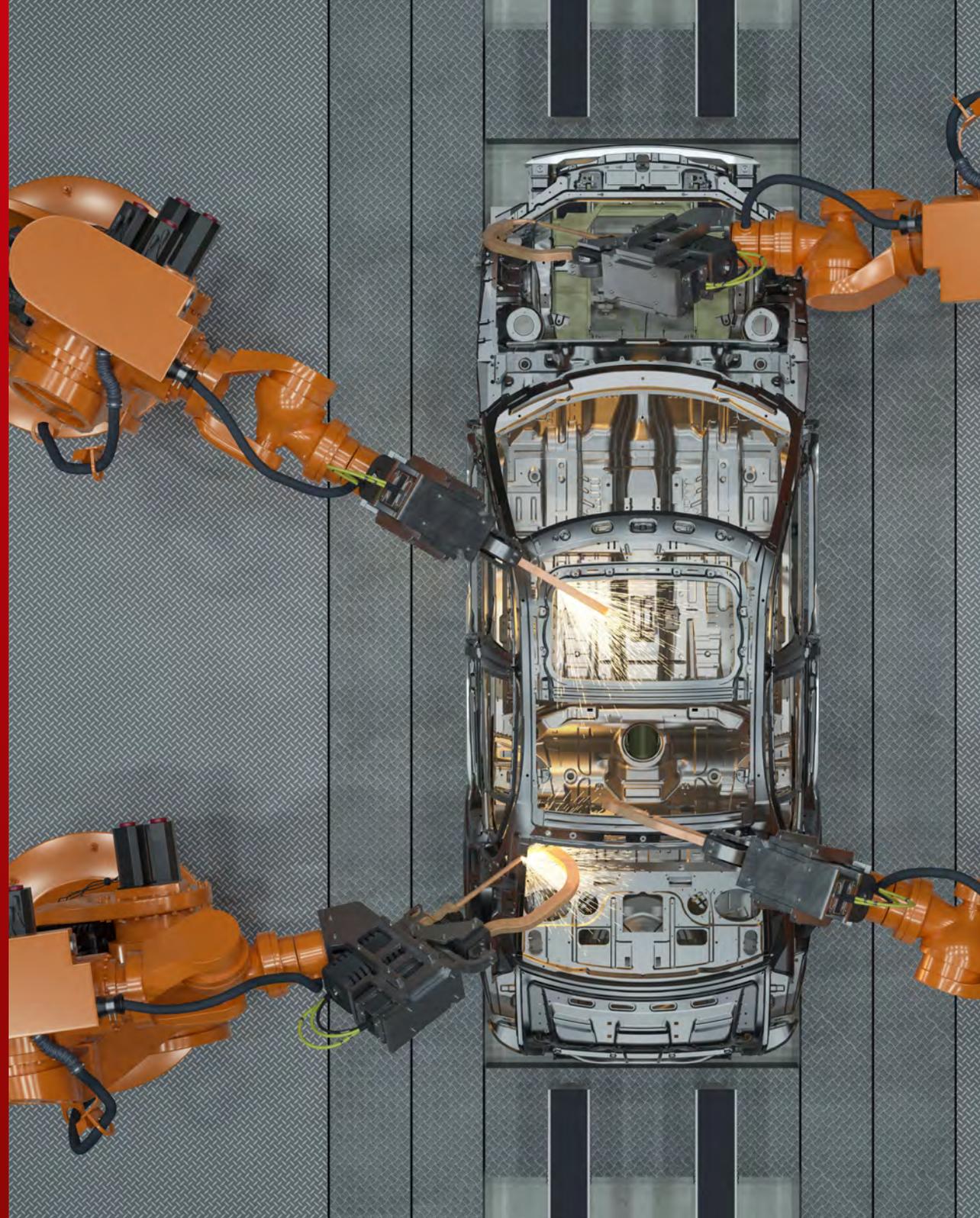


# Die Herstellung von Morgen

## Schnell den Fokus finden.

Industrie- und Fertigungsunternehmen auf dem europäischen Festland müssen sich neu erfinden – mit digitaler Transformation als Sprungbrett für diesen Umschwung des Geschäfts. Die Digitalisierung bringt viele Vorteile mit sich, schafft aber auch eine zu komplexe, zunehmend unüberschaubare Technologieumgebung. Dadurch ist die Verwaltung von IT-Anlagen und Geschäftsabläufen kostspielig und vor Angriffen, Verletzungen und dem Verlust von geistigem Eigentum zu schützen. Um die Verwaltungskosten zu senken und die Cyber-Resilienz zu erhöhen, müssen Unternehmen Technologie-Stacks modernisieren und rationalisieren; das beginnt mit einer besseren Asset-Visibilität. Hier sind drei Beispielanwendungen für die Einführung einer Endpunktplattform, die Ihnen Daten und Einblicke mit hoher Genauigkeit in Echtzeit liefert.



	<b>Verwaltung des Asset-Lebenszyklus</b>	<b>Automatisierung im großen Stil</b>	<b>Cyber-Resilienz</b>
<b>Die große Frage</b> <i>Welche Fragen werden Ihnen auf geschäftlicher Ebene gestellt?</i>	<p>Reduzierung der langfristigen Betriebskosten, da das Unternehmen von einer reinen On-Premise- zu einer Hybrid-Cloud-Umgebung umgestaltet wird. KPIs: Reduzierung der Gesamtbetriebskosten und Konsolidierung des Technologie-Stacks.</p> <p><b>Sonstige geschäftliche Auswirkungen/Ziele:</b></p> <ul style="list-style-type: none"> <li>Bessere Kontrolle über die Schatten-IT und die Federation des Technologiemanagements</li> <li>Reduzierung der technischen Schulden, die sich über viele Jahre der M&amp;A-Aktivität angesammelt haben</li> <li>Schaffen Sie größere Brücken und die Ausrichtung zwischen IT und OT</li> <li>Unterstützung des Wachstums in neue Produkttechnologien, wie z. B. Elektrifizierung</li> </ul>	<p>Steigern Sie die Produktivität, indem Sie das Servicemanagement stärker automatisieren und die domänenübergreifende Effizienz steigern. KPIs: Leistung pro Kopf, Fehlerdichte, Build-Stabilität und Betriebszeit.</p> <p><b>Sonstige geschäftliche Auswirkungen/Ziele:</b></p> <ul style="list-style-type: none"> <li>Neuausrichtung des Unternehmens auf der Plattform eines neuen Anbieters (d. h. Microsoft, ServiceNow)</li> <li>Qualifikations-/Fachkräftemangel in wichtigen operativen Bereichen wie Engineering und IT</li> <li>Änderung der Wirtschaftsbedingungen, die die Nachfrage nach bestimmten margenstarken SKUs ankurbeln</li> <li>Langsame Reaktionszeiten des Servicemanagements auf unternehmenskritische Geschäftsanwendungen</li> </ul>	<p>Reduzieren Sie das Risiko für die Lieferkette infolge der Neuausrichtung von industriellen Verarbeitungsschritten von ausländischen Märkten. KPIs: schnellere Audits und verbesserte ESG-Performance.</p> <p><b>Sonstige geschäftliche Auswirkungen/Ziele:</b></p> <ul style="list-style-type: none"> <li>Notwendiges Vereinheitlichen von Sicherheit und ITOps, um das Wachstum bei Zero-Day-Angriffen zu bekämpfen</li> <li>Geplante Einführung der Compliance-Automatisierung zur Einhaltung neuer regulatorischer Änderungen</li> <li>Rationalisierung der Risikoberichterstattung durch Konsolidierung des Volumens widersprüchlicher Datenfeeds</li> <li>Investitionen in neue, unerprobte Lieferanten, um bisherige Lieferanten/Hersteller zu ersetzen</li> </ul>
<b>Die Mini-Roadmap</b> <i>Welche Fragen werden Ihnen auf geschäftlicher Ebene gestellt?</i>	<ol style="list-style-type: none"> <li>Schaffen Sie Visibilität übergreifend über alle Technologien, die Sie haben und nutzen. Katalogisieren Sie Ihr gesamtes IT-System und erstellen Sie einen Prozess für regelmäßige Aktualisierungen. Dazu gehören neben der IT auch die Bereiche Herstellung und Produkttechnologie.</li> <li>Berechnen Sie Ihre Betriebskosten (TCO) für die Verwaltung und den Schutz Ihrer Vermögenswerte. Dazu gehören Hardware-Kapitalinvestitionen und Softwarelizenzen sowie alle Vollzeitäquivalent-Ressourcen (FTE), die für die Verwaltung und den Schutz Ihrer Technologie erforderlich sind.</li> <li>Starten Sie eine Initiative zur systematischen und methodischen Vereinfachung und Rationalisierung. Identifizieren Sie Redundanzen und Konsolidierungsmöglichkeiten innerhalb von IT und ITOps. Festlegung von Zielen zur TCO-Reduzierung und eines Governance-Rahmenwerks zur Messung des Erfolgs. Machen Sie die Gesamtbetriebskosten zu einem wichtigen KPI in Ihrer Unternehmensführung und schaffen Sie mit dieser Initiative einen Prozess für den laufenden Betrieb und eine Komponente der Finanzplanung.</li> </ol>	<ol style="list-style-type: none"> <li>Beurteilen Sie die Ausgangssituation der Produktivität Ihres Unternehmens. Legen Sie fest, welche Prozesse automatisiert und welche zugrunde liegenden Systeme beteiligt sind, einschließlich FTEs. Beantworten Sie für jeden wichtigen Prozess: „Was kostet es mich, x, y oder z zu erreichen?“</li> <li>Legen Sie Ziele für die Verbesserung fest und starten Sie eine interne Initiative zum Erreichen dieser Ziele. Konzentrieren Sie sich auf die Liste mit den minimalen Plattformanforderungen, die für eine effektive Automatisierung benötigt werden.</li> <li>Erstellen Sie einen laufenden Prozess zur Messung, Überprüfung und Korrektur der Produktivität im Rahmen der laufenden Betriebsführungs- und Budgetierungszyklen. Identifizieren Sie System- und Datenbeschränkungen, die sich auf die Produktivität ausgelagerter Services auswirken.</li> </ol>	<ol style="list-style-type: none"> <li>Bewerten Sie die Ausgangssituation der Cyber-Resilienz des Unternehmens und decken Sie alle Aspekte des Risikomanagements ab. Indizieren Sie alle Systeme, Prozesse und Mitarbeiter, die zur Erfüllung der Compliance-Ziele erforderlich sind. Erweitern Sie das Audit über die IT und InfoSec hinaus.</li> <li>Setzen Sie sich konkrete, messbare Ziele, um die Cyber-Resilienz zu verbessern und gleichzeitig die Komplexität und die anfallenden Kosten zum Erreichen der Ziele zu reduzieren. Nutzen Sie die Vorteile der Rationalisierung von Technologie und groß angelegten Automatisierungsinitiativen.</li> <li>Integrieren Sie wichtige IT- und ITSec-Tools in zentrale Repositories, um die Verfügbarkeit von Informationen und die Geschwindigkeit der Behebung zu verbessern. Entwickeln Sie einen hochgradig reproduzierbaren Prozess, um Ihre Cyber-Resilienz nachzuverfolgen und zu korrelieren sowie steuerliche und betriebliche Überprüfungszyklen abzustimmen.</li> </ol>
<b>Der Tech-Enabler</b> <i>Wie kann Tanium unterstützen?</i>	<p><b>Assets-Discovery und -Inventory</b></p> <p>Discover</p>	<p><b>Endpoint Management</b></p> <p>Discover, Enforce, Asset, Deploy, Patch, Performance</p>	<p><b>Risiko- und Compliance-Management</b></p> <p>Discover, Enforce, Benchmark, Impact, Reveal, Comply, Deploy, Patch</p>

Tanium, der branchenweit einzige Anbieter von konvergentem Endpunktmanagement (XEM), führt den Paradigmenwechsel bei herkömmlichen Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an. Nur Tanium schützt jedes Team, jeden Endpunkt und jeden Arbeitsablauf vor Cyber-Bedrohungen, indem es IT, Compliance, Sicherheit und Risiko in eine einzige Plattform integriert, die umfassende Transparenz über alle Geräte hinweg, eine einheitliche Reihe von Kontrollen und eine gemeinsame Taxonomie für ein einziges gemeinsames Ziel bietet: den Schutz kritischer Informationen und Infrastruktur in großem Umfang.

Weitere Informationen zu diesen Lösungen erhalten Sie von Ihrem lokalen Tanium-Vertriebsbüro. [tanium.de](https://tanium.de)

