TANIUM

Die Ungewissheit beenden:

Best Practices für das Melden von Risiken

Experten bieten Informationen und Empfehlungen zur Meldung von Risiken in den schnelllebigen und stark verstreuten Unternehmensumgebungen von heute.

TANIUM

Die Ungewissheit beenden: Best Practices für das Melden von Risiken

Experten bieten Informationen und Empfehlungen zur Meldung von Risiken in den schnelllebigen und stark verstreuten Unternehmensumgebungen von heute

Inhalt

Expertentipps zur Risikomessung

Das Risikomanagement ist eine der wichtigsten Aufgaben eines jeden Führungsteams, das strategische Ziele erreichen will. Allerdings können Führungskräfte nur die Risiken managen, die sie kennen. Wie sich herausstellt, hängt eine wirksame Führung von Risikoberichterstattung, Risikobewusstsein und Kommunikation ab.

In diesem eBook geht es um die Meldung von Risiken an die Geschäftsleitung und den Vorstand Ihres Unternehmens, damit diese die richtigen Entscheidungen zur Risikominderung treffen können, was Ihr Unternehmen bei der Erreichung seiner strategischen Ziele unterstützt.

Wenn Sie noch nicht mit der Durchführung von Risikobewertungen vertraut sind, empfehlen wir Ihnen, **unser eBook zur Risikomessung zu lesen,** um mehr über die Befragung von Fachleuten und die Berechnung der Risikowahrscheinlichkeit zu erfahren, die in Risikoberichte einfließen.

In diesem E-Book liegt unser Schwerpunkt auf der Risikoberichterstattung selbst. Das bedeutet, die richtigen Informationen für das Führungsteam Ihres Unternehmens zu finden und sie so weiterzugeben, dass effektiv darauf reagiert werden kann.

Am Ende dieses eBooks finden Sie eine Checkliste, die die Ratschläge zusammenfasst.

KAPITEL 1:

Melden von Risiken, die für die Unternehmensführung von Bedeutung sind

Risiko hat für viele Menschen eine ganz unterschiedliche Bedeutung. Wenn Sie mit IT-Fachleuten über Risiken sprechen, werden Sie wahrscheinlich von der Gefahr von Serverausfällen, Datenverletzungen oder Schwachstellen in der Software hören, die zu Datenschutzverletzungen führen könnten.

Vielleicht hören Sie auch von nicht autorisierten Geräten, Bring-Your-Own-Device (BYOD)-Richtlinien und davon, wie schwierig es ist, den Umgang der Mitarbeiter mit den Unternehmensdaten in ihren Heimnetzwerken zu überwachen, da sie nun aus der Ferne arbeiten.

All diese Dinge – von Serverausfällen bis hin zu externen Mitarbeitern – stellen Risiken der einen oder anderen Art dar. Wenn Sie jedoch für die Risikoberichterstattung an die Geschäftsleitung und den Vorstand Ihres Unternehmens zuständig sind, beabsichtigen Sie dann wirklich, ihnen eine Liste der ungepatchten Systeme oder eine Schätzung der Anzahl an Mitarbeitern vorzulegen, die BYOD-Geräte verwenden?

Welche Risiken sind dem Führungsteam Ihres Unternehmens letztendlich wichtig?

Um diese Frage zu beantworten, müssen wir über die Risiken selbst nachdenken. Glücklicherweise gibt es eine allgemein vereinbarte Risikodefinition, zumindest unter IT-Experten. ISO 31000, die Leitlinien der Internationalen Organisation für Normung für das Risikomanagement, definiert Risiko als „die Auswirkung von Ungewissheit auf bestimmte Ziele“.

„Ungewissheit“ scheint einfach genug zu sein. Wenn etwas sicher ist, besteht kein Risiko. Wenn wir genau wissen, dass unsere Server niemals ausfallen werden, besteht auch kein Risiko, dass sie ausfallen.

Aber wie sieht es mit „Zielen“ aus? Jeder Mitarbeiter, jedes Team, jede Abteilung und jedes Unternehmen hat Ziele. Wenn Sie dem Führungsteam und dem Vorstand Risiken melden, müssen Sie sich fragen, welche Ziele für sie wichtig sind. Es ist nicht so, dass ihnen die Ziele der einzelnen Teams und Projekte gleichgültig wären. Aber die Aufgabe der Unternehmensführung ist es, sich auf das große Ganze zu konzentrieren.

Hier sind drei Ziele, von denen Sie sicher sein können, dass sie den Führungskräften in Ihrem Unternehmen wichtig sind:

- Vertraulichkeit, Integrität und Verfügbarkeit von Daten
- Geschäftskontinuität
- Einhaltung gesetzlicher Bestimmungen

Es können auch andere Ziele verfolgt werden, wie ein bestimmter Prozentsatz des Umsatzwachstums oder ein guter Ruf auf dem Markt. Jedoch können Sie sicher sein, dass sich die Unternehmensführung um die Verwaltung und den Schutz wichtiger Daten kümmert, IT-Ausfälle, die den Geschäftsbetrieb zum Erliegen bringen, vermeidet und sicherstellt, dass das Unternehmen niemals aufgrund von Bußgeldern in die Schlagzeilen gerät.

Jedes dieser Ziele erfordert wahrscheinlich eine detaillierte Berichterstattung, um die Gesamtrisikobewertung des Ziels zu unterstützen. Die Daten, um die sich der Vorstand kümmert, erstrecken sich beispielsweise auf Kundendaten, Mitarbeiterdaten, Finanzdaten und geistiges Kapital wie Produktdesigns und Patente. All diese Datentypen müssen verwaltet und gesichert werden.

Unterschiedliche Datentypen können mit verschiedenen Risikoarten von unterschiedlicher Schwere konfrontiert sein. Der Vorstand muss wissen, inwieweit ein Ziel insgesamt gefährdet ist und welche spezifischen Datentypen möglicherweise neue Investitionen in die Sicherheit oder in die Schulung der Mitarbeiter erfordern.

Bevor Sie einen Bericht über Risiken in Ihrem Unternehmen erstellen, stellen Sie sicher, dass Sie die Ziele Ihres Führungsteams verstehen. Einige dieser Ziele können auf der Website Ihres Unternehmens veröffentlicht sein. Andere könnten jedoch in einem internen, langfristigen Strategieplan aufgeführt sein. So oder so müssen Sie jedoch wissen, was diese Ziele sind, da Sie diese als Rahmen für die Erörterung des Risikos verwenden werden.

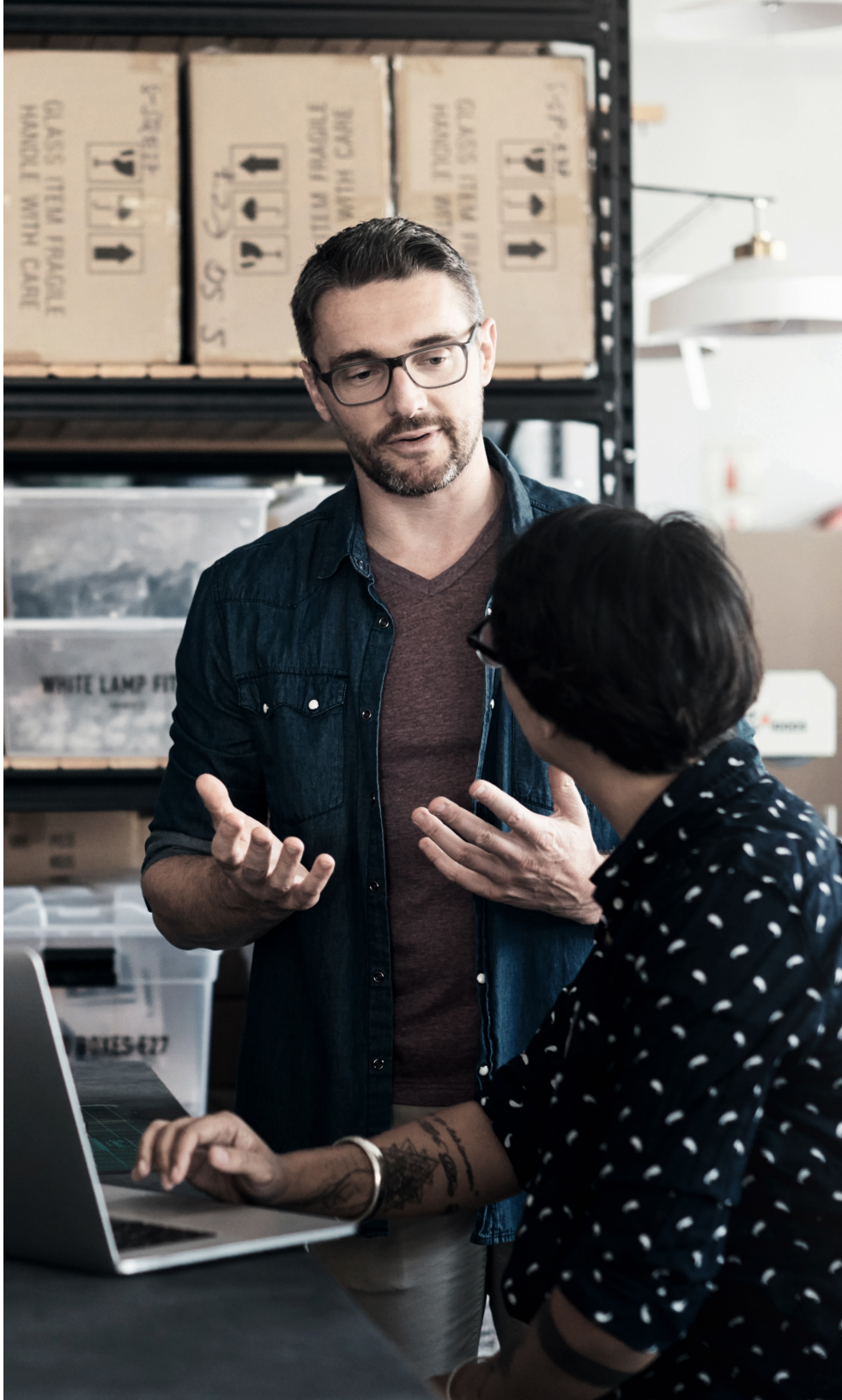
Wie wir in unserem eBook über die Risikomessung erwähnt haben, sollten alle Risiken, die Sie verfolgen und dem Führungsteam melden sollten, in einem konkreten Zusammenhang mit diesen übergeordneten Zielen stehen.

Sie sollte beispielsweise über alle Risiken für Menschen, Prozesse oder Technologien berichten, die für die Geschäftskontinuität Ihres Unternehmens entscheidend sind. Wenn ein geschäftskritisches Rechenzentrum nachweislich mit seinem Patch-Zeitplan im Rückstand ist, stellt dies ein großes Risiko dar, da nicht nur das Patchen eine Best Practice ist, sondern auch ungepatchte Server mit größerer Wahrscheinlichkeit Sicherheitsangriffen ausgesetzt sind oder unter Performance-Problemen leiden.

Weitere Informationen zur Erstellung gewichteter Risikomessungen finden Sie in unserem **eBook *Was Sie nicht wissen, kann Ihnen schaden: Expertentipps zur Risikomessung.***

Ihr Risikobericht sollte dem Führungsteam die Informationen bereitstellen, die es braucht, um kluge Entscheidungen darüber zu treffen, welche Maßnahmen zu ergreifen sind, um die Risiken im Zusammenhang mit den strategischen Zielen des Unternehmens zu mindern.

Wenn Sie Risikoinformationen präsentieren und Ihr Publikum gelangweilt oder verwirrt wirkt, liegt das wahrscheinlich daran, dass Sie Ihre Ausführungen nicht auf die Themen ausgerichtet haben, die dem Führungsteam wirklich am Herzen liegen.



KAPITEL 2:

Risiken erkennen hilft Ihnen, wie ein Angreifer zu denken

Es gibt einen zusätzlichen Vorteil, wenn Sie Ihre Risikoberichte auf diese Weise formulieren. Wenn Sie die Risiken für Ihre Daten und die Geschäftskontinuität Ihres Unternehmens erkannt haben, haben Sie auch die Schwachstellen identifiziert, die von kriminellen Vereinigungen und feindlichen Staaten angegriffen werden könnten.

Wenn ein Cyberkrimineller jedoch versucht, in die IT-Systeme Ihres Unternehmens einzudringen, was macht er dann? Höchstwahrscheinlich versuchen sie entweder, an Ihre Daten heranzukommen, um sie zu stehlen oder weiterzugeben, oder sie versuchen, an die Systeme zu gelangen, die Ihre Daten verarbeiten, und diese Systeme möglicherweise durch Ransomware oder eine andere Form des Angriffs zu stören.

Da Sie das Risiko jetzt jedoch auf der Grundlage strategischer Ziele messen und melden, verfügen Sie über einen detaillierten, gewichteten Bericht über die Schwachstellen und Anfälligkeiten im Zusammenhang mit Ihren Daten und den Systemen, die Ihre Daten speichern, verarbeiten und präsentieren. Auf der Grundlage Ihrer detaillierten Kenntnisse über Schwachstellen, Wahrscheinlichkeiten usw. wissen Sie, was am ehesten ins Visier genommen werden kann und wie Sie es schützen können.

All diese unterstützenden Informationen machen die Risikobewertung, die Sie dem Vorstand vorstellen, viel glaubwürdiger und nützlicher. Der Vorstand sieht, wie die Daten und die Geschäftskontinuität gefährdet sind, welche Kontrollen vorhanden sind, um diese Risiken zu mindern, und wie diese Kontrollen verbessert oder ausgeweitet werden könnten, um die Risiken im Einklang mit der Gesamtstrategie des Unternehmens weiter zu reduzieren.

KAPITEL 3:

Risiken betreffen den IT-Betrieb, nicht nur die IT-Sicherheit

Geschäftskontinuität bedeutet, dass die Mitarbeiter der IT-Organisation alles erhalten, was sie zur Aufrechterhaltung ihrer Produktivität und zur Unterstützung der Partner und Kunden des Unternehmens benötigen. Die Gewährleistung der Geschäftskontinuität erfordert die Bewertung und Abschwächung von Risiken für Websites, Datenbanken, Finanzsysteme, E-Mail-Server, Geschäftsprozesse und vieles mehr.

Außerdem ist eine Kapazitätsplanung erforderlich, insbesondere wenn das Unternehmen wächst. Die Kapazitätsplanung wiederum kann zu neuen Cloud-Migrationsprojekten, neuen Technologieanschaffungen oder der Entwicklung neuer Anwendungen führen, die allesamt neue Risiken für das Unternehmen mit sich bringen können.

Schließlich kann die Geschäftskontinuität IT-Prozesse wie Patch-Management, Mitarbeiterschulungen innerhalb und außerhalb der IT-Abteilung sowie Partnerbeziehungen umfassen.

Die Unternehmensleitung muss die Risiken in jedem dieser Bereiche sowie die kumulativen Risiken verstehen, die sich auf die Fähigkeit des Unternehmens auswirken, seine Geschäftskontinuitätsziele insgesamt zu erreichen.

KAPITEL 4:

Teilen Sie den Bericht mit den Geschäftsbereichen, die Sie bei der Erstellung unterstützt haben

In unserem E-Book zur Messung von Risiken haben wir hervorgehoben, wie wichtig es ist, mit Stakeholdern in den einzelnen Abteilungen und Geschäftsbereichen zu sprechen, um mehr über ihre Wahrnehmung von Risiken zu erfahren. Wahrscheinlich sind ihnen Risiken und Prioritäten bekannt, die Ihnen beim Scannen der Asset-Bestände in der IT-Abteilung entgehen könnten.

Nachdem Sie nun einen Bericht erstellt haben, teilen Sie Ihre Ergebnisse mit diesen Stakeholdern. Erkundigen Sie sich, was sie über die Art und Weise denken, wie Risiken gemessen und gemeldet wurden. Sobald das Führungsteam und der Vorstand die Gelegenheit hatten, den Bericht zu prüfen, sollten Sie den Autoren des Berichts alle Neuigkeiten über neue Investitionen, veränderte Prioritäten usw. mitteilen.

Die Menschen möchten wissen, dass ihnen zugehört wird und sie verstanden werden. Durch die Weitergabe der Berichtsergebnisse schließen Sie den Kreis der Menschen, mit denen Sie zu Beginn Ihres Risikomanagementprozesses gesprochen haben, und erhöhen die Wahrscheinlichkeit, dass sie in Zukunft zu den Risikobewertungen beitragen werden.

KAPITEL 5:

Einrichtung von Systemen zur Beschleunigung der Berichterstattung

In vielen Unternehmen erfolgt die Berichterstattung über Risiken jährlich oder vierteljährlich. Aber die Risiken verlagern sich ständig. Vorschriften ändern sich. Neue Wettbewerber erschließen Märkte. Es tauchen neue Malware-Varianten auf. Neue Geschäftsinitiativen und digitale Transformationen können die Prioritäten verschieben, einige Risiken beseitigen und andere schaffen.

Richten Sie die IT-Systeme darauf aus, dass sie Workflow-Prozesse zur Automatisierung und Beschleunigung der Datenerfassung für die Risikoberichterstattung unterstützen. Dadurch erhalten Sie zu jedem Zeitpunkt einen wesentlich zeitnaheren und genaueren Bericht über Risiken. Dies erleichtert auch die schnelle Bewertung von Risiken, wenn neue Bedrohungen auftreten oder wenn Ihr Unternehmen einen neuen Markt betritt oder eine neue Technologie einführt.

Eine wichtige Voraussetzung für die Automatisierung der Risikoanalyse ist die Sicherstellung, dass Sie Echtzeitdaten von Endpunkten – Desktops, Laptops, Tablets, Smartphones und Servern, auf die Ihre Mitarbeiter angewiesen sind – erfassen können. Durch **den Echtzeitzugriff auf das Geschehen an den Endpunkten** erhalten Sie Einblicke in die Mitarbeiterproduktivität, den Bedrohungsstatus, die Nutzung von IT-Ressourcen und vieles mehr.

Risikoberichterstattung als laufende Praxis

Angesichts der zunehmenden Cyberbedrohungen und der Tatsache, dass sich Unternehmen schneller als je zuvor weiterentwickeln, ist es für Führungskräfte unerlässlich, die Risiken, die ihr Unternehmen gefährden könnten, zu verstehen und zu minimieren. Dieses Verständnis beginnt mit einer effektiven Risikoberichterstattung.

In diesem E-Book haben wir besprochen, was die Risikoberichterstattung erfolgreich macht. Wir haben betont, wie wichtig es ist, Risiken als Unsicherheiten in Bezug auf Ziele zu verstehen und die Risikomessungen mit den strategischen Zielen abzustimmen, die dem Führungsteam Ihres Unternehmens am wichtigsten sind.

Wir haben außerdem über strategische Ziele gesprochen, die in den meisten Unternehmen gleich sind, und wie die Konzentration auf diese Ziele Ihrem Sicherheitsteam bei der Identifizierung möglicher Angriffsziele von Cyberkriminellen auf die IT-Infrastruktur Ihres Unternehmens helfen kann.

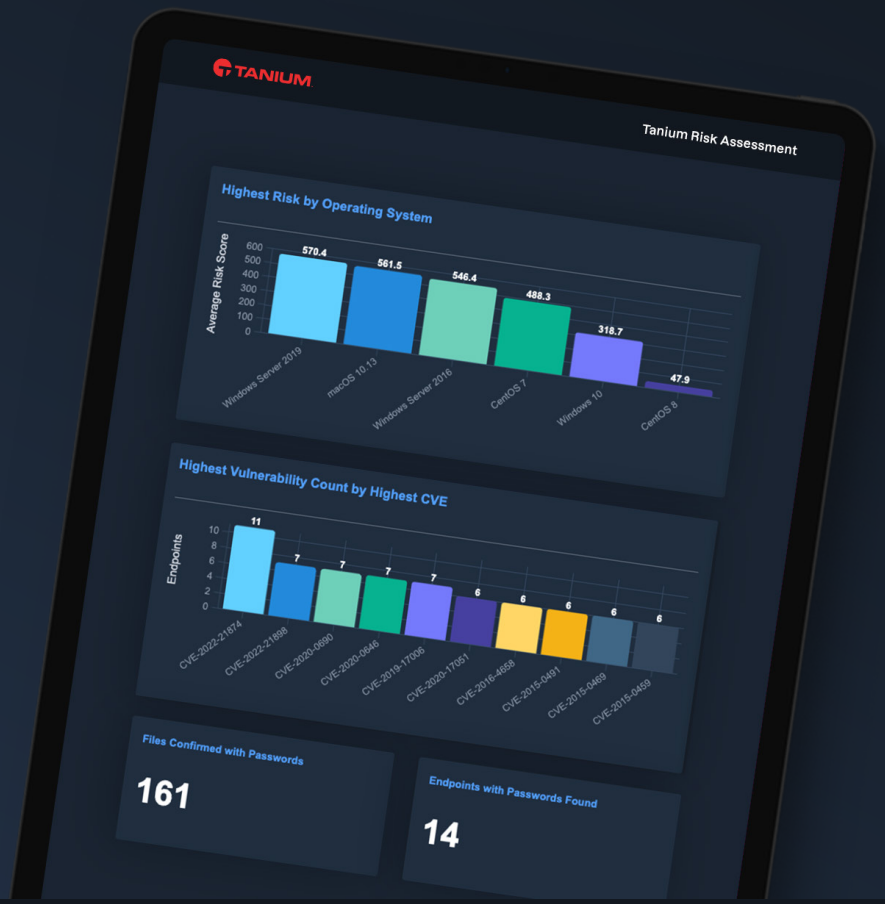
Idealerweise sollte die Risikoberichterstattung eine kontinuierliche Praxis sein. Die Risiken ändern sich ständig, sei es durch neue Geschäftsinitiativen oder neue Arten von Cyberbedrohungen. Durch die Automatisierung der Datenerfassung und Risikobewertung erhält das Führungsteam Ihres Unternehmens die wichtigen Informationen, die es benötigt, um die richtigen Entscheidungen zur Risikominderung zu treffen und die Unternehmensziele zu erreichen.

Endpunkte spielen eine wichtige Rolle bei der Risikobewertung und Berichterstattung. Die Tanium Converged Endpoint Management (XEM)-Plattform kann Unternehmen dabei helfen, mehr Transparenz über ihre Sicherheitsmetriken zu erhalten, sodass sie Risiken identifizieren und in Echtzeit beheben können. Tanium Benchmark ist die einzige Lösung, die Risikovergleiche mit Branchenkollegen in Echtzeit ermöglicht.

Erfahren Sie mehr über **Tanium Benchmark.**

Bewerten Sie Ihre Endpunkte anhand mehrerer Risikovektoren und Branchen-Benchmarks – in 5 Tagen und ohne Kosten.

Mehr erfahren →



Als branchenweit einziger Anbieter von Converged Endpoint Management (XEM) führt Tanium den Paradigmenwechsel bei herkömmlichen Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an. Nur Tanium schützt jedes Team, jeden Endpunkt und jeden Arbeitsablauf vor Cyberbedrohungen, indem es IT, Compliance, Security und Risk in eine einzige 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 Infrastruktur. Mehr als die Hälfte der Fortune-100-Unternehmen und die US-Streitkräfte vertrauen auf Tanium, um Einzelpersonen zu schützen, Daten zu verteidigen, Systeme zu sichern und jeden Endpunkt, jedes Team und jeden Workflow überall zu identifizieren und zu steuern. Das ist die Power of Certainty.

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