SOFTTAILOR

STATE OF ENDPOINT MANAGEMENT IN DACH 2025/26

info@softtailor.de
Hilpertstr. 20, 64295 Darmstadt
www.softtailor.de

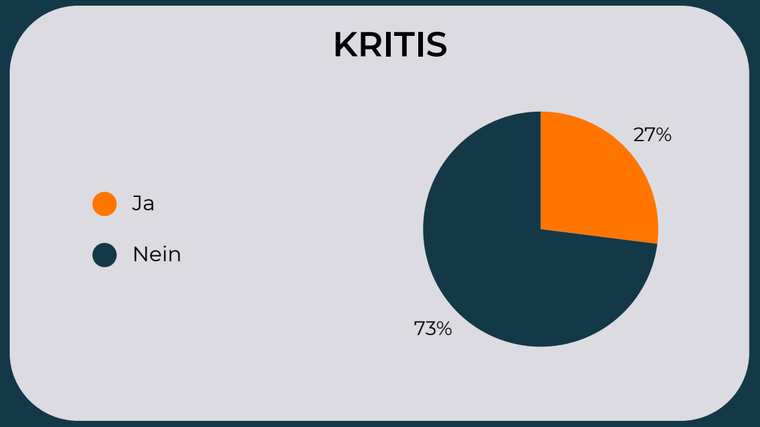
Überblick / Methodik

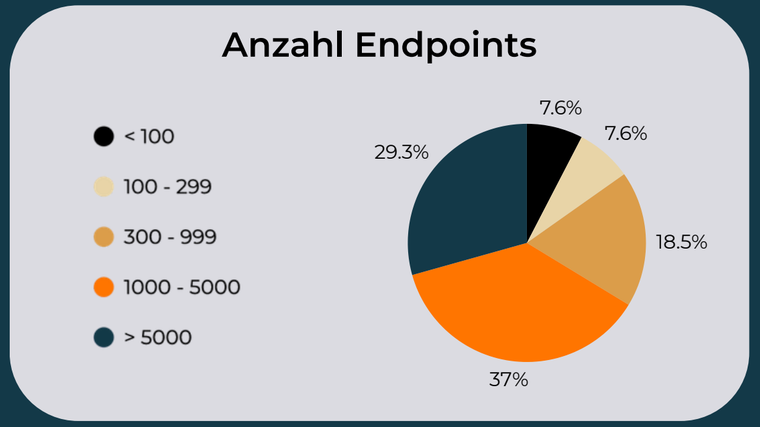
Die erste Studie zum *State of Endpoint Management* im deutschsprachigen Raum schließt eine bisher bestehende Lücke. Ziel war es, erstmals ein belastbares Bild der **Endpoint Management Realität in DACH** zu zeichnen und damit eine Grundlage für Vergleich, Einordnung und Diskussion zu schaffen.

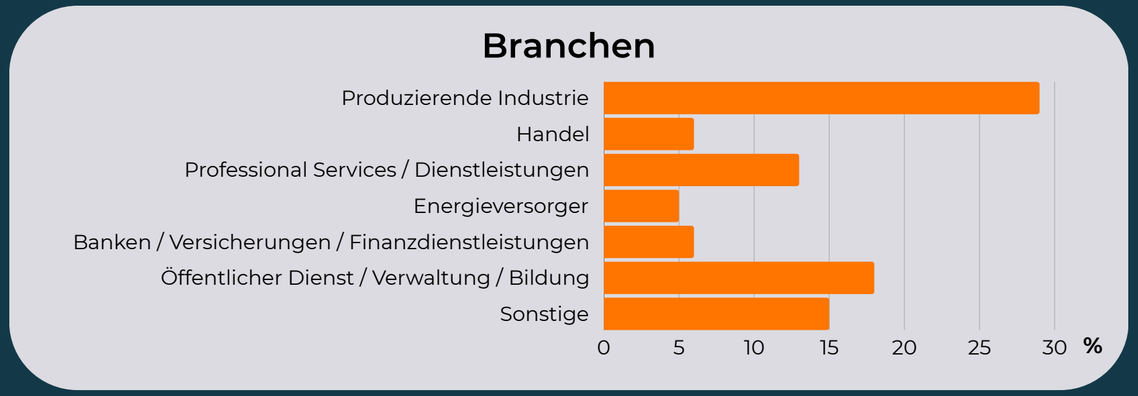
Dazu haben wir über **100 Organisationen unterschiedlichster Größen und Branchen** (Infos in den Grafiken) befragt. Die Organisationen zeigen eine große Bandbreite an Zielsystemen und verdeutlichen, wie unterschiedlich Reifegrad, Komplexität und Anforderungen im Endpoint Management ausfallen – teilweise unabhängig von Unternehmensgröße oder Branche. Dennoch gibt es deutliche Kernaussagen, die viele Organisationen gemeinsam haben!

Ein Punkt vorab: Immer wieder zeigt sich, wie stark IT-Abteilungen unter Druck stehen. Zum Zeitpunkt der Umfrage, bis in den Spätherbst 2025, waren z.B. **nur 64 % der Unternehmen vollständig auf Windows 11 migriert.**

Wir wünschen **viel Spaß und Erkenntnisse** beim Lesen der Studie!







Kernaussagen

1

In Zeiten diverser Betriebssysteme wird **Unified** Endpoint Management immer mehr zum **Vorteil.** Viele Organisationen möchten daher Ihre Anzahl an **UEM Lösungen konsolidieren.** **30 %** der Organisationen sehen sich **nicht gut** aufgestellt. **Intune** ist klarer **Marktführer.** Unklar bleibt häufig, wie Server verwaltet werden.

2

Die deutlichsten **Defizite** im Endpoint Management von DACH-Organisationen bestehen in der **Systemhärtung**, wobei Diskrepanzen in den Daten zum Patch Management vermuten lassen, dass die Selbsteinschätzung zu gut ist und insbesondere **3rd Party Patch Management** unterschätzt wird.

3

Die befragten Organisationen **wissen**, an welchen **Stellschrauben** sie zu arbeiten haben, aber **Komplexität, Zeitmangel und Verzögerungen** durch interne Diskussionen und Bürokratie **erschweren** den Weg und sind frustrierend.

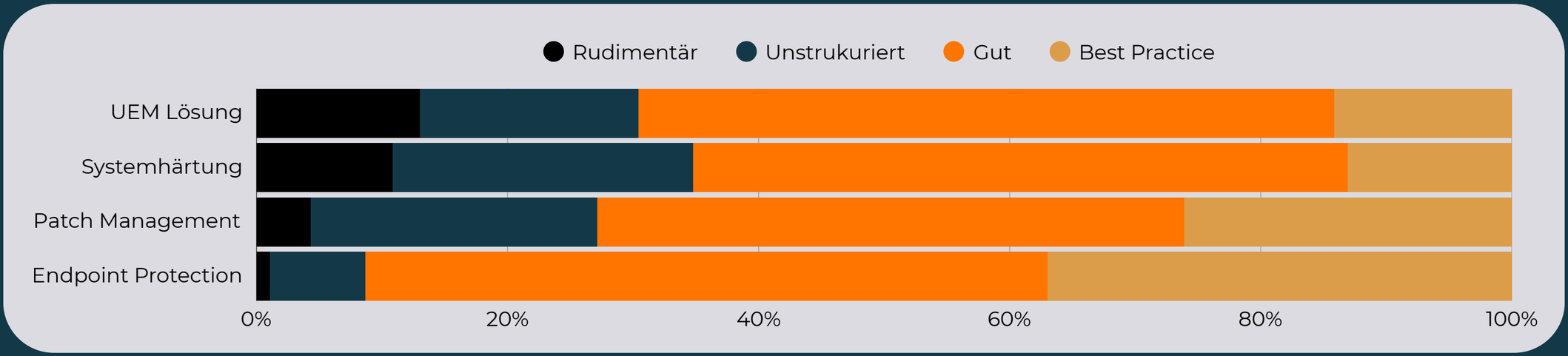
Selbsteinschätzung

Wir haben gefragt: “Wie schätzen Sie Ihre Organisation bzgl. der vier Bestandteile ganzheitlichen Endpoint Managements & Security ein?” und vier Reifegrade zur Auswahl gestellt.

Die Selbsteinschätzung offenbart **deutliche Defizite:** Je nach Kategorie ordnen sich **10–35 %** der Unternehmen den Stufen **rudimentär oder unstrukturiert** zu. Im Bereich **Patch Management** und **Endpoint Protection**, glauben wir, dass der Anteil an **Organisationen mit unzureichenden Prozessen** bei genauerem Nachfragen **noch viel höher** wäre. Hier stößt unsere Studie an Ihre Grenzen (siehe Details auf den Seiten zu Patch Management & Endpoint Protection).

Gleichzeitig sind die **Ambitionen hoch:** Für die kommenden zwölf Monate sehen sich je nach Bereich nur noch 8–14 % der Unternehmen in diesen niedrigen Reifegraden. Umgekehrt streben **86–92 % an, künftig** gut oder nach Best Practice aufgestellt zu sein.

Dies zeigt eine hohe Reflexionsfähigkeit und **klaren Willen zur Verbesserung**. Sie macht aber auch die Größenordnung des angestrebten Fortschritts sichtbar – und wirft die **Frage** auf, ob ein so umfassender **Reifegrad-Sprung innerhalb eines Jahres realistisch** umsetzbar ist.

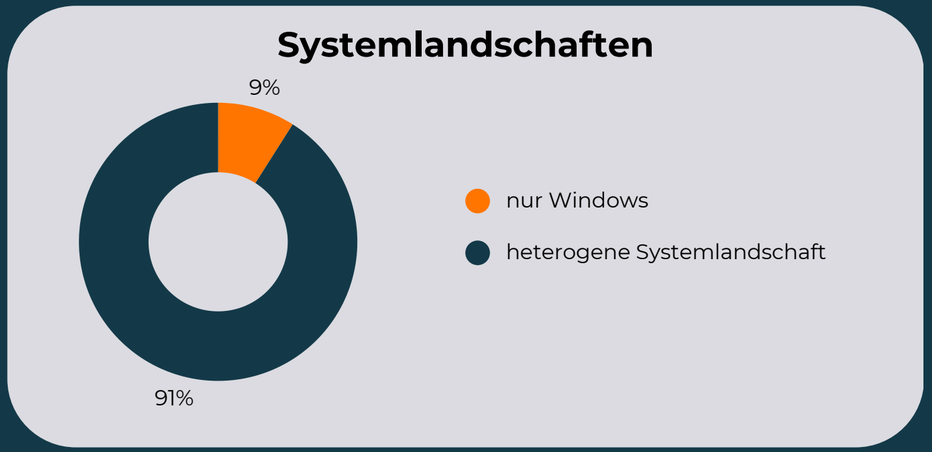


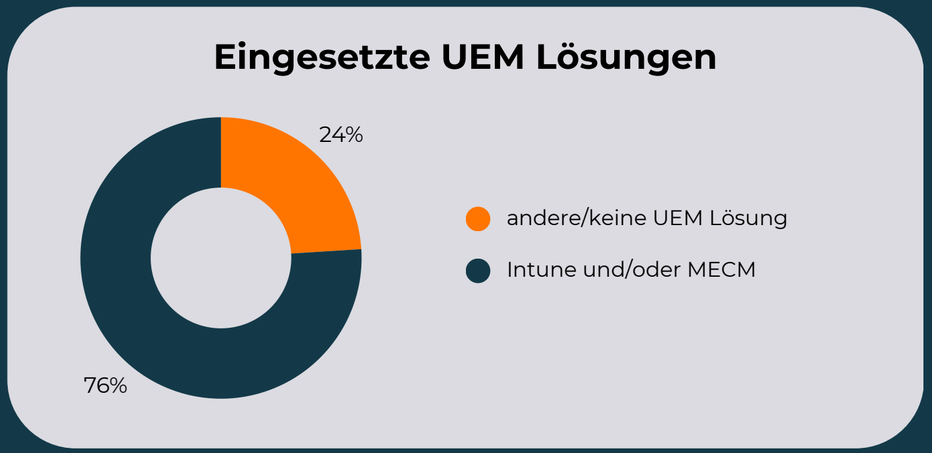
UEM Lösung

Nicht einmal 10 % der befragten Unternehmen setzen **ausschließlich** auf **Windows-Geräte.** Der geringe Anteil ausschließlicher Windows-Umgebungen überrascht kaum. In der Praxis verwalten die meisten Organisationen diverse Betriebssysteme (von Windows und mac OS, über iOS / Android bis Linux) – ein klares Zeichen für die Bedeutung von **Unified** Endpoint Management.

Wohl deshalb wollen **61 % der Organisationen**, die in den nächsten zwölf Monaten eine Migration planen, **ihre UEM-Landschaft konsolidieren** und von mehreren Lösungen auf eine zentrale Plattform umstellen. Der größte **Gewinner: Microsoft Intune.** Bereits heute ist Microsoft klarer Marktführer und wird seine Position weiter ausbauen.

Offen bleibt, wie Organisationen, die angaben, nur Intune einsetzen zu wollen, **künftig Server und hochverfügbare Systeme verwalten,** da Intune hierzu nicht fähig ist, bzw. deutliche Schwächen offenbart. Ggf. werden in diesen Fällen Client- und Servermanagement getrennt. **Auffällig:** Ehemalige **Ivanti-DSM-Nutzer** migrieren deshalb meist zu einer **Kombination aus Intune und einer ergänzenden Lösung, wie baramundi.**





Systemhärtung

35 % führen keine oder nur wenig strukturierte Systemhärtung durch

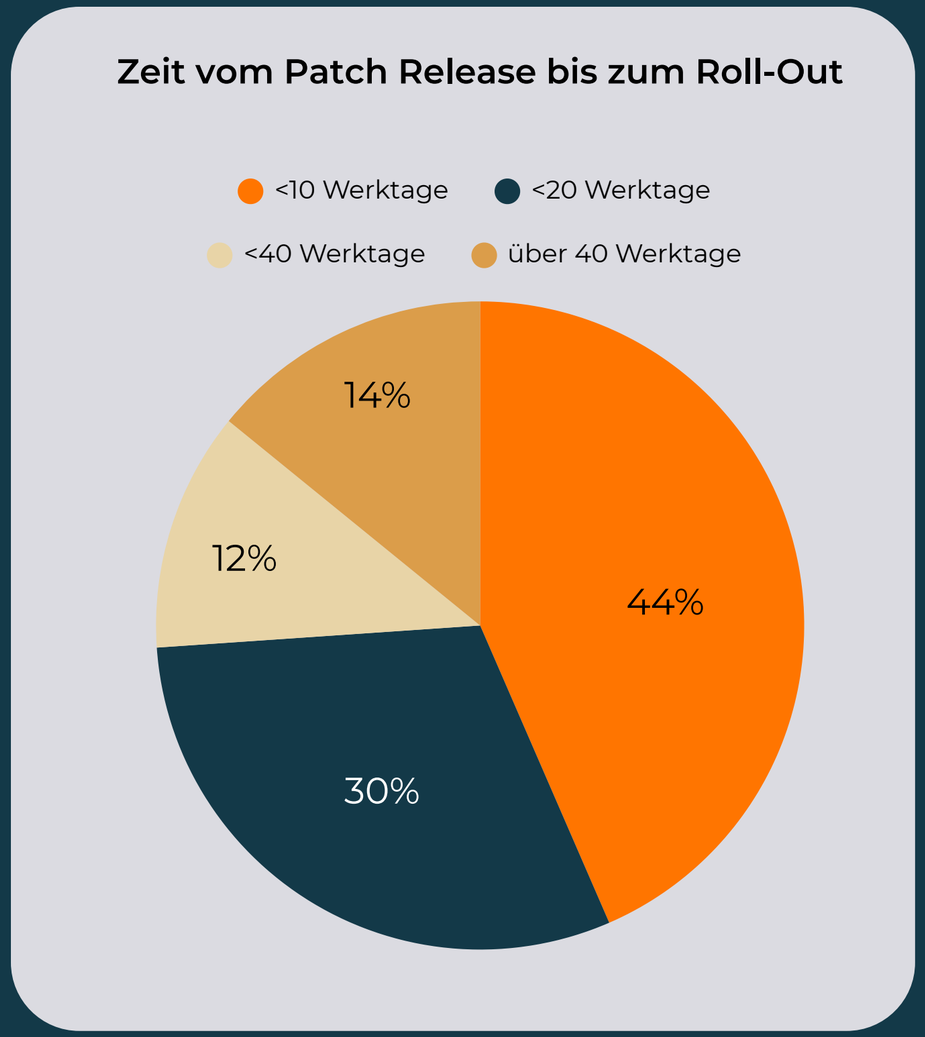
Das Ergebnis überrascht uns nicht und zeigt **dringenden Handlungsbedarf:** 35 % der befragten Unternehmen geben an, dass sie bislang keine oder nur wenig strukturierte Systemhärtung (Konfigurationsmanagement) durchführen. **Unter ihnen befinden sich auch KRITIS-Unternehmen**, bei denen man eigentlich ein höheres Sicherheitsniveau erwarten würde.

Das **wirft Fragen auf** – insbesondere im Vergleich zur recht positiven Selbsteinschätzung in anderen Bereichen. Spiegelt sich hier ein **realistisches Bewusstsein** für bestehende Lücken **oder unterschätzen** Teams die Wichtigkeit und Effektivität konsequenter Systemhärtung? Wir tippen auf Letzteres.

Noch deutlicher: Unter Organisationen, die **Microsoft 365** einsetzen**,** verfolgen **nur ca. 60 % eine dedizierte Härtung des M365 Tenants**. Ein Indiz dafür, dass - je nach Definition der Begriffe - Tenanthärtung noch mehr vernachlässigt wird, als Clienthärtung unter dem Motto: “Wir setzen Microsoft 365 aus der Cloud ein, Microsoft sorgt schon für die Sicherheit”. **Nein,** Microsoft liefert seine Produkte für größtmögliche Kompatibilität und Möglichkeiten - für restriktive Einstellungen, die die Sicherheit deutlich erhöhen, ist der Kunde selbst verantwortlich! Im Licht der **zunehmenden Bedeutung von Cloudlösungen** für Endpoint, Identity & Access Management ist das **dramatisch** und **bedarf eines Mindset-Shifts!**

Fest steht: Bei der Systemhärtung, ob Clients, Server oder Tenant haben deutsche Organisationen **deutlichen und dringenden Nachholbedarf.**

Patch Management



Die Ergebnisse zum Patch Management **überraschen uns:**

Viele IT-Abteilungen bewerten ihre Prozesse als strukturiert und regelmäßig – **74 %** geben an, einen festen Ablauf etabliert zu haben und **einen Patch in weniger als 20 oder sogar 10(!) Tagen auszurollen.**

Andere Studien zeigen **ein komplett anderes Bild:** Laut Application Management Legende Bob Kelly (*hier geht's zur Studie*) gelingt es 82 % der Organisationen nicht, ihre Windows-Applikationen innerhalb von drei Monaten vollständig zu aktualisieren. Das sehen wir auch in Gesprächen mit unseren Kunden und Organsationen im deutschsprachigen Raum.

Gründe für die Diskrepanz könnten sein:

- Unsere Fragen haben nicht in aller Deutlichkeit abgefragt, ob die Zeitangaben für **jegliche** Software (OS, OS-nah, Treiber, 3rd Party Applikationen) gelten
- Insbesondere haben wir nicht deutlich genug herausgestellt, dass wir uns explizit auch auf **3rd Party Applikationen** beziehen und nicht nur auf das **OS Patching.** Eine Unterscheidung der beiden wäre sinnvoll gewesen.

Wir sehen deshalb **mehr Handlungsbedarf**, als die Ergebnisse unserer Studie suggerieren! Insbesondere, da **58 %** der befragten Organisationen bislang **kein Tool bzw. Katalog, für das automatische Patchen von Drittanbietersoftware (wie z.B. Patch My PC)** nutzen, ohne das der Workload für kaum eine Organisation leistbar ist.

Endpoint Protection

nur 26% **der Unternehmen mit vorhandenem Vulnerability Management Tool schließen Vulnerabilities regelmäßig**

Im Bereich Endpoint Protection **schätzen sich viele Unternehmen am besten aufgestellt ein.** Oft reicht hier aber schon der flächendeckende Rollout einer EDR Lösung, wie Microsoft Defender for Endpoint, um ein positives Selbstbild zu erzeugen – **ein möglicher Trugschluss, denn man** muss regelmäßig nachjustieren **und die Daten auch nutzen:**

Unter den Organisationen, die angaben, dass Ihre Endpoint Protection Lösung eine Vulnerability Management Funktion hat, gaben **nur 26%** an, diese auch zu nutzen, **um regelmäßig und systematisch Vulnerabilities zu schließen**. Ein weiteres Indiz dafür, dass es häufig an **Kapazität fehlt**, um regelmäßige **Cyberhygiene wirklich konsequent durchzuziehen.**

Maßnahmen wie **Pentests, SOC oder SIEM** sind **weit verbreitet**, doch deutlich **weniger Aufmerksamkeit gilt dem, was passiert, wenn ein Angriff erfolgreich war** – etwa durch Incident-Response-Playbooks oder regelmäßige Drills.

Der **Endpoint Protection Reifegrad** wirkt somit auf **auf den ersten Blick hoch**, ist in vielen Fällen aber **nur oberflächlich gefestigt.**

Herausforderungen

Komplexität & Heterogenität
Endpoint-Landschaften sind stark fragmentiert: unterschiedliche Betriebssysteme, Legacy-Systeme, OT-Umgebungen und spezialisierte Plattformen treffen aufeinander. Einheitliche Steuerung und Zentralisierung stoßen dabei schnell an technische und organisatorische Grenzen.

Security-Umsetzung & Reifegrad
Sicherheitsanforderungen sind bekannt und akzeptiert, werden in der Praxis jedoch nicht immer konsequent umgesetzt. Schwachstellen-Management, Systemhärtung und 3rd Party Patch Management bleiben häufig hinter den eigenen Zielbildern zurück, da sie immer wieder Zeit und Aufmerksamkeit bedürfen.

Ressourcen & Know-How
Viele IT-Teams arbeiten am Limit. Fehlende personelle Kapazitäten und spezialisiertes Fachwissen erschweren es, Endpoint-Themen strukturiert und nachhaltig voranzutreiben. Oft bleibt wenig Raum für strategische Weiterentwicklung, da der Fokus auf dem laufenden Betrieb liegt.

“**Was brauchen wir wirklich?” & Rahmenbedingungen**
Neben technischen Fragen bremsen vor allem organisatorische Faktoren den Fortschritt. Budgetrestriktionen, unzählige Buzzwords & Tools, interne Diskussionen und fehlende Entscheidungsgrundlagen verzögern Maßnahmen und erschweren eine klare Endpoint-Strategie.

Welche Endpoint Management & Security Herausforderungen beschäftigen Sie momentan am meisten?

“Zu viel Impact, zu wenig Personal”
“Mangel an Personalressourcen”
“Personalmangel“

“Generationenprobleme. Meinungsverschiedenheiten zwischen Cloud und On-Prem Lösungen. Die Diskussionen verzögern alles.”

“In der OT sind viele verschiedene Systeme im Einsatz - von WinXp über WinCE bis Win11 LTSC/IoT. Diese Systeme alle mit einem Tool zu managen scheint unmöglich.”

“Kompatibilität von MS Defender mit anderen Platformen”
“Schlangenöl von guten Lösungen zu unterscheiden”

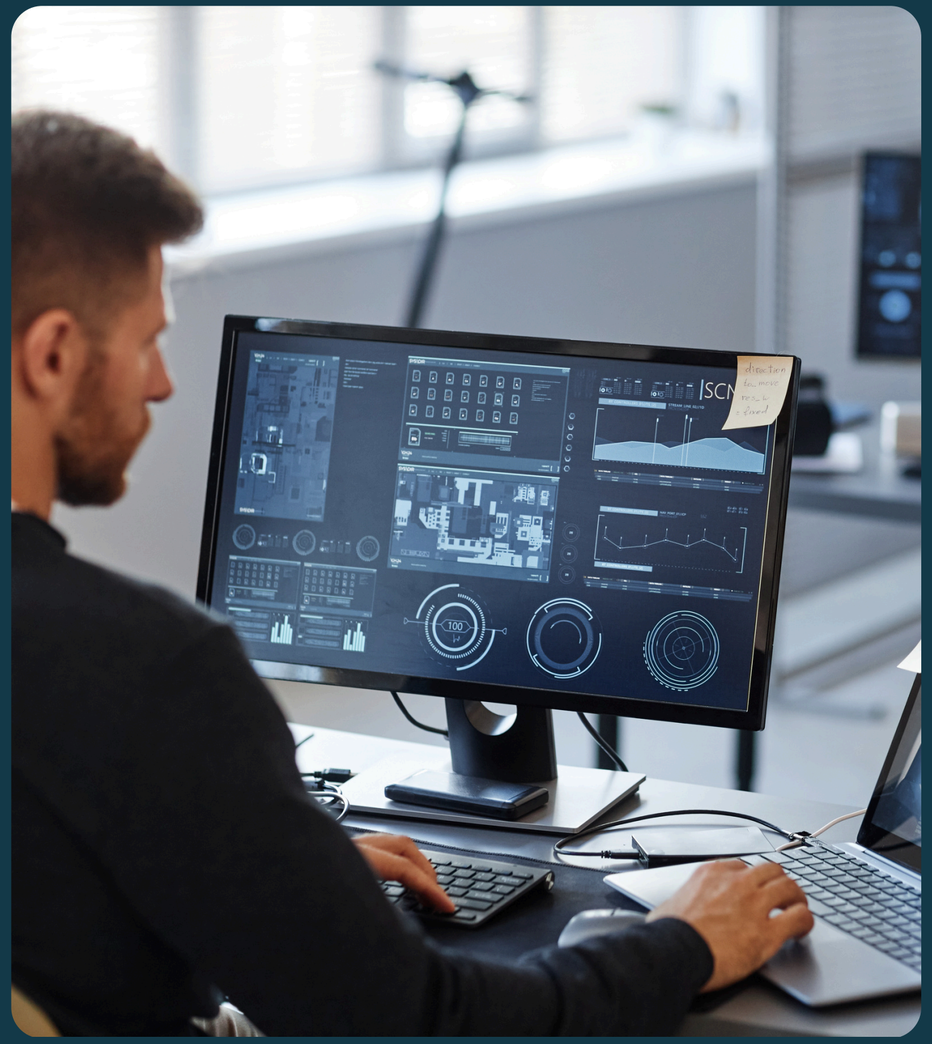
Fazit

Endpoint Management & Security in DACH ist ein Balanceakt zwischen wachsender technischer **Komplexität**, steigenden **Sicherheitsanforderungen** und begrenzten **Ressourcen**.

Die **Herausforderungen sind erkannt** – doch der Weg zur nachhaltigen Umsetzung bleibt anspruchsvoll. Viele Organisationen kennen ihre Schwachstellen sehr genau. Was häufig **fehlt, sind Orientierung und Kapazität inmitten von Buzzwords und unzähligen Tools.**

Es braucht **klare Prioritäten, standardisierte Prozesse und ausreichend Kapazitäten**, um diese Themen konsequent voranzutreiben und im Tagesgeschäft dranzubleiben. Gleichzeitig wird der Druck weiter steigen – durch regulatorische Anforderungen, zunehmende Bedrohungsszenarien und den Trend zur Nutzung diverser Betriebssysteme.

Für IT-Abteilungen bedeutet das: **Komplexitätsreduktion** steht **bei der Konzeptionierung** von Endpoint Management & Security an erster Stelle. In der Umsetzung geht es um **größtmögliche Automatisierung ohne Kontrollverlust**, um Endpoint Management & Security dann **tagtäglich** leben zu können. Insellösungen, manuelle Prozesse und gewachsene Tool-Landschaften sind langfristig nicht mehr tragfähig. Entscheidend wird sein, Komplexität zu reduzieren und vorhandene Sicherheitsfunktionen konsequent zu nutzen, anstatt das nächste Tool anzuschaffen.



Über SOFTTAILOR

Organisationen **kennen** die Kernthemen, Ihre Defizite und die relevanten Technologien in Endpoint Management & Security. Es **fehlt jedoch an Orientierung und Kapazität**, sich zuerst richtig Gedanken zu machen und dann umzusetzen.

Seit unserer Gründung im Jahr 2007 **begleiten wir Organisationen** täglich bei der Weiterentwicklung ihrer Endpoint-Strategie. Als **Spezialist für Endpoint Management & Security** mit klarem Fokus auf Intune, Microsoft Endpoint Configuration Manager (SCCM/MECM) und Baramundi unterstützen wir bei Migrationen, der nachhaltigen Modernisierung und dem Betrieb von Endpoint Management & Security Lösungen für Organisationen mit bis zu 25.000 Endgeräten.

Wir helfen, Komplexität zu reduzieren, Sicherheitsniveaus messbar zu erhöhen und Automatisierung gezielt auszubauen. Dabei verbinden wir strategische Beratung mit technischer Umsetzung – praxisnah, strukturiert und mit tiefem Verständnis für die typischen Herausforderungen von IT-Abteilungen größerer Organisationen.

Auch bei SOFTTAILOR: Softwarepaketierung aaS

Mit Softwarepaketierung fing alles an. Seit 2007 eine Kernkompetenz von SOFTTAILOR. Eure Experten für Softwarepaketierung mit PSADT.

- Individuelle Softwarepakete mit Qualität Made in Germany
- Einfacher Prozess für Onboarding, Paket-Request und Abstimmung
- Ideal als Ergänzung zu Patch My PC

Ergebnisse einordnen & nächste Schritte klären

Ihr möchtet wissen, was die Studienergebnisse konkret für eure Endpoint Strategie bedeuten? Sprich mit unseren Experten für Endpoint Management.

Jetzt unverbindlichen Termin vereinbaren