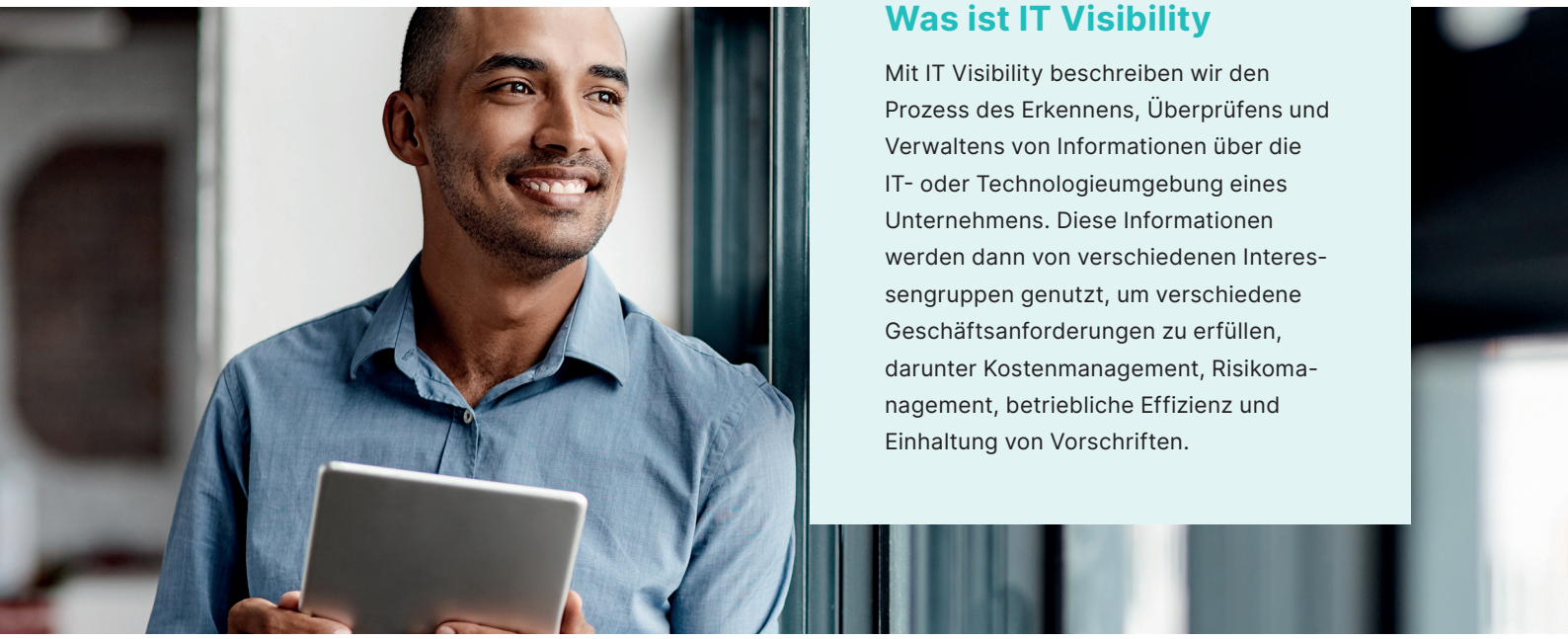
Fact Sheet

Warum ein Mangel an IT Visibility Ihre Geschäftsziele gefährden kann

Moderne IT-Strukturen sind komplex und vielschichtig. Die Systeme verlagern sich immer mehr in externe Cloud-Umgebungen mit Tausenden von Anwendungen und Diensten, die über Hunderte von Anbietern verstreut sind.

Das Wachstum von Cloud und SaaS und die Abkehr von tendenziell sichereren Unternehmensnetzwerken haben den Bedarf an IT-Visibility-Tools wie ITAM stark erhöht. Teams, die für die Verwaltung des IT-Bestands verantwortlich sind, müssen sich einen ganzheitlichen Überblick verschaffen, um zu wissen, worauf sie einen besonderen Fokus legen sollten. Und sie müssen sich auf die Informationen verlassen können, die sie zur Entscheidungsfindung nutzen. Vollständige IT-Transparenz schafft einen klaren und umfassenden Überblick über die aktuelle IT-Landschaft – von der Software, dem Rechenzentrum über die Public Cloud bis hin zu den Geräten der Mitarbeiter. Die Erkennung und Sichtbarkeit aller IT-Assets über alle Plattformen hinweg gibt Unternehmen die Möglichkeit, diese in einer einzigen, effizienten Umgebung zu kombinieren.



Was ist IT Visibility

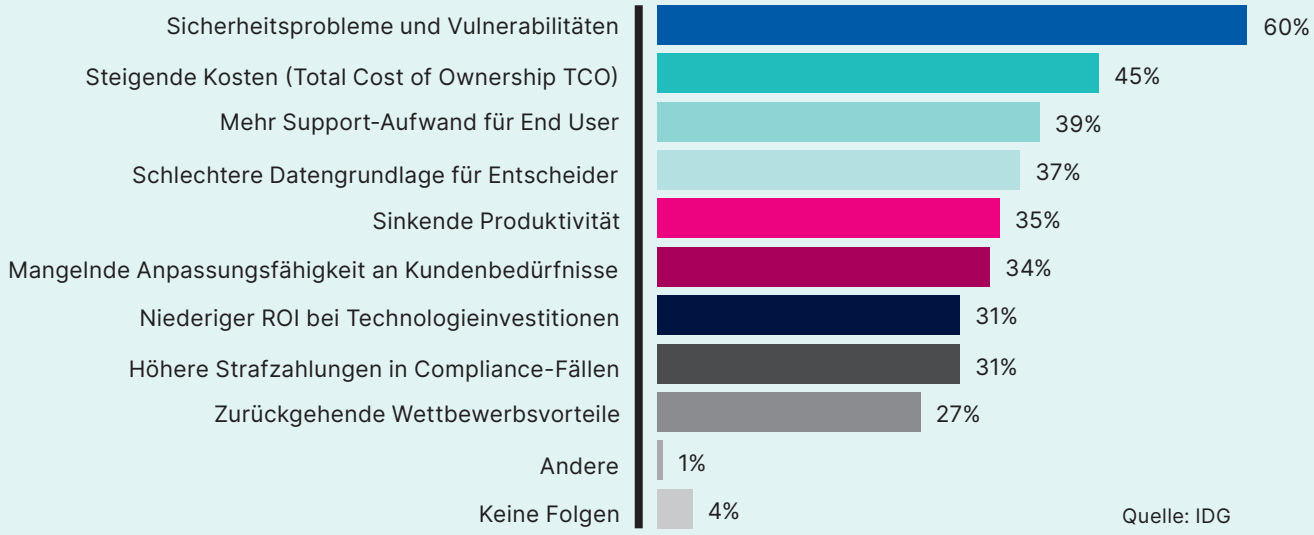
Mit IT Visibility beschreiben wir den Prozess des Erkennens, Überprüfens und Verwaltens von Informationen über die IT- oder Technologieumgebung eines Unternehmens. Diese Informationen werden dann von verschiedenen Interessengruppen genutzt, um verschiedene Geschäftsanforderungen zu erfüllen, darunter Kostenmanagement, Risikomanagement, betriebliche Effizienz und Einhaltung von Vorschriften.

Ein neuer Ansatz für IT Visibility ist erforderlich

Wenn Sie keinen genauen, aktuellen und vollständigen Überblick über Ihre Software-Assets haben, wird es schwierig, Produkte und Lizenzen effizient zu verwalten und den Überblick über auslaufende oder ungenutzte Produkte zu behalten. Aber das ist nur die eine Seite der Medaille. Wenn Ihre Daten nicht ordnungsgemäß verwaltet werden, können Sie keine wirksamen Maßnahmen ergreifen, um potenzielle Schwachstellen zu beseitigen, z. B. bei älteren Softwareprodukten oder Produkten, die von Mitarbeitern im Außendienst verwendet werden, die aber nicht mit Ihren IT-Richtlinien übereinstimmen. Genau wie ITAM benötigt auch die IT-Sicherheit einen Überblick über alle Assets, in diesem Fall jedoch zum Zwecke des Vulnerability Management oder der Abwehr von Sicherheitsrisiken und nicht zur Einhaltung von Lizenzvereinbarungen.

Laut IDG-Analyse (2022) sind Sicherheit und Schwachstellen bei weitem die größte Sorge, wenn es um den Mangel an IT-Transparenz geht, gefolgt von Auswirkungen auf die Kosten und dem erhöhten Supportbedarf der Endbenutzer.

Fehlende IT-Visibilität und mögliche Folgen



Erkennen Sie IT-Schwachstellen und bereiten sich vor

Wenn es um IT-Sicherheit geht, ist eine Bedrohung jede potenzielle Gefahr für Informationen oder Systeme. Dabei kann es sich um einen Eindringling handeln, der sich über einen Port der Firewall ins Netzwerk einklinkt, um einen Prozess, der auf Daten zugreift und damit gegen die Sicherheitsrichtlinien verstößt, um eine Überschwemmung, die eine Anlage zerstört, oder um einen Fehler eines Mitarbeiters, der vertrauliche Informationen preisgeben oder die Integrität einer Datei zerstören könnte.

Stellen Sie sich die folgende Situation vor: Ihr Governance-Team wird über eine neue kritische Software-Schwachstelle informiert. Wie sollen sie reagieren? Eine scheinbar einfache Frage: „Welche unserer Geräte sind durch diese Schwachstelle gefährdet?“ bedeutet für verschiedene Beteiligte unterschiedliche Dinge. IT-Transparenz gibt den Governance-Teams die Möglichkeit, sich einen umfassenden Überblick zu verschaffen und diese Daten bereitzustellen, um die Fragen der einzelnen Beteiligten zu beantworten und ihnen zu ermöglichen, die erforderlichen Maßnahmen zu ergreifen.

Wenn jedes Team seine eigene Erfassung und Inventarisierung mit eigenen Tools durchführt, können Risiken unzureichend gemanagt werden. Denken wir nochmal an die Auswirkungen einer veröffentlichten Softwareschwachstelle:

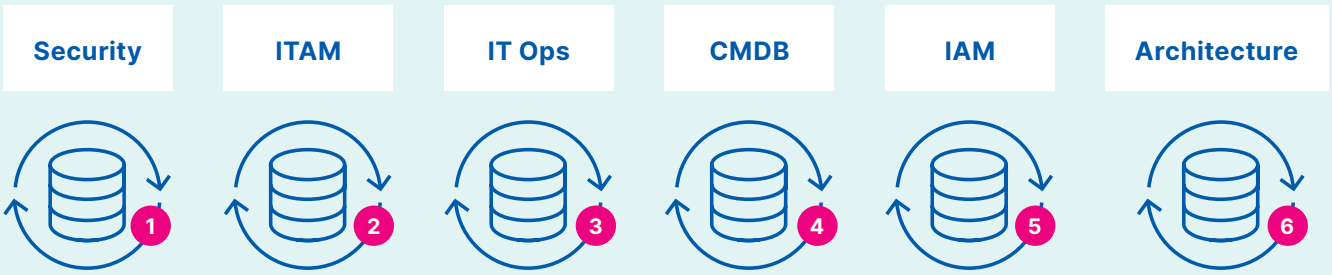
- Servicemanagement muss die betrieblichen Auswirkungen beurteilen.
- Compliance legt fest, welche Maßnahmen erforderlich sind, wie die Benachrichtigung einer Aufsichtsbehörde.
- Konfigurationsmanagement muss möglicherweise anfällige Geräte basierend auf Abhängigkeiten behandeln.
- Compliance oder Access Management benötigen eventuell Informationen über den Gerätezugriff.
- IT Operations identifiziert und patcht betroffene Geräte.
- IT-Sicherheit identifiziert und isoliert betroffene Geräte.

IT Visibility: Kollaboration anstelle von organisatorischen Silos

Jede dieser Reaktionen könnte unabhängig erfolgen, wenn nicht jeder Beteiligte über umfassende IT-Visibilität verfügt, was nicht ideal wäre. Zum Beispiel könnte ein Compliance- oder Risikomanager entscheiden, dass die Ausfallzeit eines anfälligen Geräts ein größeres Schadenspotenzial hat als ein Ansatz, bei dem das Gerät in Betrieb bleibt. Ein Service- oder Konfigurationsmanager könnte feststellen, dass Geräte sicher isoliert werden können, ohne den Service zu beeinträchtigen. IT Operations könnte feststellen, dass genügend Geräte auf Lager sind, um die anfälligen Geräte sofort zu ersetzen, und so weiter. Dies ist nur möglich mit den umfangreichen Kontextinformationen, die IT Visibility bietet.

Der große Nutzen von IT Visibility geht über isolierte operative Ansätze hinaus und nutzt sämtliche Daten zur Verwaltung und zum besseren Verständnis des IT-Bestands. Der integrierte Ansatz bietet einen detaillierten und ganzheitlichen Überblick, der es verschiedenen Beteiligten ermöglicht, operative, taktische und strategische Entscheidungen zu treffen. Das Ergebnis ist eine verbesserte Verwaltung des IT-Bestands, von der das gesamte Unternehmen profitiert, nicht nur die IT-Abteilung.

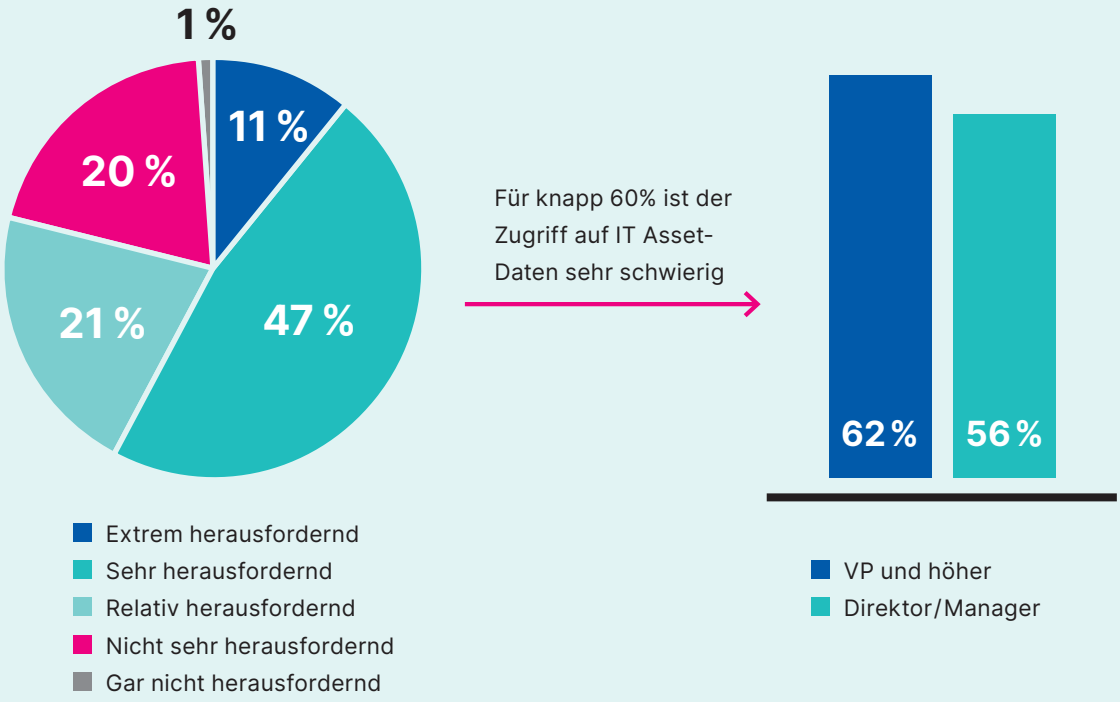
Daten-Silos innerhalb einer Organisation



IT-Verantwortliche brauchen Tools, die eine breite Palette von IT-Ressourcen erkennen, inventarisieren und sinnvoll nutzen können – wie On-prem-Software, physische Geräte, virtuelle Server, Cloud und Software-as-a-Service-Anwendungen. Dieser hybride Ansatz der modernen IT erfordert einen robusten, vielschichtigen Ansatz zur Erfassung von Governance-Daten. Ohne guten Einblick in Ihre IT-Umgebung ist es schwierig sicherzustellen, dass alle Dateneinspeisungen korrekte und verwertbare Daten liefern, und die Dinge werden schnell unübersichtlich und unorganisiert.

Für IT-Organisationen ist es nach wie vor eine Herausforderung, Zugang zu den Daten zu erhalten, die sie benötigen, um effektive Entscheidungen in Bezug auf IT-Assets zu treffen. Eine IDG-Umfrage ergab, dass 79 % der Befragten den Zugang zu Daten, die für fundierte Entscheidungen erforderlich sind, als schwierig empfinden, 47 % sogar als sehr schwierig.

Ist es für Sie schwierig, auf IT-Asset-Daten zuzugreifen, um effektive Entscheidungen zu treffen?



Vertrauenswürdige Daten sind die Grundlage der IT Visibility

Laut ISO 19770-1 (2017) sind vertrauenswürdige Daten die Grundlage des IT Asset Managements und werden wie folgt definiert: „Vertrauenswürdige Daten sind Daten, die korrekt, vollständig, relevant und für die autorisierten Benutzer, die sie zur Erfüllung einer Aufgabe benötigen, leicht verständlich und verfügbar sind."

Wenn alle Beteiligten im Unternehmen, wie z. B. IT-Sicherheit, ITAM, CMDB, Architecture, IT Ops, Finanzen, Beschaffung, oder Risikomanagement Entscheidungen auf der Grundlage derselben vertrauenswürdigen Daten treffen, werden diese Entscheidungen zweifellos besser ausfallen, als wenn alle Beteiligten in ihren Daten-Silos arbeiten und sich auf ihre eigenen Tools verlassen. Die Strategie besteht darin, verschiedene, unstrukturierte Datenströme aus den Systemen der Beteiligten zu kombinieren und zu normalisieren, um aussagekräftige Daten zu generieren, die allen Beteiligten dienen können. Der Vulnerability-Anwendungsfall zeigt, welche Folgen es haben kann, wenn Unternehmen IT Visibility nicht konsequent umsetzen. Implementieren Sie daher eine Lösung und Prozesse, um die mit den IT-Umgebungen Ihres Unternehmens verbundenen Daten besser zu verstehen und zu verarbeiten. Dies kann auf lange Sicht viel Geld und Ressourcen sparen.

Kontaktieren Sie uns – wir beraten Sie gerne.

www.usu.com