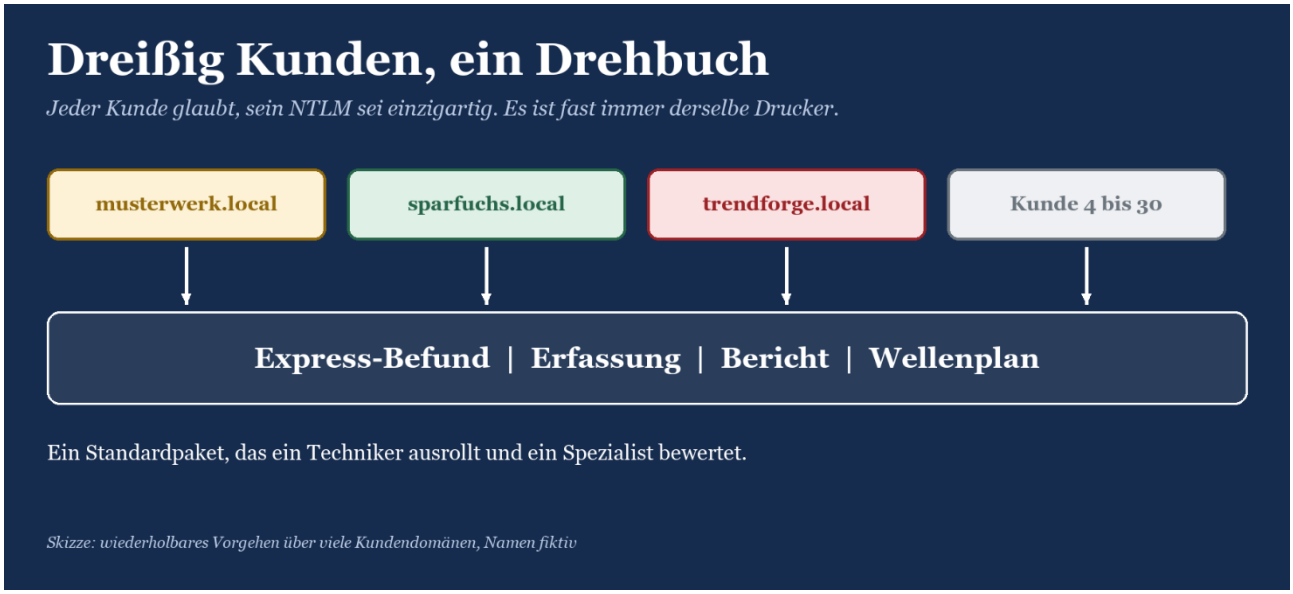
NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen



WISSEN
Wie der NTLM Diagnostiker rein lesend zeigt, wo in einer Kundendomäne noch NTLM läuft und warum.
› **NTLM Diagnostiker**

BERATUNG
Standardpaket, Rollen und Abrechnungsmodell für dein Systemhaus gemeinsam aufsetzen.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Onboarding für dein Technikerteam: Befund, Erfassung und Bericht sicher beim Kunden durchführen.
› **Schulung zum NTLM Diagnostiker**

Wenn du in einem Systemhaus arbeitest, kennst du das Gefühl: Microsoft kündigt etwas an, und am nächsten Morgen klingeln dreißig Telefone gleichzeitig. Jeder Kunde will wissen, ob er betroffen ist, was das kostet und warum du ihm das nicht schon letztes Jahr gesagt hast. Bei der NTLM-Ablösung ist es genauso, nur dass diesmal nicht ein Patch die Antwort ist, sondern ein Projekt. Pro Kunde. Mal dreißig.

Der Druck ist real. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, gesteuert über den Registrierungswert BlockNtlmv1SSO und sichtbar in den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, damit Kerberos auch ohne direkte Sichtverbindung zum Domänencontroller funktioniert. Und mit der nächsten Windows-Server-Version ist NTLM in Phase 3 standardmäßig abgeschaltet. Den kompletten Zeitplan findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Dieser Beitrag richtet sich an Systemhäuser und Managed Service Provider, an Technikerinnen und Techniker im Außendienst und an alle, die die NTLM-Ablösung nicht einmal, sondern immer wieder machen müssen. Es geht um ein wiederholbares Vorgehen, ein Standardpaket, das du jedem Kunden anbieten kannst, um saubere Abrechnung und um die Frage, wer in deinem Team was tut. Spoiler: Wenn jeder Kunde ein Einzelstück wird, verdienst du an der NTLM-Ablösung genau nichts.

FAKTEN · Die Lage für Systemhäuser auf einen Blick

NTLMv1 ist seit dem Update vom 13.10.2026 auf Windows 11 ab 24H2 und Windows Server 2025 für

Single Sign-on standardmäßig blockiert (BlockNtlmv1SSO, Ereignisse 4024 und 4025). Wer bei Kunden alte NAS-Systeme, Scanner oder Fachanwendungen betreut, bekommt die ersten Tickets bereits jetzt.

Das erweiterte NTLM-Auditing nach Microsoft KB5064479 schreibt ins Protokoll Microsoft-Windows-NTLM/Operational: 4020 bis 4023 auf Clients und Servern, 4030 bis 4033 auf Domänencontrollern, jeweils mit einer Reason ID von 0 bis 11. Verfügbar ab Windows 11 24H2 und Windows Server 2025 sowie auf Windows Server 2022 und 2019 mit den Updates ab 13.10.2026.

Ältere Systeme liefern nur die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004, ohne Ursache. In typischen Mittelstandsdomänen hast du beides gleichzeitig.

Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Jeder Kunde, der bis dahin keinen Plan hat, wird zum Notfall. Notfälle skalieren schlecht.

Warum Systemhäuser ein Vorgehen brauchen, nicht dreißig

Eine einzelne Firma kann sich die NTLM-Ablösung als Handwerksprojekt leisten: ein engagierter Administrator, ein paar Wochen Ereignisanzeige, viel Kaffee. Ein Systemhaus kann das nicht. Wenn jeder Techniker bei jedem Kunden anders vorgeht, bekommst du dreißig verschiedene Excel-Tabellen, dreißig verschiedene Wahrheiten und einen Spezialisten, der abends heimlich weint.

Die Kundschaft ist verschieden, die Ursachen sind es nicht

Das Schöne an NTLM ist seine Langweiligkeit. Die Gründe, warum Windows nicht Kerberos benutzt, wiederholen sich bei fast jedem Kunden: Zugriffe per IP-Adresse, fehlende oder doppelte Service Principal Names, lokale Konten, Geräte ohne Kerberos-Unterstützung, Anwendungen mit fest eingebautem NTLM. Microsoft liefert für genau diese Fälle die Reason IDs 0 bis 11, die im Ereignistext als „Reason ID“ stehen. Was sie bedeuten, erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

Drei typische Kunden aus deinem Portfolio, fiktiv, aber du erkennst sie trotzdem:

Kunde	Umgebung	Typische NTLM-Quellen	Erste Einschätzung
Musterwerk GmbH	180 Clients, 2 DCs Server 2022, Produktion mit Altrechnern	Maschinensteuerungen per IP-Pfad, Scanner, ERP-Dienstkonto	Gelb: viel Arbeit, aber planbar
Sparfuchs & Partner Steuerberatungs GmbH	35 Clients, 1 DC Server 2025, DMS, Kanzleisoftware	Multifunktionsgerät, ein altes NAS	Grün: überschaubar
Trendforge Digital GmbH	90 Clients, gemischte Server 2016 bis 2025, viele Entwicklersysteme	NTLMv1 von einem Build-Server, doppelte SPNs, lokale Konten	Rot: NTLMv1 aktiv, Blockade droht

Drei Kunden, drei Größen, drei Ampelfarben. Aber das Vorgehen ist bei allen gleich: messen, Ursachen bestimmen, berichten, in Wellen abschalten. Genau das macht es zum Produkt.

Was ein Standardpaket für dich leistet

- **Kalkulierbarkeit:** Du weißt vorher, wie lange jeder Schritt dauert, und kannst Festpreise anbieten.
- **Delegierbarkeit:** Techniker führen aus, ohne jedes Mal den Spezialisten zu fragen.
- **Vergleichbarkeit:** Gleiche Berichtsgliederung bei jedem Kunden, gleiche Kennzahlen, gleiche Sprache gegenüber Geschäftsführungen.

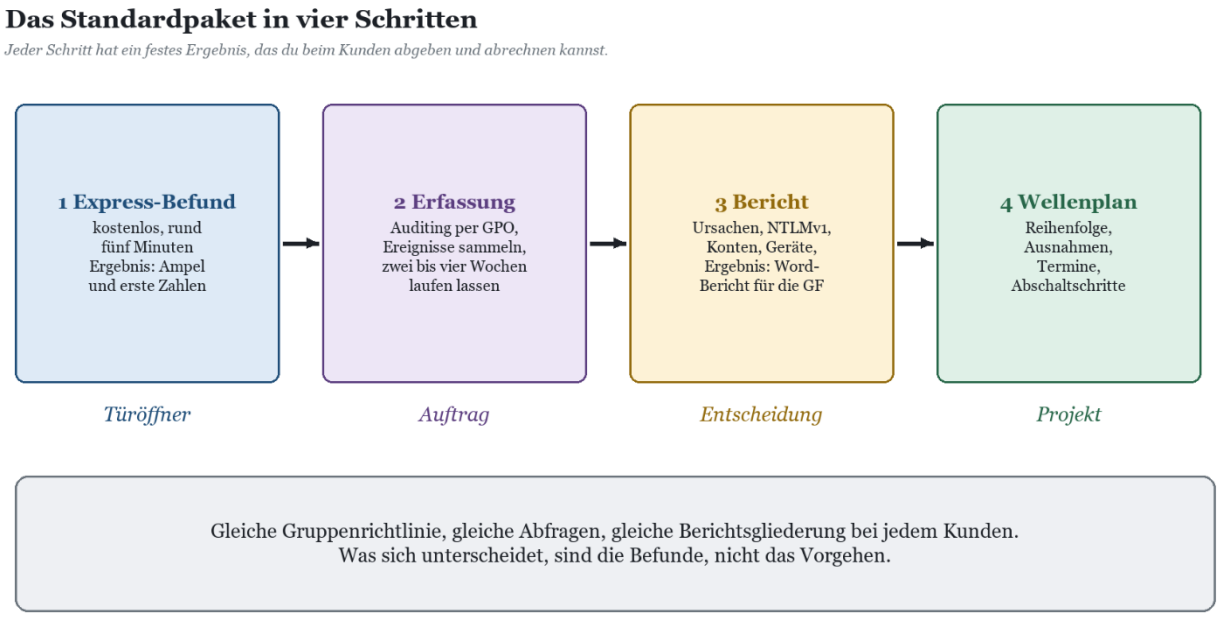
- **Lernkurve:** Die zehnte Ursache „Scanner schreibt per IP-Adresse“ behebst du in fünf Minuten, weil du sie neunmal dokumentiert hast.

WARNUNG · Der teuerste Satz im Systemhaus

„Das schauen wir uns beim Kunden mal an.“ Ohne festes Vorgehen wird aus „mal anschauen“ eine offene Aufwandsposition, die der Kunde nicht versteht und du nicht durchsetzt. Am Ende hast du drei Tage Ereignisanzeige verschenkt und der Kunde fragt, warum der Drucker immer noch geht.

Das Standardpaket: Express-Befund, Erfassung, Bericht, Wellenplan

Das Paket besteht aus vier Schritten mit jeweils einem klaren Ergebnis. Jeder Schritt ist für sich abrechenbar, und der Kunde kann nach jedem Schritt entscheiden, ob er weitergeht. Das nimmt den Druck aus dem Erstgespräch: Du verkaufst kein Projekt, sondern eine Antwort.



Skizze: Standardpaket für die NTLM-Ablösung beim Kunden

Schritt 1: der Express-Befund als Türöffner

Der erste Termin sollte kurz, konkret und für den Kunden risikolos sein. Mit Bordmitteln heißt das: Du meldest dich an einem Domänencontroller an und schaust, was das Protokoll schon hergibt. Auf aktuellen Systemen ist das erweiterte NTLM-Auditing nach KB5064479 standardmäßig aktiv, auf älteren findest du bestenfalls die Ereignisse 8001 bis 8004, sofern jemand die Überwachung jemals eingeschaltet hat.

```
# Auf dem DC: die letzten 20 NTLM-Ereignisse der Domäne als Text
wevtutil qe Microsoft-Windows-NTLM/Operational /q:"*[System[(EventID=4030 or EventID=4031)]]"
/c:20 /rd:true /f:text

# NTLMv1 im Blick behalten (Blockade für Single Sign-on)
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-NTLM/Operational'; Id=4024,4025} -
MaxEvents 50 |
  Select-Object TimeCreated, Id, MachineName
```

Das ist ehrlich und für einen ersten Eindruck brauchbar. Es ist aber kein Befund, den du einer Geschäftsführung vorlegen kannst. Du siehst Ereignisse, keine Zusammenhänge, und du siehst nur

das, was auf diesem einen Domänencontroller angekommen ist. Wie du die Nutzung systematisch ermittelst, beschreibt NTLM-Nutzung ermitteln: der komplette Leitfaden.

Schritt 2: Erfassung über zwei bis vier Wochen

Für belastbare Aussagen brauchst du die Ereignisse von Domänencontrollern, Servern und, wo möglich, Clients, über einen Zeitraum, der Monatsabschluss, Backupfenster und den einen Kollegen einschließt, der nur dienstags kommt. Dazu verteilst du die Audit-Einstellungen per Gruppenrichtlinie. Damit das bei jedem Kunden gleich aussieht, nimm ein Skript statt Klickarbeit, etwa das NTLM-Audit-GPO-Skript. Die Einzelschritte stehen in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt.

Gesammelt wird entweder direkt auf den Domänencontrollern, über einen Windows Event Collector oder per Direktabfrage. Für Kunden mit mehr als einer Handvoll Server lohnt sich Windows Event Forwarding, siehe NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding. Und dann gibt es noch die Geräte, die gar nichts protokollieren: NAS, Drucker, Scanner. Die siehst du nur indirekt am Ziel oder im Mitschnitt, mehr dazu in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

> **TIPP · Abdeckung zuerst, Auswertung danach**
>
> Bevor du Ereignisse auswertest, prüfe, wer überhaupt liefert. Ein Server ohne Ereignisse ist nicht NTLM-frei, sondern vielleicht nur stumm, weil die GPO nicht greift, das Update fehlt oder das Protokoll zu klein ist. Bei dreißig Kunden ist „stumm“ der häufigste Grund für falsche Entwarnung.

> **WICHTIG · Datenschutz vor dem ersten Ereignis klären**
>
> NTLM-Ereignisse enthalten Kontennamen und Rechnernamen, also personenbezogene Daten. Nimm eine kurze Zweckbeschreibung und Löschfrist in deinen Standardvertrag auf und kläre beim Kunden, ob ein Betriebsrat einzubinden ist. Details stehen in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Schritt 3: der Bericht

Jetzt wird es mit Bordmitteln zäh. Ein Kunde wie die Musterwerk GmbH produziert in drei Wochen schnell Zehntausende NTLM-Ereignisse. Die musst du deduplizieren, nach Quelle, Ziel und Konto gruppieren, die Reason ID aus dem Meldungstext ziehen und für jede Ursache prüfen, ob es den SPN gibt und ob der Name im DNS auflösbar ist.

```
# Reason ID aus dem Meldungstext ziehen und zählen
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-NTLM/Operational'; Id=4020,4021} |
  ForEach-Object { if ($_.Message -match 'Reason ID:\s*(\d+)') { $Matches[1] } } |
  Group-Object | Sort-Object Count -Descending

# Für jeden Verdacht von Hand gegenprüfen
setspn -Q cifs/fileserver01.musterwerk.local
setspn -X              # doppelte SPNs in der Domäne
Resolve-DnsName fileserver01.musterwerk.local
```

Bei einem Kunden ist das ein langer Nachmittag. Bei dreißig Kunden ist es ein Vollzeitjob, und zwar einer, bei dem jede Kollegin und jeder Kollege eine leicht andere Variante des Skripts pflegt. Spätestens hier lohnt sich der Blick auf NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

Der Bericht selbst sollte bei jedem Kunden dieselbe Gliederung haben: Zusammenfassung mit Ampel, NTLMv1-Befunde, Ursachen nach Häufigkeit, betroffene Konten und Systeme, Geräte ohne Protokoll, Empfehlung und Wellenplan. Die Geschäftsführung liest Seite eins. Die IT-Leitung liest den Rest. Und du hast etwas, das du in zwei Jahren wieder aus der Schublade holen kannst.

Schritt 4: der Wellenplan

Der Wellenplan übersetzt den Bericht in Termine. Welle 1 räumt die Hausaufgaben ab: IP-Pfade auf DNS-Namen umstellen (siehe NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen), fehlende SPNs setzen, Dienstkonten bereinigen. Welle 2 kümmert sich um Anwendungen und Hersteller, Welle 3 um die restlichen Ausnahmen und das Verweigern. Jede Welle beginnt mit Überwachen und endet mit Beobachten. Wie das konkret ohne Ausfälle gelingt, steht in NTLM schrittweise abschalten, ohne dass etwas ausfällt, und wie du Ausnahmen pflegst, ohne dass sie ewig bleiben, in Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

Wo das Standardpaket mit Bordmitteln an seine Grenzen kommt

Aufgabe	Bordmittel	Wo es bei vielen Kunden hakt
Erster Eindruck	Ereignisanzeige, wevtutil	nur ein DC, keine Zusammenfassung, nichts vorzeigbar
Auditing einrichten	Gruppenrichtlinien, Skript	gut skriptbar, aber Abdeckung bleibt unklar
Ereignisse sammeln	WEF, Get-WinEvent	Tausende Ereignisse, Duplikate, unterschiedliche Formate
Ursache bestimmen	Reason ID, setspn, Resolve-DnsName	Handarbeit pro Verdacht, Spezialwissen nötig
Stille Geräte	Wireshark	Mitschnitt deuten kostet Zeit, nicht jeder Techniker kann es
Bericht	Excel, Word von Hand	jedes Mal anders, schwer vergleichbar, teuer
Abschalt-Folgen	Restrict-NTLM im Überwachungsmodus	Wochen warten, bevor du etwas weißt

Genau an dieser Stelle setzt der NTLM Diagnostiker an. Er nimmt dir nicht das Denken ab, aber das Zusammensuchen: Er liest die Ereignisse direkt vom Domänencontroller, über einen Windows Event Collector oder per Direktabfrage, verdichtet sie und bestimmt die Ursache mit einer eingebauten SPN- und DNS-Prüfung. Und er arbeitet ausschließlich lesend. Das ist beim Kunden mehr wert, als es klingt: Du musst niemandem erklären, warum dein Werkzeug Änderungen am Domänencontroller vornimmt, weil es keine vornimmt.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Das Standardpaket mit dem Diagnostiker

Express-Befund: Die kostenlose Edition Express liefert einen Fünf-Minuten-Befund mit Readiness-Ampel. Das ist dein Türöffner beim Erstgespräch: Du zeigst dem Kunden in seiner eigenen Domäne, wo er steht, statt ihm Folien über Microsofts Fahrplan vorzulesen.

Erfassung: Der Abdeckungsmonitor und die OS-Landkarte zeigen, welche Systeme Ereignisse liefern und welche schweigen. Ereignisquellen sind DC direkt, Windows Event Collector oder Direktabfrage.

Auswertung: Die Ursachen-Engine prüft SPN und DNS, die NTLMv1-Hitliste zeigt, wer von der Blockade betroffen ist, Kommunikationsmatrix und Konten-Sicht zeigen, wer mit wem und unter welchem Konto spricht. Sicherheitsflaggen markieren riskante Befunde. Für stille Geräte gibt es den Wireshark-Import.

Bericht und Plan: Die Abschalt-Simulation zeigt, was beim Verweigern ausfallen würde. Der Word-

Bericht und der Excel- oder CSV-Export liefern dir die einheitliche Grundlage für jeden Kunden.

Lizenz: pro aktivem Computerkonto, je Endkunde mit Partnervermerk. Für die eigene Domäne deines Systemhauses ist der Diagnostiker kostenlos. Der Testzeitraum beträgt 7 Tage.

Rollenverteilung: Techniker und Spezialist

Der häufigste Fehler im Systemhaus ist, die NTLM-Ablösung komplett dem einen Kollegen zu geben, der „das mit Kerberos“ versteht. Der ist dann bei Kunde drei ausgebucht, bei Kunde sieben im Burn-out und bei Kunde zwölf bei der Konkurrenz. Besser ist eine klare Trennung: Techniker liefern Daten und beheben die einfachen Fälle, Spezialisten bewerten und entscheiden.

Wer macht was: Techniker und Spezialist

Der Techniker sorgt für Daten, der Spezialist für Urteile. Beide brauchen dieselbe Sicht.



Faustregel: ein Spezialist kann mehrere Techniker und damit viele Kunden parallel begleiten.

Skizze: Rollenverteilung im Systemhaus, vereinfacht

Was der Techniker beim Kunden erledigt

Der Techniker ist der, der ohnehin regelmäßig beim Kunden ist oder per Fernwartung draufschaut. Er führt den Express-Befund aus, verteilt die Audit-Gruppenrichtlinie, bindet die Ereignisquellen an und prüft nach ein paar Tagen, ob alle Systeme liefern. Die einfachen Ursachen behebt er gleich mit: ein Laufwerk, das per IP-Adresse verbunden ist, ein fehlender DNS-Eintrag, ein Scan-Ziel, das auf den alten Servernamen zeigt.

Was der Spezialist für alle Kunden übernimmt

Der Spezialist sitzt zentral und betreut mehrere Techniker. Er deutet doppelte SPNs, bewertet Dienstkonten, formuliert Herstelleranfragen (siehe Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen), bewertet die Abschalt-Simulation und nimmt den Bericht ab, bevor er zum Kunden geht. Für Kerberos-Fragen, die über NTLM hinausgehen, ist der Kompetenzbereich Microsoft Kerberos die passende Grundlage.

Aufgabe	Techniker	Spezialist	Kunde
Express-Befund durchführen	führt aus	sichtet Ergebnis	gibt Zugang

Audit-GPO verteilen	führt aus	gibt Vorlage frei	stimmt zu
Abdeckung prüfen	führt aus	eskaliert Lücken	-
Einfache Ursachen beheben	führt aus	-	informiert
SPN-Konflikte, Dienstkonten	liefert zu	bewertet, entscheidet	-
Herstelleranfragen	sammelt Daten	formuliert	versendet oder beauftragt
Bericht	liefert Daten	schreibt Empfehlung	nimmt ab
Wellenplan und Abschaltung	setzt um	plant	entscheidet, gibt frei

TIPP · Onboarding statt Heldentum

Ein Techniker, der das Standardpaket einmal unter Anleitung durchgezogen hat, schafft den nächsten Kunden allein. Plane deshalb ein strukturiertes Onboarding für dein Team ein, etwa mit der Schulung zum NTLM Diagnostiker. Das ist günstiger als der dritte Spezialist, den du ohnehin nicht findest.

Wie Zeitplan, Rollen und Aufwand innerhalb eines einzelnen Kundenprojekts aussehen, beschreibt ausführlich NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand. Hier geht es um die Ebene darüber: wie du dieses Projekt dreißigmal machst, ohne dass es dreißigmal anders wird.

Abrechnung beim Kunden: vom Festpreis bis zur Lizenz

Kunden kaufen ungern „NTLM“. Sie kaufen Ruhe, Sicherheit und die Gewissheit, dass am Tag nach dem nächsten Windows-Update noch gedruckt wird. Dein Angebot sollte deshalb Ergebnisse verkaufen, nicht Stunden. Das Standardpaket macht das leicht, weil jeder Schritt ein greifbares Ergebnis hat.

Pakete statt offener Aufwandspositionen

Baustein	Ergebnis für den Kunden	Abrechnungsmodell	Wer liefert
Express-Befund	Ampel und erste Zahlen in der eigenen Domäne	kostenlos oder Pauschale als Erstgespräch	Techniker
Erfassung	vollständige Datenbasis über zwei bis vier Wochen, Abdeckung geprüft	Festpreis nach Größe der Umgebung	Techniker
Bericht	Word-Bericht mit Ursachen, NTLMv1, Konten, Empfehlung	Festpreis	Spezialist
Wellenplan	Reihenfolge, Termine, Ausnahmen, Abschaltschritte	Festpreis oder Teil des Berichts	Spezialist
Umsetzung	Ursachen beheben, Wellen fahren, beobachten	Aufwand oder Kontingent	Techniker und Spezialist
Laufende Kontrolle	regelmäßige Messung, neue NTLM-Quellen erkennen	im Managed-Service-Vertrag	Techniker

Die Größe der Umgebung bestimmt den Preis, nicht die Laune des Tages. Die Zahl der aktiven Computerkonten ist dafür eine gute Kennzahl: Sie ist für den Kunden nachvollziehbar, du kannst sie messen, und sie passt zur Lizenzierung des Diagnostikers.

Lizenz je Endkunde mit Partnervermerk

Der Diagnostiker wird pro aktivem Computerkonto lizenziert. Im Systemhaus läuft das je Endkunde: Die Lizenz gehört zur Domäne des Kunden und trägt einen Partnervermerk, der dich als betreuendes Systemhaus ausweist. Du kannst sie damit sauber als eigene Position im Angebot ausweisen oder in deine Paketpreise einrechnen. Für deine eigene Domäne ist der Diagnostiker kostenlos, sodass du das Vorgehen intern üben kannst, bevor du zum ersten Kunden fährst.

FAKTEN · Lizenzierung für Systemhäuser kompakt

Express: kostenlos, Fünf-Minuten-Befund mit Readiness-Ampel. Ideal fürs Erstgespräch.

Testzeitraum: 7 Tage mit vollem Funktionsumfang, passend für eine erste Erfassung.

Lizenz: pro aktivem Computerkonto, je Endkunde mit Partnervermerk.

Eigene Domäne des Systemhauses: kostenlos.

Mandantenfähigkeit, also mehrere Kundendomänen in einer gemeinsamen Oberfläche, ist geplant, aber derzeit nicht vorhanden. Bis dahin arbeitest du je Kunde mit einer eigenen Installation.

WARNUNG · Keine Zusagen auf Funktionen, die es noch nicht gibt

Anwendungskatalog, Ausnahmelisten- und Skript-Generator, Phasenplan, Kerberos-Gegencheck und Verlauf stehen auf der Liste der geplanten Ausbaustufen. Verkaufe sie deinem Kunden nicht als vorhanden. Wer heute etwas verspricht, das erst morgen kommt, hat übermorgen ein Gespräch mit dem Einkauf.

Der Express-Befund im Erstgespräch

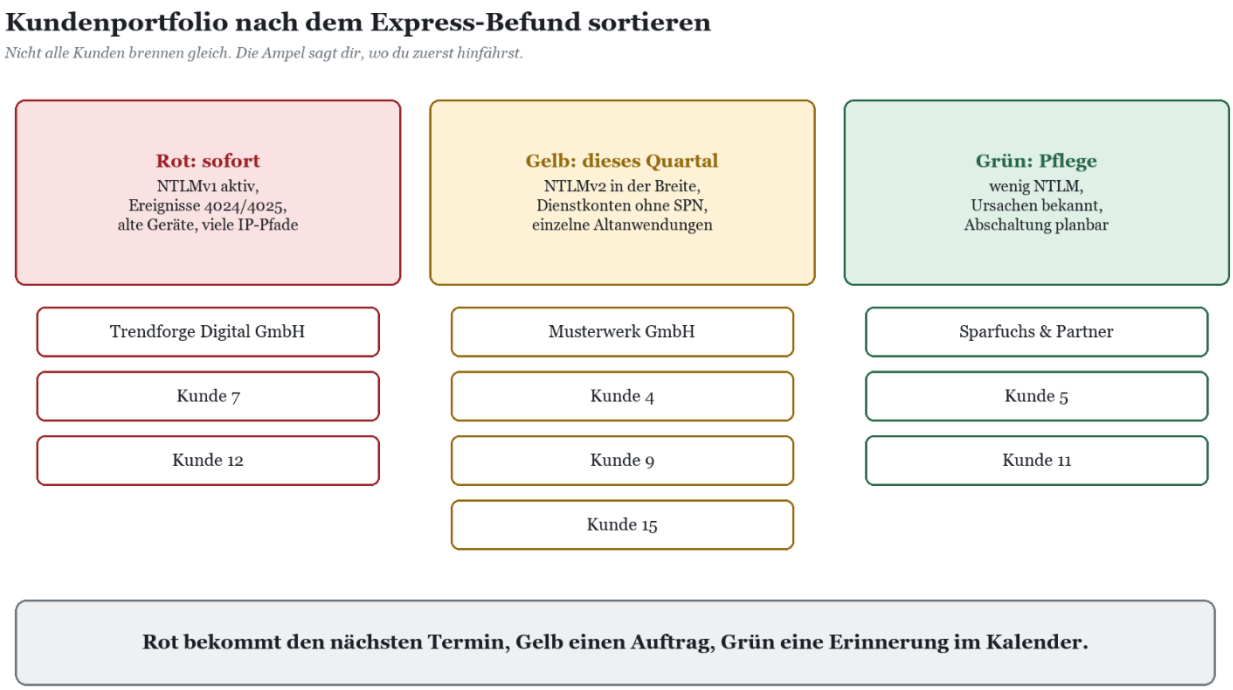
Der Express-Befund ist der ehrlichste Vertriebsweg, den es gibt: Du verkaufst nichts, du zeigst etwas. Fünf Minuten in der Domäne des Kunden, und auf dem Bildschirm steht eine Ampel. Ist sie grün, freut sich der Kunde, und du hast Vertrauen gewonnen. Ist sie rot, musst du nichts mehr erklären. Ist sie gelb, und das ist sie meistens, hast du den perfekten Einstieg in Schritt 2.

AUS DER PRAXIS · Ein Erstgespräch bei der Trendforge Digital GmbH

Der Geschäftsführer hatte zwanzig Minuten. Nach fünf stand die Ampel auf Rot, und die NTLMv1-Hitliste zeigte einen Build-Server, der seit Jahren mit NTLMv1 auf eine Dateifreigabe zugreift. Seit dem Update vom 13.10.2026 hätte dieser Zugriff beim nächsten Neustart des Clients auf Windows 11 24H2 Probleme machen können. Die restlichen fünfzehn Minuten ging es nicht mehr um das Ob, sondern um das Wann. Das Angebot für die Erfassung war am selben Nachmittag unterschrieben.

Vom Einzelkunden zum Portfolio: priorisieren und staffeln

Wenn du dreißig Kunden hast, kannst du nicht alle gleichzeitig angehen. Musst du auch nicht. Der Express-Befund liefert dir für jeden Kunden eine Ampel, und aus dreißig Ampeln wird eine Prioritätenliste. Rot zuerst, weil dort NTLMv1 bereits heute Ärger macht. Gelb danach, weil dort die meiste Arbeit liegt. Grün zuletzt, aber nicht vergessen.



Skizze: Priorisierung mehrerer Kunden nach Readiness-Ampel, Namen fiktiv

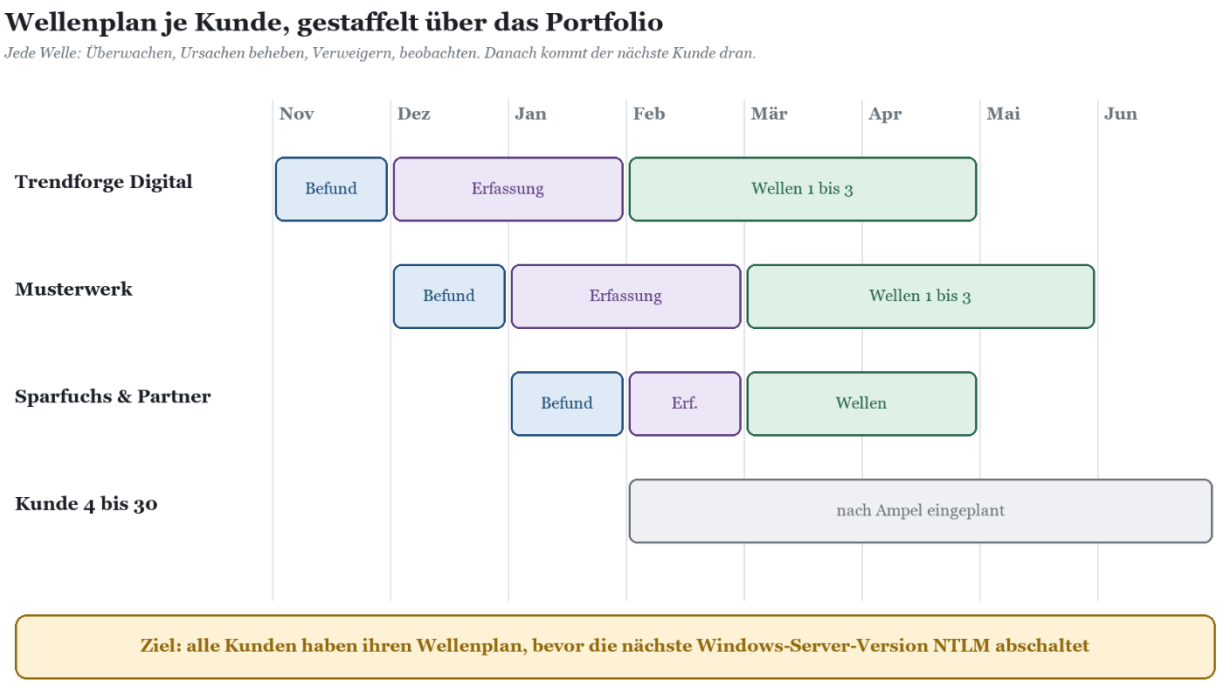
Wer zuerst dran ist

Kriterium	Hohe Priorität	Niedrige Priorität
NTLMv1	aktiv, Ereignisse 4024 oder 4025 vorhanden	kein NTLMv1 gefunden
Betriebssysteme	viele Clients auf Windows 11 24H2, Server 2025 im Einsatz	noch ältere Systeme, Wechsel erst später geplant
Geräte ohne Protokoll	viele NAS, Scanner, Maschinensteuerungen	wenige, gut dokumentiert
Branche	Klinik, Verwaltung, regulierte Umgebungen	kleines Büro ohne Fachanwendungen
Abhängigkeit von Herstellern	Fachanwendungen mit fest eingebautem NTLM	Standardsoftware

Kliniken und Verwaltungen gehören fast immer nach oben, nicht wegen der Ampel, sondern wegen der Vorlaufzeiten bei Herstellern und Freigaben. Wenn du solche Kunden betreust, lies NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Wellenplan über das ganze Portfolio

Pro Kunde läuft das Standardpaket mit seinen eigenen Wellen. Über das Portfolio gesehen staffelst du die Kunden so, dass deine Spezialisten nie mehr als eine Handvoll Berichte gleichzeitig schreiben und deine Techniker nicht in jeder Woche drei Abschaltwellen fahren.



Skizze: gestaffelte Kundenprojekte, Zeitachse beispielhaft

TIPP · Gleiche Ursache, gleiche Lösung, gleiches Dokument

Pflege eine interne Sammlung typischer Ursachen mit Lösung: „Scanner-Modell X schreibt per IP“, „Kanzleisoftware Y braucht Negotiate“, „ERP-Dienstkonto ohne SPN“. Beim fünften Kunden mit demselben Fall sparst du dir die Recherche komplett. Das ist der eigentliche Skaleneffekt im Systemhaus.

WARNUNG · NTLMv1 wartet nicht auf deinen Wellenplan

Kunden mit aktivem NTLMv1 haben schon jetzt ein Problem, nicht erst bei der nächsten Windows-Server-Version. Prüfe die Ereignisse 4024 und 4025 bei jedem Kunden zuerst. Wie du sie liest, steht in Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen, was seit Oktober nicht mehr geht, in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Wenn du das Standardpaket, die Rollen und das Abrechnungsmodell nicht allein aufsetzen möchtest, unterstützt dich die Beratung zur NTLM-Ablösung beim Zuschnitt auf dein Systemhaus, einschließlich der ersten Kunden als Pilot.

FAQ: NTLM-Ablösung im Systemhaus

Lohnt sich ein Standardpaket schon bei zehn Kunden?

Ja. Schon ab dem dritten Kunden sparst du Zeit, weil Gruppenrichtlinie, Abfragen und Berichtsgliederung feststehen. Ab dem zehnten verdienst du daran, statt Lehrgeld zu zahlen.

Kann ich mehrere Kundendomänen in einer Oberfläche des Diagnostikers verwalten?

Noch nicht. Mandantenfähigkeit ist geplant. Bis dahin arbeitest du je Kunde mit einer eigenen Installation und einer Lizenz je Endkunde mit Partnervermerk.

Was kostet der Diagnostiker für unser eigenes Systemhaus?

Nichts. Für die eigene Domäne des Systemhauses ist er kostenlos. Das ist der ideale Ort, um das Vorgehen zu üben, bevor du es beim Kunden einsetzt.

Darf ich den Express-Befund beim Kunden einfach laufen lassen?

Technisch ändert er nichts, denn der Diagnostiker arbeitet ausschließlich lesend. Organisatorisch solltest du trotzdem eine kurze Freigabe einholen, weil Konten- und Rechnernamen sichtbar werden. Datenschutz und gegebenenfalls Betriebsrat gehören zum Standardvertrag.

Wie rechne ich die Lizenz beim Kunden ab?

Die Lizenz wird pro aktivem Computerkonto vergeben, je Endkunde mit Partnervermerk. Du kannst sie als eigene Position ausweisen oder in deine Paketpreise einrechnen. Wichtig ist nur, dass der Kunde versteht, wofür er zahlt.

Was mache ich mit Kunden, deren Server noch kein erweitertes Auditing haben?

Dort nutzt du die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004, die auch auf älteren Systemen verfügbar sind, allerdings ohne Reason ID. Sobald Windows Server 2022 oder 2019 die Updates ab 13.10.2026 haben, kommen die Ereignisse 4020 bis 4023 und 4030 bis 4033 hinzu.

Brauchen wir für jeden Kunden einen Kerberos-Spezialisten?

Nein. Ein Spezialist kann mehrere Techniker und damit viele Kunden begleiten, wenn die Techniker das Standardpaket sicher beherrschen. Genau dafür ist das Onboarding da.

Fazit: ein Drehbuch, viele Aufführungen

Die NTLM-Ablösung ist für Systemhäuser kein technisches Problem, sondern ein organisatorisches. Die Ursachen wiederholen sich, die Werkzeuge sind bekannt, die Fristen stehen fest. Was fehlt, ist meist das eine Vorgehen, das jeder Techniker bei jedem Kunden gleich durchzieht: Express-Befund, Erfassung, Bericht, Wellenplan. Dazu eine klare Rollenverteilung, Festpreise statt offener Aufwände und eine Lizenzierung, die zum Kunden passt.

Mit Bordmitteln kommst du bei einem Kunden ans Ziel, bei dreißig kommst du ans Limit. Wer jetzt sein Standardpaket baut, hat die roten Kunden versorgt, bevor sie anrufen, und die grünen gepflegt, bevor sie gelb werden. Alle anderen erleben die nächste Windows-Server-Version als kollektiven Montagmorgen. Mit dreißig klingelnden Telefonen. Und einem Spezialisten, der gerade Urlaub hat.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet
› NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand
› NTLM-Nutzung ermitteln: der komplette Leitfaden
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst
› NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker