

servicenow®

TANIUM



**Verbesserung der Visibilität
und Senkung des Risikos
mit Tanium ITX und Security
Operations für ServiceNow**

Nahtlose Visibilität, Behebung und Automatisierung mit
einem einheitlichen Plattformansatz von ServiceNow und Tanium

Inhaltsverzeichnis

- 03 Vertrauen Ihre IT-, Sicherheits- und Risikoteams den Daten in Ihrer CMDB?
- 04 Eine einheitliche Plattform für verbesserte Visibilität, Kontrolle und Behebung
- 05 Eine vollständige, genaue und aktuelle CMDB mit Tanium ITX für ServiceNow
- 06 Vollständige Echtzeit-Visibilität von Tanium ITX
- 07 Identifizieren, korrelieren und priorisieren Sie das Risiko von Endpunktschwachstellen und Compliance-Lücken mit Tanium Security Operations für ServiceNow
- 08 Jede Sekunde zählt
- 09 Kundengeschichte: Globales Transportunternehmen
- 10 Kundengeschichte: Große Bundesbehörde
- 11 Kundengeschichte: Cognizant
- 12 Kundengeschichte: Lebensmittel- und Einzelhandelsunternehmen
- 13 Schlussfolgerung

Vertrauen Ihre IT-, Sicherheits- und Risikoteams den Daten in Ihrer CMDB?

Ein moderner Endpunkt-Management-Lebenszyklus hängt von drei kritischen Elementen ab: Visibilität, Kontrolle und Behebung.

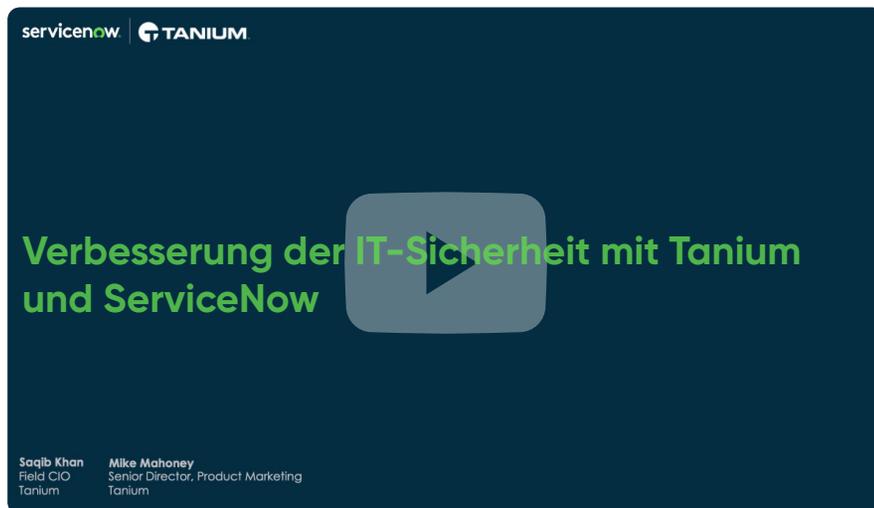
Sie müssen jeden Endpunkt in jedem Netzwerk überall sehen können. Wenn Sie ihn nicht sehen können, können Sie ihn nicht warten oder schützen.

Sie benötigen auch Echtzeitkontrolle, damit Sie sofort Maßnahmen ergreifen und die Ergebnisse einsehen können, wenn Sie Zwischenfälle untersuchen oder Änderungen vornehmen.

Wenn es darauf ankommt, müssen Sie in der Lage sein, in großem Umfang und in Echtzeit zu reagieren, um Risiken zu stoppen, bevor sie echten Schaden anrichten.

Die meisten IT-, Sicherheits- und Risikomanager streben zwar nach dieser ganzheitlichen Vereinheitlichung, werden jedoch durch nicht miteinander verbundene Lösungen – **55 % der IT- und SecOps-Organisationen verwenden 20 oder mehr Lösungen** – und einen inhärenten Mangel an Vertrauen in die Daten der CMDB behindert. Die daraus resultierenden manuellen Prozesse tragen zu einer Eskalation von Risiken, Kosten und Zeitplänen sowie zum Zusammenbruch der Automatisierung bei, wodurch proaktive Sicherheit immer schwieriger – wenn nicht gar unmöglich – wird.

Es ist an der Zeit, Ihre Abläufe mit einer integrierten Plattformlösung zu vereinheitlichen, die Ihre Visibilitäts-, Kontroll- und Behebungsmöglichkeiten transformieren und eine einzige Echtzeit-Informationsquelle für IT, Sicherheit und Risiko schaffen kann.



Die Videos in diesem E-Book enthalten Einblicke aus einem Podcast-Interview von ServiceNow Global Partner Marketing mit Saqib Khan, dem CIO von Tanium Field, der die ServiceNow-Partnerschaft leitet. Sehen Sie sich das vollständige Interview auf Abruf an, um mehr über den integrierten Plattformansatz von ServiceNow und Tanium zu erfahren.



Die Hauptelemente eines modernen Endpunkt-Management-Lebenszyklus



werden behindert durch



mehrere getrennte Lösungen, die zu Folgendem beitragen:



manuelle Prozesse, reaktive Reaktion und



erhöhte Kosten und Risiken

Eine einheitliche Plattform für verbesserte Visibilität, Kontrolle und Behebung

ServiceNow und Tanium arbeiten besser zusammen, um einen einheitlichen Ansatz für das Verständnis und die Verwaltung Ihres IT-Bestands mit verbesserter Geschwindigkeit, höherer Effizienz und reduziertem Risiko zu bieten.

Wie? Stellen Sie sich Tanium als die Augen und Hände Ihrer Operation und ServiceNow als das Gehirn vor.



AUGEN: Tanium sieht alle Endpunkte und erfasst Echtzeitdaten aus Hardware, Software und virtuellen Assets über alle Netzwerke hinweg



GEHIRN: ServiceNow nutzt Daten aus der CMDB, um Arbeitsabläufe, Aufgaben und Behebungsmaßnahmen zu koordinieren und die teamübergreifende Zusammenarbeit von einer einzigen Informationsquelle aus zu ermöglichen.



HÄNDE: Tanium ergreift Maßnahmen an Endpunkten, von Softwareverteilungen bis hin zur Host-Isolierung und zum Schwachstellen-Patching

Tanium bietet Visibilität und Rechenschaftspflicht für die Arbeitsabläufe und Funktionen von Geschäftsprozessen, die für ServiceNow von zentraler Bedeutung sind. Das Ergebnis? Bessere Visibilität, Kontrolle und Behebung – im großen Maßstab.



Visibilität

Optimieren Sie Software und Hardware sowie Cloud-Nutzung, Performance und Kosten mit Echtzeitvisibilität und CMDB-Daten, denen Sie vertrauen können.



Kontrolle

Korrelieren Sie Konfigurationselemente automatisch mit der Echtzeit-Compliance der Schwachstellenkonfiguration und den Bewertungen der Änderungsautorisierung.



Behebung

Ergreifen Sie Maßnahmen in großem Maßstab mit automatisierter, intelligenter Priorisierung, Behebung und Auditierung, die an Service-Desk- und Änderungsmanagementprozesse gebunden sind.

Eine vollständige, genaue und aktuelle CMDB mit Tanium ITX für ServiceNow

Mit Tanium ITX für ServiceNow erhalten Sie beispiellosen Zugriff auf Endpunktdaten in Echtzeit und bieten umfassende Einblicke in all Ihre Hardware, Software und virtuellen Assets. Diese fortschrittliche gemeinsame Lösung stellt sicher, dass Sie Ihre gesamte IT-Infrastruktur unabhängig vom Umfang Ihres Betriebs effizient verwalten und überwachen können. Dies ermöglicht Organisationen Folgendes:

- **Zugriff auf aktuelle Endpunktdaten** auf allen Geräten, online oder offline, über jedes Netzwerk
- **Verbesserung in Hinblick auf SLAs für mittlere Untersuchungszeit (MTTI) und mittlere Behebungszeit (MTTR)**
- **Kosten senken und Risiken mindern** durch ungenutzte, nicht ausgelastete Assets oder nicht konforme Software
- **Verbessern der Endbenutzer-Softwareanforderungen** mit Self-Service-Softwareverteilungen
- **Automatisieren der Patching-Verteilungen, die an Change-Management-Prozesse gebunden sind**, um die IT-Umgebung proaktiv zu sichern

servicenow | **TANIUM**

Ihre CMDB ist die Grundlage für bessere Ergebnisse

Saqib Khan
Field CIO
Tanium

Mike Mahoney
Senior Director, Product Marketing
Tanium

Der aktuelle Zustand:

94 % der Unternehmen können mindestens 20 % ihrer netzwerkverbundenen Assets nicht sehen.

70 % der IT-Teams haben nicht genug Vertrauen in die Visibilität von mehr als 85 % ihrer Endpunkte.

Organisationen, die Tanium und ServiceNow implementieren, melden verbesserte Ergebnisse:

94 % der IT-Entscheidungsträger entdeckten Endpunkte, die sie vor Tanium nicht kannten.¹

93 % der Tanium-Kunden berichten von einer Reduzierung der wöchentlichen Scanzzeiten ihrer Hardware, Software und virtuellen Assets.²



¹ <https://www.tanium.com/partners/servicenow/spotlight/>

² <https://www.tanium.com/partners/servicenow/spotlight/>

Vollständige Echtzeit-Visibilität von Tanium ITX für ServiceNow

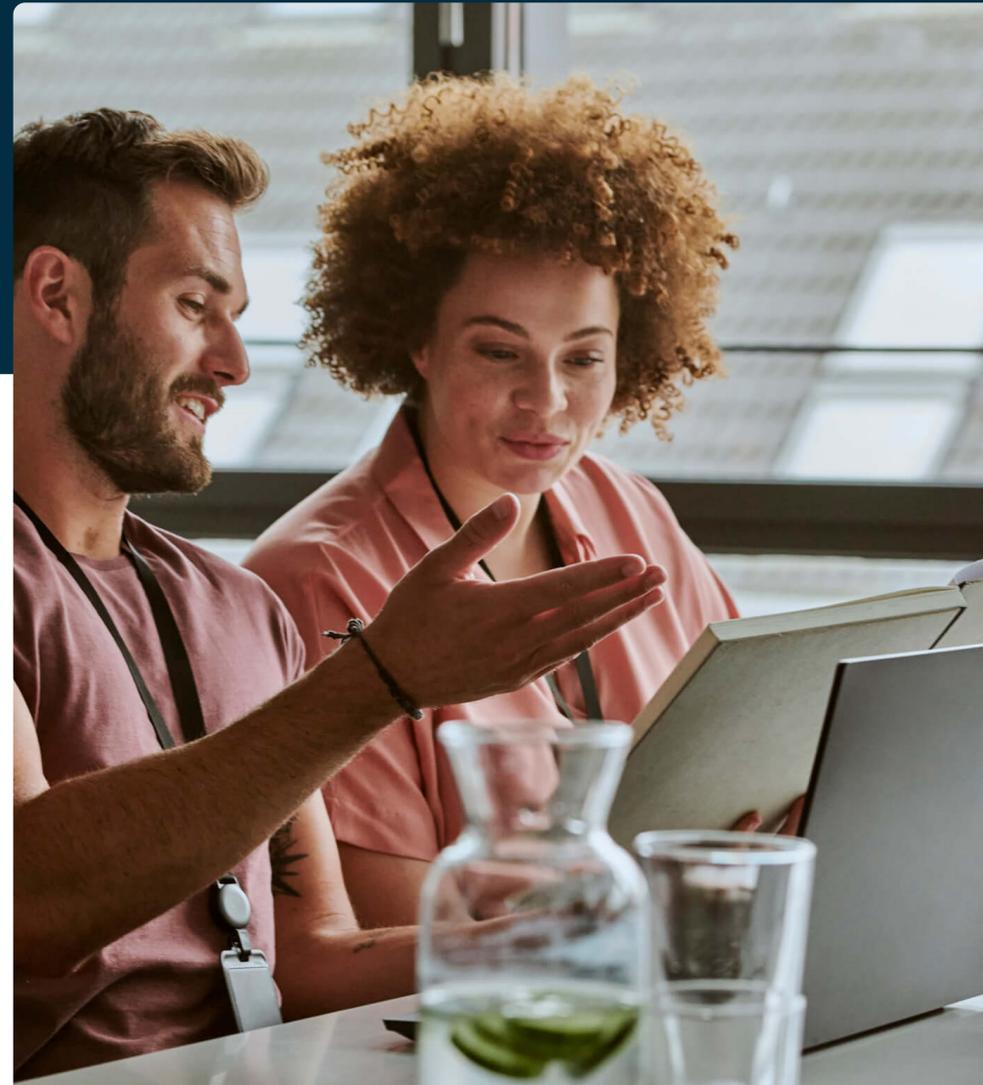
Alles beginnt mit einer vollständigen, genauen und aktuellen CMDB.

Die CMDB ist das Herzstück von ServiceNow und entscheidend für effektive Arbeitsabläufe und Entscheidungsfindung in Ihrer gesamten IT-Organisation. Dennoch haben viele Organisationen Schwierigkeiten mit der Wartung einer vollständigen, aktuellen und vertrauenswürdigen CMDB.

Das Erkennungs- und das Converged Endpoint Management von Tanium ITX erfasst Echtzeitdaten über alle Endpunkte und Netzwerke hinweg und leitet diese Daten konsistent direkt in die ServiceNow CMDB ein. Dies ermöglicht einen ganzheitlichen Überblick über Ihr Hardware-, Software- und virtuelles Asset-Inventar und Ihre Nutzung.

ServiceNow verarbeitet die Daten und Warnmeldungen von Tanium, um die Automatisierung von Arbeitsabläufen, die Priorisierung, die Berichterstattung und die Zusammenarbeit voranzutreiben – und ermöglicht es gleichzeitig jedem Team, von einer einzigen Informationsquelle aus zu arbeiten.

Beide Plattformen können gemeinsam Maßnahmen im gesamten IT-Bereich ergreifen und dabei Ihre Änderungskontrollen und Reaktionsrichtlinien mit einem vollständigen Auditverlauf verfolgen.



Tanium ITX für ServiceNow



Identifizieren

Tanium sieht alle Endpunkte und erfasst Echtzeitdaten und Risiken aus Hardware, Software und virtuellen Assets über alle Netzwerke hinweg, um die ServiceNow-CMDB zu aktualisieren und Warnungen auszulösen.



Priorisieren

ServiceNow verarbeitet die Warnungen, ruft aktuelle Daten aus der CMDB ab und priorisiert automatisch für die Behebung, während Arbeitsabläufe, Zuweisungen, Aktionen und teamübergreifende Zusammenarbeit mit intelligenter Validierung koordiniert werden.



Beheben

ServiceNow weist Tanium an, Maßnahmen auf Endpunkten, Servern und netzwerkgebundenen Geräten zu ergreifen. Dazu gehören Aufgaben wie Softwareverteilungen, Host-Isolierung, Schwachstellen-Patching und Aufzeichnungsaktionen zur Auditkontrolle.

Erfahren Sie mehr

Entdecken Sie, wie Tanium und ServiceNow Ihrer Organisation helfen können, Cybergefahren zu reduzieren und die Kontrolle zu erhöhen.

Tanium Security Operations für ServiceNow

Identifizieren, Korrelieren und Priorisieren des Risikos von Endpunktschwachstellen und Compliance-Lücken in Echtzeit.

Die Aufrechterhaltung der Cyber-Resilienz und des Schwachstellenmanagements bei gleichzeitiger schnellerer Reaktion auf Sicherheitszwischenfälle wird jeden Tag schwieriger. Die Erweiterung der physischen und virtuellen Infrastruktur und die Verbreitung von Software und Endbenutzergeräten machen es immer schwieriger, Schwachstellen und Risikoexpositionen zu identifizieren, zu korrelieren und zu priorisieren.

Tanium Security Operations für ServiceNow vereint IT-, Sicherheits- und Risikoteams für eine verbesserte Zusammenarbeit und Geschwindigkeit im großen Maßstab. So funktioniert es:

- 1 **Echtzeitdaten zu Schwachstellen, Compliance und Sicherheitseignissen** werden erfasst und in ServiceNow eingespeist, um zusätzliche Plattform-Intelligence-Augmentation zu ermöglichen.
- 2 **ServiceNow korreliert Risikodaten mit Konfigurationselementen in der CMDB und** ermöglicht eine automatisierte Priorisierung basierend auf allen Datenpunkten – nicht nur einem einzigen Tool.
- 3 Wenn es um die Behebung von Risiken geht, **kann ServiceNow Tanium intelligent anweisen, Maßnahmen im großen Maßstab zu ergreifen** – unabhängig davon, ob es sich um das Patching von Schwachstellen oder die Automatisierung der Reaktion auf Sicherheitszwischenfälle handelt.

Vorhersage, Erkennung und kontinuierliche Überwachung

Herausforderungen für Organisationen:

43 %

der Risikomanager haben im letzten Jahr mehr als 3 kritische Risikoereignisse erlebt, [so Forrester](#)

600 Mrd. USD

Die Kosten aufgrund von Cyberkriminalität pro Jahr weltweit, [gemäß Mordor Intelligence](#)

33 %

der gesamten Kosten für Datenschutzverletzungen sind auf entgangene Geschäfte zurückzuführen, [so das Poniman Institute](#)



Jede Sekunde zählt

Zero-Days und erweiterte Malware sind nicht die größten Bedrohungen für Ihre Organisation. Tatsächlich werden die meisten Vorfälle durch bekannte Schwachstellen oder Fehlkonfigurationen ausgenutzt, und die überwiegende Mehrheit der Angriffe hätte durch bekannte Patches oder ordnungsgemäße Konfigurationen verhindert werden können. Aufgrund ineffizienter Tools und isolierter Teams haben viele Organisationen jedoch Probleme mit einer effizienten Patch-Verwaltung und koordinierten Verteidigungsmaßnahmen, wodurch sie potenziellen Bedrohungen ausgesetzt sind.

Durch die Präsentation von Zwischenfalldaten auf eine Weise, die sowohl sinnvoll als auch umsetzbar ist, können Organisationen die Komplexität reduzieren, eine größere Kontrolle gewinnen, die Audit- und Berechtigungs-Compliance sicherstellen und die betriebliche Resilienz erhöhen.

WICHTIGE ERGEBNISSE ENTHALTEN:



Identifizierung und Korrelierung von proaktiven Endpunktschwachstellen und Konfigurationslücken mit ServiceNow-CMDB-Konfigurationselementen



Automatisierung von Patching, um Schwachstellenrisiken durch geplante Änderungsmanagementprozesse zu eliminieren



Eliminierung der Risikoexposition und Vorbereitung auf Audits



Identifizierung und Warnung bei unbefugten Änderungen an Dateien und Registries, bevor ein Zwischenfall zu einem Problem wird



Bereicherung von Sicherheitszwischenfällen mit Echtzeit-Intelligence, um Reaktions- und Behebungszeiten erheblich zu reduzieren



Minimierung der Auswirkungen und Kosten von Vorfällen

Integrationen, die Tanium Security Operations für ServiceNow umfassen, sind:

- ✓ Integration der Schwachstellenreaktion
- ✓ Integration von Konfigurations-Compliance
- ✓ Integration von Sicherheitsoperationen
- ✓ Patch-Orchestrierung für Schwachstellenreaktion
- ✓ Dateiintegrität und Überwachung nicht autorisierter Änderungen

Entdecken Sie, wie Tanium und ServiceNow Ihrer Organisation helfen können, Cybergefahren zu reduzieren und die Kontrolle zu erhöhen.

[Erfahren Sie mehr](#)



KUNDENGESCHICHTE

Globales Transportunternehmen

Eines der weltweit größten und angesehensten Unternehmen in den Bereichen Transport, E-Commerce und Business Services benötigte eine Lösung, um seine Hardware- und Software-Assets zu erkennen und zu verwalten und gleichzeitig die Größe und den Umfang seiner Operationen zu unterstützen.

Die bestehenden Prozesse erforderten mehrere punktuelle Lösungen und es fehlte an Datentreue und Visibilität, die erforderlich sind, um nicht nur das operationelle, sondern auch das regulatorische Risiko aufgrund der Nichteinhaltung finanzieller Anforderungen zu reduzieren. Die Synchronisierung von CMDB-Daten dauerte Tage oder Wochen und die Audit-Compliance erforderte erhebliche manuelle Prozesse.



“ Es ist eine Sache zu sagen, dass man X-, Y- und Z-Anwendungsfälle hat und bestimmte Ergebnisse erzielt, aber **wenn man tatsächlich einen greifbaren ROI sieht, der von Produkten von ServiceNow von Tanium in Echtzeit bereitgestellt wird**, dann sieht man den [Wert] sofort.

Saqib Khan
Field CIO
Tanium

→ Die Lösung:

Jetzt nutzt die Organisation ServiceNow IT Asset Management und Tanium Converged Endpoint Management, die ihr vollständige, genaue und Echtzeit-Visibilität in ihre Hardware- und Software-Assets in ihrer ServiceNow CMDB bieten.

Durch die Nutzung von ServiceNow Software Asset Management Professional ist die Organisation auch strategisch in der Lage, die IT-Prozesse mithilfe digitaler Arbeitsabläufe und Analysen zu automatisieren und das Softwarelizenzrisiko zu mindern.

→ Ergebnisse:



Konsolidierung von Systemen und punktuellen Lösungen mit Einsparungen von 3 Mio. USD bei der Toolverlagerung

60 %

reduzierte Gemeinkosten in ServiceNow

500.000 USD

Erwartete Einsparungen von 500.000 USD bei den Bußgeldern für das Audit des Software-Asset-Managements

27,3 Mio. USD

Lizenzkosten für nicht ausgelastete Software entdeckt



Erhöhtes Vertrauen und Effizienz im IT Asset Management (ITAM)

KUNDENGESCHICHTE

Große Bundesbehörde

Eine unvollständige CMDB führte bei einer großen Bundesbehörde zu Problemen bei der Einhaltung der Vorschriften für Cloud Data Management(CDM)-Software und Hardware. Man benötigte alle 72 Stunden Übersichtsseiten-Updates, eine Aufgabe, die in Altsystemen unmöglich war. Durch die Verwendung mehrerer punktueller Lösungen, darunter Qualys, Tenable und Splunk, nahmen die Datenkomplexität und die Kosten der Behörde aufgrund sich überschneidender Tools stetig zu.



→ Die Lösung:

Durch die Nutzung der Tanium IT Asset Management(ITAM)-Integration reduzierte diese Agentur sofort die Kosten nach einer Implementierung, die nur drei Wochen dauerte. Mit der Asset-Integration, die Echtzeit- und vollständige Software- und Hardwaredaten in ihre CDM-Übersichtsseite einfügte, konnte die Agentur ihre täglichen Compliance-Anforderungen vollständig automatisieren. Darüber hinaus reduzierte die Eliminierung doppelter und nicht ausgelasteter punktueller Lösungen die Komplexität und die Kosten des Unternehmens erheblich.

→ Ergebnisse:



Erfüllte die regulatorischen CDM-Anforderungen vollständig mit automatisierten, täglichen Updates

~2 Mio. USD

Nahezu 2 Mio. USD Einsparungen durch Lizenzreduzierungen und Tool-Konsolidierung

90 %+

Über 90 % Automatisierung manueller Compliance-Prozesse

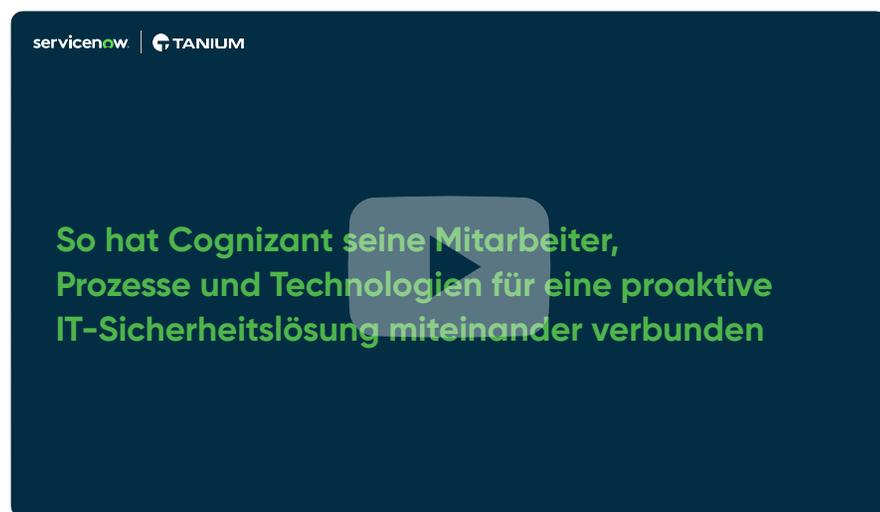
92 %

Durch die Nutzung der sofort einsatzbereiten Integration von Tanium in ServiceNow wurde die Konformität für Hardware-, Software- und Schwachstellenanforderungen von null auf 92 % gesteigert

KUNDENGESCHICHTE



Seit 2019 hat Cognizant, ein Anbieter von professionellen Dienstleistungen, zu denen digitale Dienste, Beratung und Anwendungsentwicklung gehören, mehr als 3 Milliarden USD für Akquisitionen ausgegeben. Dieses aggressive Wachstum ging mit einem erhöhten Risiko in Form von erworbenen IT-Architekturen, Endpunkt-Management-Tools und Sicherheitsprotokollen einher, die alle so gesichert und verwaltet werden mussten, als gäbe es sie schon immer – und zwar schnell.



“ [Seit Tanium und ServiceNow] gibt es eine einheitliche Agenda. Ehrlich gesagt, verbringen wir nicht viel Zeit damit, über „IT“ und „Sicherheit“ zu reden – wir arbeiten als Einheit. **Die Teams arbeiten nahtlos zusammen.** ”

Tim Dwyer
 Head of Global Infrastructure, Engineering, and Operations
 Cognizant

→ Die Lösung:

Durch die Integration von ServiceNow ITAM und Tanium Converged Endpoint Management konnte Cognizant die Aktualisierung seiner CMDB von Tagen auf knapp drei Stunden beschleunigen und so für vollständige Visibilität und Vertrauen in dieser schnell wachsenden Organisation sorgen.

Durch die Nutzung von ServiceNow Software Asset Management Professional ist die Organisation auch strategisch in der Lage, die IT-Prozesse mithilfe digitaler Arbeitsabläufe und Analysen zu automatisieren und das Softwarelizenzrisiko zu mindern.

→ Ergebnisse:



Tägliche ServiceNow-CMDB-Aktualisierung sämtlicher Hardware und Software



Konsolidierung und Reduzierung der Gemeinkosten, die bei der ServiceNow-Wartung erforderlich sind



Vollständige Hardware- und Software-Erkennung für alle Netzwerke und Endpunkte



Deutlich reduzierte Kosten für Softwarelizenzen durch Rückgewinnung nicht ausreichend genutzter Software



Mehr ITAM-Vertrauen und -Effizienz

KUNDENGESCHICHTE

Lebensmittel- und Einzelhandelsunternehmen

Im Unternehmenszentrum von Arizona stand ein führender Lebensmitteleinzelhändler mit 35.000 Mitarbeitern und einem Jahresumsatz von 6 Milliarden USD an einem digitalen Scheideweg. Es wollte eine einzige Quelle der Wahrheit in einer Echtzeit-basierten und genauen CMDB etablieren, die Zeit für die Verteilung von Patches und die Validierung von Behebungserfolgen verkürzen und präzise Audit-Berichte für PCI-Anforderungen liefern – und das alles unter Einhaltung der strengen Branchenstandards des Center for Internet Security (CIS), des National Institute of Standards and Technology (NIST) und des Cybersecurity Framework (CSF).

Die operative Landschaft war jedoch komplex. Der Einzelhändler betreibt Geschäfte in 23 Bundesstaaten in einem Umfeld, das aufgrund der Abhängigkeit von mehreren Einzellösungen mit manuellen, segmentierten Prozessen behaftet war. Diese Unordnung führte zu fehlenden Patch-Vereinbarungen und einer ineffektiven CMDB, die von veralteten, doppelten Daten geplagt wurde. Das Asset-Management für Hardware und Software war auf reine Vermutungen reduziert worden.



→ Die Lösung:

Heute profitiert der Einzelhändler dank der automatischen Patch-Orchestrierung und Schwachstellenreaktion von Tanium von einer einheitlichen Konsole, die eine präzise Erfassung und Behebung von Schwachstellen sowie eine nahtlose Integration in das Orchestrierungssystem von ServiceNow ermöglicht.

→ Ergebnisse:



Echtzeit-basierte und vollständige CMDB

150.000 USD

Einsparungen jährlich



Automatisierte Patches und Behebungen



Fähigkeit, Audit-Zeitpläne einzuhalten und konform zu bleiben

servicenow®

TANIUM



servicenow | TANIUM

Gründe, die für Tanium für ServiceNow sprechen

Saqib Khan
Field CIO
Tanium

Mike Mahoney
Senior Director, Product Marketing
Tanium

Erhalten Sie den maximalen Wert schneller

Verschaffen Sie sich vollständige Visibilität über alle Ihre Assets und stärken Sie Ihre Sicherheit durch nahtlose IT-Abläufe und Sicherheitsarbeitsabläufe – und das alles, während Sie eine stabilere, intelligenteren CMDB aufbauen, die für die zukünftige Wertschöpfung gerüstet ist.

Erfahren Sie mehr

Über ServiceNow

ServiceNow (NYSE: NOW) macht die Welt für alle besser. Unsere cloudbasierte Plattform und unsere Lösungen helfen Organisationen bei der Digitalisierung und Vereinheitlichung, damit sie intelligentere, schnellere und bessere Wege finden, um Arbeitsabläufe zu optimieren. So können Mitarbeiter und Kunden besser vernetzt, innovativer und agiler sein. Und wir können alle die Zukunft gestalten, die wir uns vorstellen. The world works with ServiceNow™. Weitere Informationen finden Sie unter: www.servicenow.com.

Über Tanium

Tanium, der einzige Anbieter der Branche für Converged Endpoint Management (XEM), führt den Paradigmenwechsel bei veralteten Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an. Nur Tanium schützt jedes Team, jeden Endpunkt und jeden Arbeitsablauf vor Cyberbedrohungen, indem es IT, Compliance, Sicherheit und Risiko in einer einzigen Plattform integriert, die umfassende Visibilität über alle Geräte hinweg, einen einheitlichen Satz von Kontrollen und eine gemeinsame Taxonomie für einen einzigen gemeinsamen Zweck bietet: den Schutz kritischer Informationen und Infrastrukturen in großem Maßstab. Besuchen Sie uns unter www.tanium.com.