten Splunk nicht nur, sondern nutzen es, um in unseren Daten nach versteckten Schätzen zu suchen."

20-15395-Tier2-Imprivata-A4-101-CS