TANIUM

Zurück zu den Basics: Cyber-Hygiene beginnt mit dem Asset-Management

Ein neuer Ansatz zu Asset-Discovery und -Inventory, zur Verbesserung der Cyber-Hygiene und ein erster Schritt auf dem Weg zu Zero Trust.

Zurück zu den Basics: Cyber-Hygiene beginnt mit dem Asset-Management

Ein neuer Ansatz zu Asset-Discovery und -Inventory, zur Verbesserung der Cyber-Hygiene und ein erster Schritt auf dem Weg zu Zero Trust.

Inhalt

Die Herausforderung der Asset-Visibilität in modernen Netzwerken

Ihre Herausforderung: die Verwaltung von Millionen dynamischer, dezentral verteilter und vielfältiger Assets.

Aufgrund global verteilter Belegschaften und verborgener Assets, deren Anzahl exponentiell ansteigt, sind die Beibehaltung eines vollständigen und genauen Inventars aller IT-Assets sowie eine skalierte Visibilität in Echtzeit schwieriger als jemals zuvor. Schließlich müssen wir wissen, wie viele Türen und Fenster es gibt und wo sie sich befinden, damit wir diese Türen und Fenster verschlossen halten können.

Und dennoch konnte die Branche keine praktikable Lösung für das Problem mit der Visibilität liefern und bietet Hub-and-Spoke-Modelle als langsame und durchweichte Netzwerke an, die stattdessen die Visibilität in modernen und komplexen Umgebungen einschränken.

Es ist also kein Wunder, dass viele Unternehmen wesentliche Details über ihre Umgebung nicht genau melden können.

Zur Lösung dieses Problems heißt es also, zurück zu den Basics zu gehen.

Um die Cyber-Hygiene aufrechtzuerhalten und zu verbessern, müssen Sie zunächst wissen, welche IT-Assets Sie haben. Nutzen Sie 50.000, 100.000 oder 500.000 Computer und Server in Ihrer Organisation? Wo befinden sich diese? Was sind sie? Was wird auf ihnen ausgeführt? Welche Dienstleistungen bieten sie an?

Bei der Beantwortung dieser Fragen geht es um die Entwicklung der Asset-Visibilität – und um die Befolgung eines **Asset-Discovery und -Inventory-Prozesses**. Das ist die Grundlage für die Schaffung und Aufrechterhaltung von Cyber-Hygiene. Und wir haben dieses E-Book geschrieben, um Ihnen beim Erreichen der nötigen Visibilität zu helfen.

In diesem E-Book beschäftigen wir uns mit Folgendem:

- Warum Asset-Visibilität für eine Aufrechterhaltung der Cyber-Hygiene notwendig ist
- Wie Sie in modernen Netzwerken für Asset-Visibilität sorgen
- Welche Tools Sie benötigen, um diese Ergebnisse zu erzielen

Warum die Cyber-Hygiene von Asset-Visibilität abhängt

Die Verwaltung ist nicht möglich, falls Ihnen die Assets nicht bekannt sind.

Um Ihre Endpunkte zu verwalten, benötigen Sie Wissen und Informationen auf drei Ebenen:

1. Welche Assets haben Sie und wo befinden sich diese?
2. Welche Software wird darauf ausgeführt und ist sie lizenziert? Sie benötigen mehr als einen Hostnamen oder eine IP-Adresse.
3. Wie stehen die Maschinen in Ihrem Netzwerk in Beziehung und was ist ihr Zweck? In Serverumgebungen können Sie beispielsweise eine Gruppe von Servern haben, die ausschließlich einen Dienst hosten, wie z. B. eine Unternehmenswebsite.

Alle Unternehmen, unabhängig von ihrer Größe, benötigen diese Informationen, die sich in der modernen IT zudem auch ständig ändern. Netzwerk-Assets kommen und gehen, insbesondere bei in vielen Unternehmen mittlerweile gängigen und zunehmend verbreiteten BYOD-Richtlinien („Bring Your Own Device“). Einige Assets tauchen dabei nur gelegentlich im Netzwerk auf. Da immer mehr Unternehmen die Mitarbeiter dazu ermutigen, von zu Hause aus zu arbeiten (WFH = „Work from Home“), steigt die Komplexität.

Und da die Netzwerke immer komplexer werden und sich schneller verändern, wird es immer schwieriger, die Visibilität beizubehalten – und die Konsequenzen, wenn der genaue Überblick über die Assets und deren Aktionen fehlt, werden immer größer.

Die Nachteile der Unwissenheit für den operativen Betrieb

Um es mit den Worten des ehemaligen Eagle Don Henley zu formulieren: „Wenn Sie mit geschlossenen Augen fahren, werden Sie bestimmt mit etwas zusammenstoßen.“ Wenn Sie nicht wissen, welche Assets sich in Ihrem Netzwerk befinden, entspricht das für Ihre IT einer Fahrt mit geschlossenen Augen.

Eines der ersten Dinge, auf die Sie wahrscheinlich „stoßen“ werden, sind Sicherheitslücken. Wenn Sie ein Asset nicht verwalten können, können Sie es nicht schützen. Und die Verwaltung ist nicht möglich, wenn Ihnen die Assets erst gar nicht bekannt sind. Sie wissen dann einfach nicht, ob die Software richtig gepatcht ist. Es kann also Angriffsvektoren geben, die Ihnen gar nicht bewusst sind.

Wie sieht es mit den finanziellen Auswirkungen aus? Haben Sie allgemein ein Gefühl dafür, wofür Sie Ihr Geld ausgeben? Zum Beispiel für Softwarelizenzen von gängigen Produktivitätsprogrammen wie Microsoft Office. Wenn Sie eine Lizenz für 10.000 Kopien haben, verwenden Sie 20.000 oder nur 5.000 davon? Nutzen Sie die Lizenz, für die Sie bezahlen, effizient? Oder sind Sie nicht compliant und Ihnen drohen unter Umständen teure rechtliche Schritte?

Darüber hinaus geht es bei Compliance nicht nur um Softwarelizenzen. Es ist ein weiterer Betriebsbereich, der sehr stark von dem Wissen abhängt, welche Assets sich in Ihrem Netzwerk befinden.

Nehmen wir das Gesundheitswesen als Anwendungsfall. Gesundheitsorganisationen müssen die Einhaltung der DSGVO- und PCI-Bestimmungen nachweisen, die geschützte Gesundheits- und Kreditkartendaten abdecken. Wissen Sie, wo diese Daten gespeichert werden? Ist das nicht der Fall, lässt sich die Compliance nicht nachweisen. Wenn die Compliance nicht nachgewiesen werden kann, bringt das zwei erhebliche Nachteile: regulatorische Sanktionen und kein effektives Erbringen Ihrer Dienstleistungen.

Die Beispiele dafür sind schier endlos. Wenn Sie nicht wissen, welche Assets sich in Ihrem Netzwerk befinden und welche Aktionen sie ausführen, können Sie sie nicht schützen, Sie können sie nicht verwalten und Sie können in Ihrer gesamten Umgebung keine effektive Cyber-Hygiene erreichen.

Und – leider – haben viele Unternehmen derzeit Schwierigkeiten, grundlegende Fragen zu den Assets in ihrer Umgebung zu beantworten. Hier sind die Gründe dafür.

Warum Unternehmen Schwierigkeiten haben, Asset-Visibilität zu schaffen

Es gibt zwei Hauptgründe, weshalb Unternehmen Schwierigkeiten dabei haben, grundlegende Fragen zu ihren Assets zur Aufrechterhaltung der Cyber-Hygiene zu beantworten.

Erstens bewegt sich die Endpunkterkennung als Zielsetzung ständig weiter.

Nicht jeder Endpunkt in einem Netzwerk ist ein Desktop-Computer, Laptop oder Server. Dazu gesellen sich Drucker, Telefone, Tablets und eine wachsende Anzahl von IoT-Geräten (Internet of Things). Mobile Device Management (MDM) ist ein wachsendes Anwendungsfeld.

Aber warum sollten Sie sich Sorgen darum machen müssen, dass ein IoT-Endgerät das Unternehmensnetzwerk beeinträchtigt? Hier sind die Gründe dafür: Eine Mitarbeiterin von einem unserer Kunden arbeitete von zu Hause aus. Das Sicherheitsteam des Unternehmens erhielt Warnmeldungen, dass jemand versuchte, in ihren Laptop einzubrechen. Die Quelle war ein Kühlschrank mit Malware, die das Heimnetzwerk scannte und in das Gerät eindringen wollte, das sich vorübergehend im Unternehmensnetzwerk befand. Dasselbe kann bei einem intelligenten Lichtschalter, Thermostat, einer Sicherheitskamera – oder was auch immer passieren.

Dies gilt auch für Maschinen im Fertigungsbereich, von denen viele mit Sensoren ausgestattet sind, die über drahtlose Netzwerke und das Internet mit Fertigungsanwendungen kommunizieren.

Dieses Feld mit der Bezeichnung „operative Technologie“ macht im Wesentlichen aus jeder Maschine in einer Fabrikhalle ein Netzwerkgerät.

Jeder Gerätetyp kann Betriebs- und/oder Sicherheitsrisiken bergen, und die Anzahl dieser Typen wird in den kommenden Jahren nur noch weiter zunehmen.

Zweitens haben ältere Tools Schwierigkeiten, in dieser neuen Umgebung Visibilität zu schaffen.

Tools zur Asset-Erkennung, die vor 10 Jahren entwickelt wurden, griffen vielen Aspekten voraus, mit denen moderne IT-Umgebungen heute täglich arbeiten. Zwei Beispiele: Container und Hybrid Clouds.

Diese Tools können die Geschwindigkeit der Veränderungen, die wir jetzt sehen, nicht bewältigen. Dennoch halten viele Unternehmen an vertrauten Tools fest, auch wenn viele davon nicht einfach zu bedienen sind.

Vielleicht sind sie sogar stolz darauf, mit schwer zu bedienenden Tools zurecht zu kommen. Sie haben möglicherweise benutzerdefinierte Skripte verfasst, damit sie effektiver arbeiten können. Nicht nur das: Ein ganzes Partner-Ökosystem hat sich darum entwickelt, IT-Abteilungen genau bei diesen Aufgaben zu unterstützen.

Die unbeabsichtigten – und bedauerlichen – Folgen davon sind IT-Richtlinien und -Prozesse, die nicht deshalb entwickelt wurden, weil sie die beste Möglichkeit zur Problemlösung bieten, sondern weil sie den Fähigkeiten der verwendeten Tools entsprechen. Das ist praktisch die IT-Version der Weisheit „wenn man einen Hammer hat, muss alles ein Nagel sein“. Die Richtlinien sind: „Es muss genagelt werden.“ Festgefahrene Tools werden Teil des IT-Ökosystems. Aber die besten IT-Richtlinien sollten nicht vom Tool abhängen. Ein Tool, das 1993 – oder 2010 – entwickelt wurde, kann diese Flexibilität nicht bieten.

Das Ergebnis dieser beiden Probleme

Wenn Unternehmen versuchen, mithilfe älterer Tools Asset-Visibilität in modernen Umgebungen zu schaffen, wird ihr Asset-Discovery- und -Inventory-Prozess:

- **Komplex:** Sie müssen immer mehr Tools hinzufügen, nur um ihre Assets zu identifizieren, und jedes dieser Tools muss in die anderen integriert werden.
- **Teuer:** Sie zahlen für teure Software – und die Support-Teams bzw. -Infrastruktur, die niemand verwendet, ist wahrscheinlich veraltet und verbraucht Ressourcen.
- **Veraltet:** Sie produzieren unvollständige Daten, die oft Tage, Wochen oder sogar Monate zu spät vorliegen und nicht den aktuellen Zustand des Netzwerks widerspiegeln.

Zusammenfassung: Organisationen brauchen eine neue Möglichkeit, um Asset-Visibilität in modernen Netzwerken aufzubauen.

Wie Sie in modernen Netzwerken für Asset-Visibilität sorgen

Überdenken Sie Ihre alten Tools zur Asset-Visibilität

Zunächst müssen Sie entscheiden, ob Ihre alten Tools für die Asset-Visibilität Ihnen noch zu Diensten stehen. Wenn Sie Schwierigkeiten haben, Visibilität in Ihrem gesamten Bestand zu schaffen, müssen Sie möglicherweise die Nutzung eines oder mehrere Ihrer bisherigen Tools einstellen und diese durch moderne Optionen ersetzen.

Welche Funktionen sind für ein modernes Toolset für die Asset-Verwaltung wichtig?

Die Tools oder Plattformen, die Sie für Asset-Discovery und -Inventory verwenden, sollten über folgende Eigenschaften verfügen:

- Genauigkeit
- Geschwindigkeit
- Skalierbarkeit
- Benutzerfreundlichkeit

Genauigkeit, Geschwindigkeit und Skalierung sind eng miteinander verbunden. Wenn es zwei Wochen oder einen Monat dauert, bis Sie fertig sind, hat sich in der Zwischenzeit das Netzwerk verändert und Sie haben zweifellos etwas verpasst.

Das Ergebnis ist nicht mehr zutreffend, egal wie sorgfältig Sie waren. Je größer das Netzwerk ist, desto stärker wird das zum Problem. Deshalb ist die Skalierung von Bedeutung. Benutzerfreundlichkeit kommt ebenfalls ins Spiel, da ein schwer zu konfigurierendes Tool Fehler verursacht und die Anwender es mit der Zeit nicht mehr verwenden möchten.

Zum Schaffen effektiver Asset-Visibilität und Vorantreiben eines modernen Asset-Discovery- und -Inventory-Prozesses müssen Ihre Tools diese vier Eigenschaften vereinen.

Streben Sie nach den richtigen Ergebnissen in Hinblick auf die Asset-Visibilität

Zweitens müssen Sie die richtigen Ergebnisse für Ihre Funktionen zur Asset-Visibilität anvisieren. „Asset-Visibilität“ kann ein breites Thema sein, man verliert sich leicht beim Versuch, zu viele Ergebnisse auf einmal zu erreichen. Konzentrieren Sie sich zunächst auf die Visibilität für einige wichtige Ergebnisse.

Welche Ergebnisse sind für eine moderne Asset-Visibilität wichtig?

Sie sollten die erforderliche Asset-Visibilität entwickeln für:

1. **Einblicke in die Endpunkte, derer Sie sich nicht bewusst sind, um das Risiko zu reduzieren.** Nicht sichtbare Endpunkte lassen sich nicht verwalten. Die vielfältige, dynamische und dezentral verteilte Infrastruktur von heute schafft eine komplexe Umgebung, in der sich Endpunkte leicht verstecken können und sich ständig ändern, wodurch die Sicherheitsrisiken steigen. Sie sollten folgende Fähigkeiten besitzen:
   - Entdeckung aller Endpunkte in Ihrer Umgebung innerhalb von Minuten – nicht Tagen oder Wochen – einschließlich schwer zu findender Endpunkte in entfernten Subnetzen.
   - Nachverfolgung eines Echtzeit-Bestands, in dem kontinuierlich neue Assets entdeckt und kategorisiert werden und es Ihnen möglich ist, diese zu verwalten.
   - Verschaffen eines Überblicks der Abhängigkeiten von Anwendungsdiensten und des aktuellen Status Ihrer Assets in Echtzeit, einschließlich des letzten bekannten Status von Offline-Assets.
2. **Wertsteigerung Ihrer CMDB mit genauen Echtzeitdaten.** Die meisten älteren Tools können nur eine einzige Frage für eine einzelne Asset-Klasse beantworten, was Unternehmen zum Einsatz Dutzender komplexer, individueller Produkte zwingt. Die IT-Teams versuchen dann, die von diesen Punktlösungen bereitgestellten Daten in ihre CMDB zu integrieren, zu zentralisieren und zu normalisieren. Die Folge davon sind ungenaue und unzureichende Asset-Daten. Eine bessere Vorgehensweise wäre:
   - Die Verbindung mit Ihrer CMDB unter der Gewissheit, dass Endpunkt- und Nutzungsdaten aktuell und zutreffend sind.
   - Der regelmäßige Export Ihrer Asset-Daten nach einem Zeitplan in die CMDB, basierend auf den Anforderungen für eine konsistente Berichterstattung, bessere Zusammenarbeit und fundierte Entscheidungsfindung.
   - Schaffung einer Single Source of Truth, die von Sicherheits-, Betriebs-, Risiko-, Beschaffungs-, Finanz- und Führungsteams verwendet wird.
3. **Vermeiden Sie unnötige Hard- und Softwarekosten.** Unternehmen können heute nur schwer erkennen, welche Software auf den Rechnern installiert ist und wie stark sie verwendet wird. Sie können ihre Software weder für Audits noch für Wiederverwendungszwecke genau bewerten. Das führt zu hohen Softwareausgaben – sowohl bei den Audit-Gebühren als auch bei den wiederkehrenden Lizenzkosten. Sie sollten diese Fähigkeiten besitzen:
   - Eine vollständige Liste der Software nach Produkt oder Anbieter in Ihrer Umgebung muss jederzeit verfügbar sein.
   - Nicht autorisierte oder nicht ausgelastete Software muss auffindbar sein, um Lizenzen zurückzufordern oder neu zu verteilen.
   - Sofort einsatzbereites Reporting ist zu verwenden, um Nutzungsstatistiken auf einen Blick zu verstehen.

Halten Sie mit dem vierstufigen Zyklus der Asset-Visibilität die Cyber-Hygiene aufrecht

Als Nächstes sollten Sie erkennen, dass die Schaffung von Asset-Visibilität und Cyber-Hygiene kein einmaliges Projekt ist. Ihre Umgebung verändert sich ständig und erfordert für ein klares Bild und grundlegende Sicherheit im jetzigen Zustand einen kontinuierlichen Prozess.

Viele unserer Kunden nutzen den folgenden Prozess, um für eine effektive Visibilität und Cyber-Hygiene ihrer Assets zu sorgen:

SCHRITT 1

Sorgen Sie für Visibilität, indem Sie die gesamte Umgebung zunächst einmal umfassend scannen.

SCHRITT 2

Finden Sie Probleme, indem Sie unbekannte, nicht verwaltete und anfällige Assets in der Umgebung aufdecken.

SCHRITT 3

Schützen Sie Ihre Geräte und andere Endpunkte, indem Sie Schwachstellen schließen und unbekannte und nicht verwaltete Endpunkte so gut wie möglich kontrollieren.

SCHRITT 4

Etablieren Sie eine kontinuierliche Asset-Überwachung; wiederholen Sie diesen Zyklus, wenn neue Assets hinzukommen und sich der Status bekannter Assets ändert.

Denken Sie über die Cyber-Hygiene hinaus und legen Sie die Grundlage für Zero Trust

Schließlich sollte Cyber-Hygiene nur der erste Schritt zu einer höheren Sicherheit in Ihrer Organisation sein. Die richtige Fähigkeit zur Asset-Visibilität bildet auch die Grundlage für nahezu jede Zero-Trust-Strategie oder -Lösung, die Sie umsetzen möchten.

Wenn alle Geräte Netzwerkgeräte sind, gehen von allen diesen Geräten potenzielle Schwachstellen für die Sicherheit aus. Daher benötigen Sie Richtlinien und Verfahren, die Endpunkte in drei Kategorien unterteilen: verwaltet, nicht verwaltet und keine Verwaltung möglich.

Endpunkt-Discovery ist der erste entscheidende Schritt für den Trend hin zu Zero-Trust-Lösungen. CSO Online beschreibt Zero Trust[1] als „ein Sicherheitskonzept, das sich auf die Überzeugung konzentriert, dass Unternehmen nicht automatisch Ressourcen *innerhalb* oder *außerhalb* der Schutzzone Ihres Netzwerks vertrauen sollten und stattdessen alles überprüfen müssen, das den Versuch einer Verbindung mit den Systemen startet, bevor Zugriff gewährt wird."

Tools für Threat Response und die Behebung von Bedrohungen sind nur so gut wie die Breite der Endpunkte, auf denen sie ausgeführt werden. Und da der Endpunkt die Zone des Netzwerks erweitert, beginnt Cyber-Hygiene und -Sicherheit tatsächlich mit der Endpunkt-Discovery, und die Implementierung einer Zero-Trust-Praxis ist der nächste sinnvolle Schritt auf diesem Weg.

[1] https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Wie Tanium Asset-Visibilität schafft und Cyber-Hygiene fördert

Was ist Tanium?: Asset-Visibilität für moderne Umgebungen

Tanium ist eine konvergente Plattform, die in modernen Umgebungen Visibilität und Kontrolle über vielfältige, dynamische und dezentral verteilte Assets bietet.

Die *Asset-Discovery und -Inventory*-Lösung von Tanium stellt ein umfassendes, zuverlässiges und umsetzbares Bild Ihrer Endpunktumgebung dar. Die Technologie untersucht effizient Bereiche des Netzwerks, in denen gängige Endpunkt-Tools möglicherweise nicht wissen, wie oder wo sie nach „versteckten" Geräten suchen – einschließlich Endpunkten, die über herkömmliche Methoden nicht ordnungsgemäß berichten.

Tanium bietet auch zusätzliche kontextbezogene Details zu jedem Endpunkt – einschließlich Hardwarekonfigurationen, installierter Software und Details zur Nutzung dieser Software über 30-, 60- und 90-Tage-Intervalle.

Mit Tanium können Sie fundamentale Fragen über Ihre IT-Umgebung mit genauen, kompletten und aktuellen Daten über all Ihre Endpunkte innerhalb von Sekunden beantworten, nicht erst in Stunden, Tagen oder Wochen.

Mit Tanium haben viele unserer Kunden:

- Die wöchentliche Scandauer um 93 % reduziert.
- 35 % mehr Endpunkte entdeckt, als ihnen bisher bekannt waren
- 20 % mehr nicht verwaltete Assets erkannt, als ihnen bewusst war

Und so geht's.

Vorteile von Tanium: Visibilität, Geschwindigkeit und Wahrheit

Tanium korrigiert die Probleme mit älteren Tools und nutzt eine moderne Architektur, die für Asset-Visibilität in modernen Netzwerken entwickelt wurde. Tanium nutzt:

- **Ein erweiterbares Datenmodell**, mit dem Sie nach Belieben neue Ad-hoc-Daten von Ihren Endpunkten erfassen können.
- **Ein verteiltes Kommunikationsprotokoll**, das Daten innerhalb von Sekunden an Millionen von Endpunkten ohne intermediäre Infrastruktur erfasst und verteilt.
- **Ein einzelner, leichter Agent** mit minimalen Auswirkungen auf die Endpunktleistung, der auf die kleinsten Chips passt.

Dieser grundlegend andere Ansatz von Tanium bietet Ihnen:

- **Geschwindigkeit.** Sie können jeden Endpunkt in Ihrer Umgebung erkennen und in wenigen Minuten einen umfassenden Bestand erstellen. Sie generieren Echtzeit-Visibilität für Tausende, vielleicht Hunderttausende von Assets, stellen grundlegende Fragen und erhalten Antworten in Sekundenschnelle und integrieren diese Echtzeitdaten in Tools von Drittanbietern wie CMDBs und SIEMs.
- **Visibilität.** Sie werden Ihre gesamte Umgebung in wenigen Minuten kategorisieren und sehen, wie Ihre Hardware, Software und Infrastruktur-Assets verwendet werden. Sie erstellen eine vollständige Liste der Assets in Ihrer Umgebung, entdecken nicht verwaltete Assets, bringen diese unter Kontrolle und erfahren, wie Sie Ihren Bestand optimieren können.
- **Wahrheit.** Sie stellen Ihre IT-Assets zentral und vertrauenswürdig dar und vereinheitlichen Ihre IT-Betriebs-, Sicherheits- und Risikoteams mit einem genauen Datensatz. Sie erstellen eine einzige Quelle der Wahrheit (Single Source of Truth) und ein System zur genauen Aufzeichnung aller Ihrer Assets und können zuversichtlich Entscheidungen treffen, die sich auf mehrere Teams auswirken.

Neun Möglichkeiten, wie Tanium die Asset-Entdeckung und -Inventarisierung verbessert

Keine davon ist nur Theorie. Tanium kann Ihren Asset-Discovery- und -Inventory-Prozess sinnvoll verbessern und Ihnen greifbare Ergebnisse liefern. Mit Tanium können Sie:

1. Unbekannte Endpunkte auffinden. 10–20 Prozent mehr Endpunkte in Ihrer Umgebung identifizieren, als Ihnen derzeit bekannt sind. Was Sie nicht sehen können, können Sie auch nicht sichern.
2. Endpunktdaten kontinuierlich erfassen. Entwickeln Sie eine einzige Quelle der Wahrheit (Single Source of Truth), die ein aktuelles und zuverlässiges Bild Ihrer gesamten Umgebung vermittelt.
3. Verlorene Assets katalogisieren. Führen Sie überall und jederzeit genau Bestand über Remote-Assets und verstehen Sie zugleich den Status dieser Assets.
4. Erhöhen Sie den Prozentsatz der verwalteten Endpunkte. Reduzieren Sie Risiken, indem Sie eine größere Anzahl Ihrer Endpunkte mithilfe flexibler Erkennung und Automatisierung sichern und verwalten.
5. Die mittlere Verwaltungszeit senken. Identifizieren Sie schnell neue Endpunkte, die in Ihre Umgebung gelangen, und bringen Sie sie unter Ihre Kontrolle.
6. Verfolgen Sie die Softwarenutzung und die Abdeckung in Prozent nach. Verfolgen Sie die Nutzung und den Prozentsatz der nicht verwendeten installierten Software auf jedem Ihrer Endpunkte nach.
7. Weisen Sie Ressourcen neu zu. Hören Sie auf, 90 Prozent Ihrer Zeit mit der Datenerfassung zu verbringen, und nutzen Sie diese Daten stattdessen für Ihre Arbeit in der Praxis.
8. Ihre Investitionen optimieren. Analysieren Sie Nutzungsdaten über Hardware- und Software-Assets hinweg, um Ihre Ausgaben zu rationalisieren und durch robuste Integrationen zusätzlichen Wert aus bestehenden Lösungen zu ziehen.
9. Das Risiko und Ineffizienz mindern. Zentralisieren Sie Visibilität und Kontrolle für verwaltete und nicht verwaltete Assets. Steigern Sie die Konsistenz und eliminieren Sie Variabilität und das Rätselraten.

Verbessern Sie die Asset-Visibilität und die Cyber-Hygiene – ab heute

Der Unterschied ist klar. Mit herkömmlichen Tools erfassen Sie veraltete, ungenaue und unvollständige Daten aus Ihren Assets und können die Cyber-Hygiene nur schwer aufrechterhalten. Mit Tanium erfassen Sie aktuelle, genaue und umfassende Daten aus jedem Asset in Ihrer Umgebung und sorgen für eine zuverlässige Cyber-Hygiene.

Erfahren Sie mehr über die **Asset-Discovery and -Inventory-Lösung von Tanium** und kontaktieren Sie uns, um **eine Demo und Beratung zu vereinbaren.**

Tanium ist die Plattform, der Unternehmen vertrauen, wenn sie Visibilität und Kontrolle für alle Endpunkte in lokalen, Cloud- und hybriden Umgebungen erzielen möchten. Unser Ansatz bietet eine Lösung für die wachsenden Herausforderungen der heutigen IT. Durch die Bereitstellung präziser, vollständiger und aktueller Endpunktdaten erhalten Teams für IT-Betrieb, -Sicherheit und -Risiko die Möglichkeit, ihre Netzwerke schnell zu verwalten, zu sichern und zu schützen. Tanium verfolgt die Mission, Organisationen dabei zu helfen, jeden Endpunkt zu erfassen und zu kontrollieren. Das ist die Power of Certainty.

Besuchen Sie uns unter www.tanium.com und folgen Sie uns auf LinkedIn und Twitter.