ivanti

Compliance für die komplexen Audits von heute

Ein moderner, auf den Menschen ausgerichteter Ansatz zur Beseitigung der durch Compliance-Bemühungen verursachten Risiken, Kosten und Unterbrechungen

Inhalt

Einführung

Compliance-Audits machen Leute nervös. Insbesondere die IT-Mitarbeiter machen sich Sorgen darüber, ob sie wohl die verwirrenden und operativ herausfordernden gesetzlichen Vorschriften tatsächlich erfüllen konnten. Sie machen sich Gedanken darüber, ob sie den möglicherweise skeptischen Prüfern die Compliance glaubhaft beweisen können. Und sie sorgen sich, wie stark ein Audit-„Probealarm“ ihr Team stören und Produktivität absorbieren wird, die anderswo dringend gebraucht wird.

Dieser Zustand der Sorge ist jedoch nicht zwingend. Mit einem automatisierten richtlinienbasierten Ansatz für den IT-Betrieb, bei dem die Menschen im Mittelpunkt stehen, können Sie das Risiko einer Non-Compliance erheblich reduzieren. Sie können für Prüfer eine beeindruckende und glaubwürdige Dokumentation Ihrer Compliance-Maßnahmen bereitstellen. Und wenn Sie sicherstellen, dass Ihre IT-Betriebsabläufe an sich stets prüfungsbereit sind, können Sie die Compliance-Kosten minimieren.

Das Beste daran ist jedoch, dass dieser außergewöhnliche Grad an Vertrauen in die Compliance sogar ein sekundärer Nutzen Ihres mitarbeiterorientierten, auf der Basis von Richtlinien automatisierten IT-Betriebs sein kann. Der primäre Nutzen besteht in der Fähigkeit, Ihren Mitarbeitern Zugriff auf die digitalen Ressourcen zu geben, die sie tagtäglich zur Erledigung ihrer Aufgaben benötigen, schneller, sicherer, präziser und mit weniger Aufwand, selbst wenn Ihr digitales Business von ständigem Wandel und Wachstum geprägt ist.

Eine auf die Mitarbeiter ausgerichtete, richtlinienbasiert automatisierte IT-Abteilung ist daher ein Gewinn für die Compliance-Führung, das IT-Team, die Mitarbeiter, das Unternehmen und für seine Kunden.

Warum Compliance belastet

Compliance verlangt eine strenge Regelung der Verhaltensweisen eines Unternehmens durch Richtlinien. Diese werden in der Regel in Form von allgemeinen Grundsätzen definiert. Compliance erfordert ferner eine glaubwürdige Dokumentation, die belegt, dass diese Richtlinien tatsächlich und universell im gesamten Unternehmen durchgesetzt werden.

IT-Compliance gibt Anlass zur Sorge, ist mühsam, teuer und störend, da die IT nie für solche Anforderungen ausgelegt wurde. Stattdessen wurde die Entwicklung der IT durch Kräfte wie Technologien, Zweckdienlichkeit und organisatorische Risikofreudigkeit vorangetrieben. Als das Unternehmen PCs brauchte, musste die IT-Abteilung PCs liefern. Als es CRM verlangte, lieferte die IT CRM. Als es Analysen verlangte, lieferte die IT diese.

IT-Führungskräfte und die unterstützenden Teams haben über die Jahre hinweg bemerkenswerte Arbeit geleistet und kontinuierlich bahnbrechende Technologien für das Unternehmen bereitgestellt, trotz begrenzter Budgets, widersprüchlicher Behauptungen von Anbietern und einer nie dagewesenen Forderung nach ununterbrochenem Lernen.

Doch unter dem Druck anhaltender Forderungen seitens des Unternehmens, die richtigen Technologien zum richtigen Preis und mit dem geringsten Risiko bereitzustellen, stand die Compliance niemals im Mittelpunkt. Das Ergebnis ist ein IT-Betriebsmodell, das in mehrerer Hinsicht grundsätzlich im Konflikt mit der Compliance steht, wie in der folgenden Grafik gezeigt:

	IT-Betriebsmodell	Compliance-Modell
Funktionsprinzip	Zweckmäßigkeit: Dinge erledigen, wenn das Geschäft sie erfordert, innerhalb von Budget- bzw. Personalzwängen. Lassen Sie nicht zu, dass Perfektionismus zum Feind des Guten wird. Nehmen Sie eventuell nötige Verbesserungen im nächsten Quartal vor.	Richtlinie: Machen Sie alles im Einklang mit den gesetzlichen Vorschriften. Fehler und Lücken sind inakzeptable Versäumnisse, die Geldstrafen, Bestrafung des Verhaltens und andere widrige Konsequenzen zur Folge haben können.
Organisationseinheit	Technologie: Der Geschäftsbetrieb ist nach Infrastruktur (Server, Storage, Netzwerke), nach Anwendungs- bzw. Ressourcentyp (ERP, CMS, E-Mail) und/oder nach Funktion (Entwickler, Betrieb, Sicherheit, Support) organisiert.	Menschen und deren Verhalten: Bestimmen Sie das Wer, Was, Wann und Wie. Hat irgendein Mitarbeiter Daten gesehen, die er nicht hätte einsehen dürfen? Könnte sich jemand, der nicht im Unternehmen arbeitet, als privilegierter Benutzer ausgeben? Wie schnell können Sie die Zugriffsrechte eines gekündigten Mitarbeiters widerrufen?
Risikoschwelle	Unternehmensebene: Entscheiden, wie viele Risiken das Unternehmen im Bestreben, Wettbewerbsvorteile, Marktanteile oder andere Ziele zu erreichen, bereit ist einzugehen.	Staatliche/gesellschaftliche Ebene: Entscheiden, wie viel Risiko in den Augen der Regulierungsbehörden für die einzelnen Bürger und für die Gesellschaft als Ganzes annehmbar ist.
Begründung für Automatisierung	Vornehmlich wirtschaftlich gesehen: Automatisieren, um die Arbeitskosten signifikant zu senken, und/oder um Fehler zu verhindern, die ebenfalls mit signifikanten Kosten verbunden sind.	Vornehmlich unter dem Governance-Aspekt: Automatisieren, um sicherzustellen, dass alles überall stets gemäß den derzeit geltenden Richtlinien getan wird.
Dokumentation	Sekundär: Das Wichtigste: Tun Sie, was zu tun ist. Gute Ergebnisse dokumentieren sich selbst. Berichte sind nur dahingehend wertvoll, dass Sie uns helfen, Probleme zu verstehen und zu lösen.	Wesentlich: Eine glaubwürdige Dokumentation einer konsistenten, zuverlässige Umsetzung von Richtlinien ist von der Umsetzung selbst nicht zu unterscheiden. Was nicht geprüft werden kann, ist nicht geschehen.

Diese Brüche erklären, warum die IT-Compliance nach heutigem Stand nahezu immer eine kostspielige, ungewisse und störende Belastung im Nachhinein darstellt, die sich Unternehmen noch zusätzlich zu ihren ohnehin schon beträchtlichen Technologieinvestitionen aufbürden müssen. Da Compliance nicht in die IT integriert ist, haben sie es schwer, Richtlinien auf mehrere ungleichartige Kontrollmechanismen aufzuerlegen. Sie verschwenden Stunden, die sie nicht übrig haben, um aus verschiedenartigen Protokolldateien auditwürdige Berichte zusammenzuschustern, ganz zu schweigen vom ständigen Hin und Her, das damit einhergeht, diese auf Anfragen des Prüfers mit immer mehr Daten zu überarbeiten. Trotz dieser Bemühungen sehen Unternehmen Audits immer noch mit Furcht entgegen. Schlimmer noch, die Ergebnisse dieser Audits bedeuten oft Geldstrafen für das Unternehmen und mehr Probleme für die IT, Probleme, die noch umfangreichere ToDo-Listen und einen Verlust an Glaubwürdigkeit in der Führungsetage nach sich ziehen.

Zweifellos muss es einen besseren Weg geben.

Menschen im Mittelpunkt

IT-Betriebsabläufe sind weiterhin rund um Hardware, Software und Daten organisiert. Dies ist ein Überbleibsel aus den Anfängen der IT, als Technologie vollständig in einem Rechenzentrum untergebracht war und die Endbenutzer an statischen ortsfesten Terminals saßen. Selbst bei IT-Abteilungen, die mit Mobility-Management-Tools auf das digitale Unternehmen reagiert haben, liegt der Fokus in der Regel immer noch auf Hardware und Software, d. h. dem Endbenutzergerät und dessen Betriebssystem, MAC-Adresse usw.

Doch im Mittelpunkt von beidem, der IT und der Compliance, steht der Mensch, nicht sein Gerät. Konkret muss die IT, um von Haus aus konform zu werden, dafür sorgen, dass die Verwaltung jeder einzelnen digitalen Arbeitssitzung in Echtzeit von Folgendem bestimmt sein muss:

- **Den Identitätsattributen der Person**. Es reicht nicht aus, lediglich die Rolle einer Person zu bestätigen. Der Zugriff auf digitale Ressourcen muss auch auf der Basis der Attribute und Verantwortlichkeiten einer Person bestimmt werden. Stellenbezeichnung/Position, Bereich oder Abteilung, aktuelle Projekt- bzw. Teamaufgaben und ähnliches entscheiden, ob eine bestimmte Person zu einer bestimmten Zeit Zugriff auf eine bestimmte Ressource haben sollte. Manche Informationen befinden sich vielleicht in einem System des Personalwesens. Andere können von einem Bereichs- oder Abteilungsleiter bestimmt werden. Doch diese Informationen über jede Person, die aktiv versucht, auf digitale Ressourcen zuzugreifen, sind entscheidend für die Compliance, die Sicherheit und die Ausrichtung an den Geschäftszielen.

- **Der Kontext der Arbeitssitzung der Person**. Compliance erfordert mehr, als nur zu wissen, dass ein legitimer Mitarbeiter ein legitimes Gerät nutzt. Der Kontext jeder digitalen Arbeitssitzung ist ebenfalls wichtig. Erfolgt die Anmeldung aus einem Café mit nicht sicherem WLAN? Von einem ungewöhnlichen Ort zu einer ungewöhnlichen Zeit? Wurden besondere Bescheinigungen unterzeichnet, die von der Compliance-Organisation verlangt werden? Eine wirklich auf den Menschen ausgerichtete IT wird die Antworten auf diese und andere Fragen in ihr Echtzeitmanagement des digitalen Arbeitsplatzes des Individuums einbeziehen.

Richtliniengesteuert

Richtlinien sind einfache Regeln, die Verhaltensweisen bestimmen. Bezogen auf die IT-Compliance sind Richtlinien Regeln, die IT-Prozesse und Zugriffsrechte von Benutzern gemäß den Vorschriften bestimmen, die von verschiedenen Organisationen außerhalb des Unternehmens stammen.

Wie oben angemerkt steht dies in auffälligem Kontrast zu den typischen „Betriebsregeln“ der IT-Abteilung, die durch die Anforderungen des Geschäfts bestimmt und tendenziell in ihrer Logik und ihren Parametern etwas beschränkt sind: schnellstmöglich auf neue Rechteanfragen reagieren, keinen Netzwerkzugriff von einem Endpunkt zulassen, der nicht erkannt wurde, auf übermäßig viele Zugriffsversuche aufmerksam machen usw.

Damit die IT ihrem Wesen nach Compliance erreicht, muss sie die Fähigkeit entwickeln, Regeln mit mehr Parameter und in einer größeren Komplexität zu definieren, zu speichern, durchzusetzen und zu modifizieren, als sie von externen Agenturen verlangt wird. So kann es beispielsweise sein, dass die IT-Abteilung eine liberale Geofencing-Richtlinie für Collaboration-Tools, eine restriktivere Geofencing-Richtlinie für die Mehrzahl der Enterprise-Anwendungen und eine noch strengere Geofencing-Richtlinie für Anwendungen einführen muss, die personenbezogene Daten von Kunden einschließen. Die Richtlinien müssen dann basierend auf dem Kontext des Benutzers durchgesetzt werden, damit sichergestellt ist, dass sie durchgesetzt werden.

Diese Einhaltung von Richtlinien ist nicht nur deshalb notwendig, damit die gesetzlichen Vorschriften operativ erfüllt werden können. Ein zentralisiertes, gut verwaltetes Richtlinien-Repository ist auch etwas, das jeder Prüfer als Beleg für das Due-Diligence Compliance-Programm eines Unternehmens erwartet.

Automatisiert. Ohne wirksame Automatisierung sind Richtlinien kaum durchsetzen und nur Worte auf Papier. Eine richtliniengesteuerte Automatisierung der Kontrolle des Arbeitsbereichs von Benutzern bildet aus mehreren Gründen die Grundlage der Umsetzung von Compliance im IT-Betrieb, darunter:

Vertrauen in die Compliance. Compliance, die von manuellen Prozessen, selbstentwickelten Skripts und anderen diversen Mechanismen abhängt, ist anfällig für Fehler und Versäumnisse. Compliance-Manager und Prüfer können Mechanismen zur Durchsetzung von Richtlinien nicht trauen, wenn diese nicht vollständig automatisiert sind.

Reaktion in Echtzeit und im Kontext. Nur mit Automatisierung kann der IT-Betrieb sofort auf die Richtlinien betreffende Bedingungen reagieren. Wenn also ein Kontextparameter wie Ort, Zeit oder Netzwerkverbindungstyp gegen eine Zugriffsrichtlinie verstößt, kann das System in Echtzeit entsprechend reagieren.

Audit-bereite Dokumentation. Automatisierte Richtliniendurchsetzung kann auch als glaubwürdige Quelle für die Selbstdokumentation dienen, da alle Zugriffsversuche und Erlaubnisse bzw. Verweigerungen im selben System erfasst werden können, das diese ausführt. Das Ergebnis ist ein einheitlicher und höchst glaubwürdiger Audit-Bericht.

Reduzierte Compliance-Arbeitslasten. Wenn Compliance-Richtlinien Mehrarbeit beim IT-Personal erforderlich machen, dann stellen die Budgets für Löhne und Gehälter stets ein Hindernis für die Umsetzung von Compliance dar. Automatisierung beseitigt dieses Hindernis, da sie die IT in die Lage versetzt, zusätzliche Compliance-Anforderungen mit der Zeit auch ohne zusätzliche Mittel zu berücksichtigen.

Anpassbarkeit von Richtlinien. In einer schlecht automatisierten Umgebung erfordert jede Änderung der gesetzlichen Anforderungen, dass das Personal die Regeln neu erlernen und Skripts neu programmieren muss, wenn diese überhaupt zu finden und/oder zu verstehen sind. Ein gut konzipiertes Automatisierungsmodul macht Änderungen dadurch einfach, dass das IT-Personal die Regeln mit ein paar Tastenanschlägen einfach neu definieren kann.

Selfservice und Delegierung. Automatisierung versetzt ferner das Bereichspersonal und den Bereichsleiter in die Lage, direkt Maßnahmen einzuleiten, ohne auf manuelle IT zu warten. Dies kann in Situationen wie der Kündigung eines Mitarbeiters von unschätzbarem Wert sein, denn die Personalabteilung kann die Rechte dieses Benutzers sofort und universell mit einem einzigen Mausklick widerrufen.

Das Fazit

Damit die IT die sich ständig ändernden Compliance-Anforderungen effektiv, glaubwürdig und kosteneffizient erfüllen kann, muss die Compliance zu einem wesentlichen Aspekt des IT-Betriebs werden. Dies bedeutet, dass die IT an sich einen stärkeren Fokus auf den Menschen haben und über einen einheitlichen Mechanismus für die Verwaltung und Automatisierung von konformitätsbezogenen Richtlinien im gesamten Unternehmen verfügen muss.

Damit die IT-Abteilung für die Compliance, Sicherheit und Abstimmung geschäftlicher Ziele sorgen kann, benötigt sie ein automatisiertes Mittel zur Durchsetzung von Zugriffsrichtlinien, die auf Benutzeridentitäten und -rollen, dem Sitzungskontext und einer Reihe klar definierter Regeln basieren, die bestimmen, wem unter welchen Bedingungen Zugriff auf was gewährt wird.

Audits können großartig sein

Gesetzliche Vorschriften werden technisch immer anspruchsvoller. Die möglichen nachteiligen Folgen eines fehlgeschlagenen Audits nehmen ebenfalls stetig zu. Die Vorteile von „Bereit zur Prüfung“:

Reduziertes Compliance-Risiko. Eine zuverlässig automatisierte und regelbasierte Governance von Zugriffsrechten für Benutzer sorgt für eine erhebliche Reduzierung des Risikos von Ereignissen und Aktionen, die gegen Vorschriften im Hinblick auf den Schutz von Kundendaten, die Transaktionsidentität und andere Anforderungen verstoßen.

Höchst glaubwürdige Audit-Dokumentation. Bei Compliance geht es nicht allein darum, konform zu sein. Vielmehr geht es auch darum, Compliance zu beweisen. Eine Audit-Dokumentation, die vom selben System generiert wurde, das Kontrollmechanismen zur Einhaltung von Unternehmensrichtlinien durchsetzt, wird höchstwahrscheinlich selbst den anspruchsvollsten Prüfer eher zufriedenstellen, als Berichte, die aus verschiedenartigen Protokollen zusammengeschustert wurden.

Minimierung von Compliance-Kosten. Eine richtlinienbasierte IT, die den Menschen in den Mittelpunkt stellt, eliminiert konformitätsbezogene Kosten in allen Bereichen: von den Kosten der Entwicklung neuer Skripts für jede neue Vorschrift bis hin zu den Kosten von „Probealarmen“ im Vorfeld von Audits.

Vermiedene bzw. reduzierte Sanktionen für Non-Compliance. Regulierer verfügen im Hinblick auf Compliance-Defizite meist über einen großen Ermessensspielraum, der sich auf Faktoren wie bestmögliches Bemühen und Engagement der Geschäftsleitung stützt. Die Implementierung von IT-Richtlinienautomatisierung kann daher über die positiven Ergebnisse hinaus, die eine Automatisierung liefert, selbst ein primärer Faktor zur Vermeidung von Sanktionen sein.

Über Compliance hinaus

Doch die Vorteile einer richtlinienbasierten IT-Automatisierung reichen weit über die Compliance hinaus. Konformitätsbezogene Richtlinien sind schließlich einfach ein Satz von Regeln. Die IT kann alle Arten von auf den Menschen ausgerichtete, kontextabhängige Regeln automatisieren, um die sich ständig verändernden Bedürfnisse des zunehmend digitalisierten Unternehmens besser zu erfüllen. Einige allgemeinere Vorteile für das Unternehmen:

Höhere Mitarbeiterproduktivität. Bei der Arbeitsweise der IT erleben die Mitarbeiter heute in den meisten Unternehmen Verzögerungen zwischen dem Zeitpunkt, zu dem sie eine Ressource benötigen und dem Zeitpunkt, zu dem ihnen die IT Zugriff darauf gewährt. Dies gilt insbesondere dann, wenn sie gerade neu eingestellt wurden oder die Position wechseln. Eine rollen- und kontextbasierte Automatisierung beseitigt diese Verzögerungen, damit die Mitarbeiter schneller produktiver sein können.

Erhöhte Sicherheit. Rollen- und kontextbasierte Automatisierung verbessert die Sicherheit, weil sie die Umsetzung des Whitelistings, die Verhinderung von fragwürdigen Zugriffsereignissen und das sofortige Offboarding gekündigter Mitarbeiter einfacher macht.

Verbesserte IT-Effizienz. Wenn das IT-Personal seine Zeit nicht mit manuellem Provisioning und Deprovisioning, dem Schreiben und der Pflege von Skripts, der Prüfung von Protokollen und anderen gängigen Aufgaben verbringen muss, kann es seine Zeit und seine Talente auf höherwertige Geschäftsaktivitäten konzentrieren. Die Umverteilung von Personalressourcen ist besonders wichtig, denn das Unternehmen verlangt weiterhin, dass die IT mehr mit weniger schafft.

Verbesserte Agilität im Unternehmen. Die Automatisierung von auf die Mitarbeiter ausgerichteten Richtlinien hilft Unternehmen nicht nur, schneller auf neue Vorschriften zu reagieren. Sie versetzt die IT-Abteilung in die Lage, die digitalen Workspaces von Mitarbeitern als Reaktion auf Fusionen, Übernahmen und Umstrukturierungen schnell umzukonfigurieren. Die hierdurch erreichte Agilität im Unternehmen senkt die Kosten solcher bedeutenden Ereignisse und stellt zugleich sicher, dass sich diese früher bezahlt machen.

Ein besseres, mehr auf den Verbraucher abgestimmtes Erlebnis für Mitarbeiter. Die Arbeitskräfte von morgen sind gegenüber IT-bezogenen Verzögerungen weit weniger tolerant als ihre Vorgänger. Eine weitgehend automatisierte IT, die genau weiß, wer die Benutzer sind, was sie brauchen und wo sie sich befinden – und die gegebenenfalls Selfservice bereitstellen kann –, wird schnell zu einem Muss, wenn es darum geht, Spitzenkräfte aus den Reihen der Digital Natives zu betreuen und zu binden.

Bessere Nutzung von Dienstleistern. Rollenbasierte Regeln vereinfachen die schnelle und sichere Zuweisung von entsprechend beschränkten Zugriffsrechten für Dienstleister und ein ebenso schnelles Widerrufen dieser Rechte, wenn die Verpflichtung abgeschlossen ist. Diese Fähigkeit ist insbesondere für Saisonbetriebe und HR-Organisationen wichtig, die ihre Personalfixkosten begrenzen möchten.

Vereinfachen Sie die Compliance mit Ivanti

Ivanti bietet Unternehmen die mitarbeiterorientierten Kontrollen, die sie benötigen, um die Konformität mit zahlreichen heutigen Datenschutzvorschriften und -standards aufrechtzuerhalten. Das Risiko von fehlgeschlagenen Compliance-Audits wird dadurch reduziert, dass der Mitarbeiter in den Mittelpunkt gestellt und der Einsatz von Automatisierung sichergestellt wird. Dies geschieht zuerst durch eine richtlinienbasierte Verwaltung des Datenzugriffs, um die Produktivität der Mitarbeiter sicherzustellen, und dann dadurch, dass man den Beweis erbringen kann, dass die erforderlichen Prozesse vorhanden sind und nicht umgekehrt. Dieser auf die Menschen fokussierte Ansatz macht Audits weniger belastend, Produktivität und Sicherheit sind gewährleistet und Richtlinien können durchgesetzt werden.

HIPAA: Der Health Insurance Portability and Accountability Act (HIPAA) schützt vertrauliche Patienteninformationen und stellt Konsistenz im gesamten Gesundheitswesen sicher. Ivanti automatisiert und schützt alle digitalen Workspaces für Krankenhäuser, Kliniken und andere Organisationen des Gesundheitswesens, die den HIPAA-Vorschriften Folge leisten müssen. Die Vorhersage der Services, die Kliniker benötigen und die Bereitstellung von kontextbezogenem Zugriff schützt Patientendaten und verbessert die Qualität der Dienstleistungen, die für Patienten erbracht werden.

SOX: Die Einhaltung des Sarbanes-Oxley Act ist für alle Aktiengesellschaften ein Muss, um die Investoren vor der Möglichkeit betrügerischer Buchführungspraktiken zu schützen. Ivanti setzt Kontrollmechanismen auf App-zu-App-Ebene ein, um sicherzustellen, dass die Mitarbeiter nur den Zugriff haben, den sie zur Erledigung ihres Auftrags benötigen, nicht mehr und nicht weniger. Stellen Sie Zugriff basierend auf Identitätsattributen und Kontext bereit, um Sicherheitsrichtlinien durchzusetzen.

PCI DSS: Der Payment Card Industry Data Security Standard (PCI DSS) ist ein weltweiter Standard für Kreditkartensicherheit. Ivanti hilft allen Organisation, die Kreditkartendaten akzeptieren, verarbeiten, speichern oder übertragen, eine sichere Umgebung für den Kreditkarteninhaber zu unterhalten. Ivanti sorgt dafür, dass Daten geschützt sind, indem die IT in die Lage versetzt wird, attributbasierten Zugriff bereitzustellen, der auf Richtlinien basiert, Zugriffsebenen zu zertifizieren und granulare Sicherheitsregeln auf Anwendungsebene auf dem Endpunkt anzuwenden.

DSGVO: Die Datenschutz-Grundverordnung (DSGVO) ist eine neue Verordnung der EU, die die personenbezogenen Daten des Einzelnen innerhalb der EU schützt. Jedes Unternehmen, das mit personenbezogenen Daten von natürlichen Personen innerhalb der EU umgeht – Verantwortliche für die Datenverarbeitung oder Auftragsdatenverarbeiter – müssen die Vorschriften der DSGVO erfüllen und Ivanti kann dabei helfen. Der Schutz von Daten durch Compliance-Maßnahmen, die für Prüfungsbereitschaft sorgen, stellt die Produktivität der Belegschaft sicher.

Wenn Sie HIPAA, SOX, PCI, DSGVO oder andere Datenschutzvorschriften einhalten müssen, kann Ivanti Ihnen durch die Durchsetzung Ihrer Governance- und Sicherheitsrichtlinien helfen, den Prozess der Erfüllung von Compliance-Audits zu vereinfachen. Unternehmen müssen für Compliance keine Abstriche bei der Produktivität hinnehmen oder umgekehrt. Compliance und Produktivität können beide aufrechterhalten werden.

www.ivanti.com

+1-888-253-6201

sales@ivanti.com