

NTLM Diagnostiker: NTLM ablösen, ohne dass der Laden stillsteht

NTLM ist wie das alte Kabel hinter dem Serverschrank, von dem keiner mehr weiß, wozu es gehört. Rausziehen traut sich niemand, weil irgendwo garantiert etwas dranhängt. Nur: Microsoft zieht demnächst selbst. Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet, und NTLMv1 wird für die einfache Anmeldung schon seit Oktober 2026 blockiert.

Der **NTLM Diagnostiker** findet heraus, was an diesem Kabel hängt. Er sammelt die NTLM-Ereignisse aus deiner Domäne ein, wertet Netzwerkmitschnitte aus, gleicht alles mit dem Active Directory ab und sagt dir für jede Verbindung: **wer, wohin, warum** und **was du dagegen tun kannst**. Am Ende steht ein Plan, mit dem du NTLM Schritt für Schritt abschaltest, statt am Stichtag zu hoffen.

Beratung
NTLM-Ablösung als Projekt: Bestandsaufnahme, Phasenplan, Begleitung.
[Zur Beratung NTLM-Ablösung](#)

Schulung
Kerberos statt NTLM: Workshop für Admins und Systemhäuser.
[Zum Schulungsangebot](#)

Wissen
Kerberos, SPNs, Delegation: das Fundament hinter der Ablösung.
[Zum Kompetenzbereich Kerberos](#)

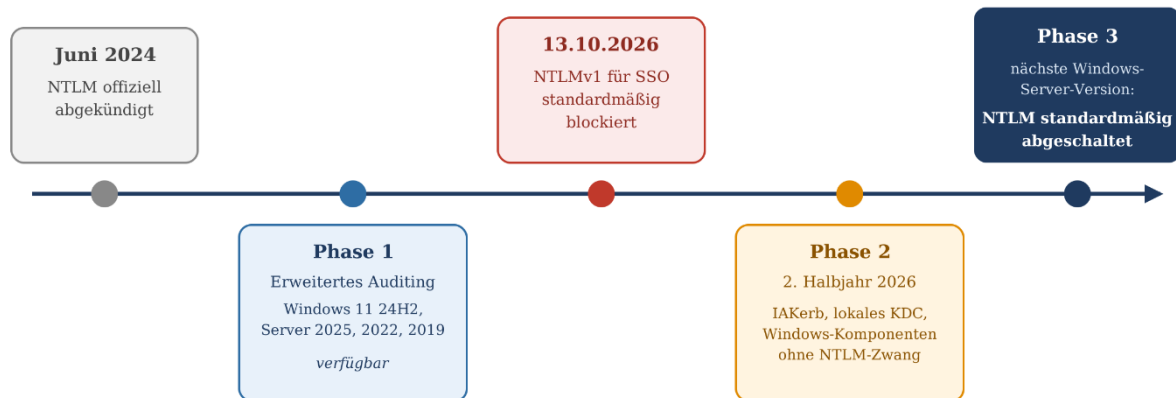
NTLM Diagnostiker auf einen Blick	
Wofür	Bestandsaufnahme, Ursachenanalyse und Abschaltplanung für die NTLM-Ablösung in Active-Directory-Umgebungen
Datenquellen	NTLM-Ereignisse von Clients, Servern und Domain Controllern, Netzwerkmitschnitte (Wireshark), Active Directory
Arbeitsweise	ausschließlich lesend; Einstellungen schlägt der Diagnostiker vor, umsetzen tust du sie selbst
Ergebnis	Kommunikationsmatrix, Ursache und Abhilfe je Verbindung, Abschalt-Simulation, Word-Bericht, Excel-Export
Editionen	Express (kostenlos), Testzeitraum (7 Tage), Lizenz pro aktivem Computerkonto
Lizenz	an die Domäne gebunden, beliebig viele Domänen eines Lizenznehmers, 18 Monate Laufzeit, kein Abo
Familie	Teil der Diagnostiker-Familie von boddenberg.de

Warum gerade jetzt?

NTLM ist seit Juni 2024 offiziell abgekündigt. Lange war das eine Meldung, die man zur Kenntnis nimmt und dann wegklickt. Seit Microsoft einen konkreten Fahrplan veröffentlicht hat, ist es eine Baustelle mit Termin.

Microsofts Fahrplan für den NTLM-Ausstieg

Die Uhr läuft bereits, und zwar in allen Phasen gleichzeitig



Wer erst bei Phase 3 anfängt zu suchen, sucht unter Zeitdruck

Skizze 1: Microsofts Fahrplan für den NTLM-Ausstieg

- **Phase 1, erweitertes Auditing:** Windows 11 ab 24H2 und Windows Server 2025 protokollieren NTLM-Anmeldungen mit deutlich mehr Details, inklusive einer Begründung, warum NTLM statt Kerberos benutzt wurde. Seit den Updates vom 13. Oktober 2026 können das auch Windows Server 2022 und 2019. Das ist die Datenbasis, auf der der Diagnostiker aufsetzt.
- **Phase 2, Lückenschluss:** Microsoft liefert Funktionen wie IAKerb und ein lokales KDC nach, damit typische Gründe für den NTLM-Rückfall wegfallen, zum Beispiel fehlende Sichtverbindung zum Domain Controller oder lokale Konten.
- **Phase 3, Abschaltung:** Mit der nächsten Windows-Server-Version und dem zugehörigen Client ist NTLM standardmäßig aus. Wer es dann noch braucht, muss es per Richtlinie ausdrücklich wieder einschalten.

NTLMv1 ist schon scharf

Seit dem Windows-Sicherheitsupdate vom 13. Oktober 2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 die einfache Anmeldung (Single Sign-on) mit NTLMv1-abgeleiteten Anmeldedaten standardmäßig, sofern der Registrierungswert BlockNtlmv1SSO nicht ausdrücklich gesetzt ist. Im Protokoll Microsoft-Windows-NTLM/Operational taucht das als Ereignis 4024 (Überwachung) beziehungsweise 4025 (blockiert) auf.

Wenn dir seit Mitte Oktober ein alter Scanner oder eine Fachanwendung Ärger macht, weißt du jetzt, warum. Details stehen bei [Microsoft zu den NTLMv1-Änderungen](#).

Das eigentliche Problem: nicht das Ob, sondern das Warum

Dass in deiner Domäne NTLM gesprochen wird, findest du mit Bordmitteln in fünf Minuten heraus. Die Antwort lautet fast immer: ja, und zwar reichlich. Spannend wird es bei der Frage, **warum** ein Client nicht Kerberos benutzt hat. Denn davon hängt ab, was du tun musst.

Genau hier helfen die neuen Ereignisse von Microsoft: Jedes ausgehende NTLM-Ereignis (4020 und 4021) trägt eine Begründung, die sogenannte Reason-ID. Der Diagnostiker übersetzt sie in Klartext und hängt die passende Abhilfe gleich mit dran.

Reason-ID	Was dahintersteckt	Typische Abhilfe
1	Die Anwendung ruft NTLM direkt auf	Hersteller fragen, ob Negotiate oder Kerberos möglich ist
2	Anmeldung mit einem lokalen Konto	Domänenkonto oder gruppenverwaltetes Dienstkonto verwenden
4	Anmeldung mit einem Cloud-Konto	Szenario prüfen, Kerberos über Entra ID bewerten
5	Zielname fehlt oder ist leer	Anwendungskonfiguration korrigieren
6	Zielname nicht auflösbar	SPN anlegen, DNS-Eintrag prüfen
7	Ziel wird per IP-Adresse angesprochen	Pfade und Verknüpfungen auf DNS-Namen umstellen
8	Zielname im AD doppelt vorhanden	Doppelten SPN bereinigen
9	Keine Sichtverbindung zum Domain Controller	Netzwerkpfad prüfen, Kandidat für IAKerb
10	Aufruf über die Loopback-Schnittstelle	Lokalen Dienstaufbau umbauen
11	Aufruf mit einer Null-Sitzung	Anonymen Zugriff abschaffen
0	Grund unbekannt	Mit Prozess, Ziel und Mitschnitt weiter eingrenzen

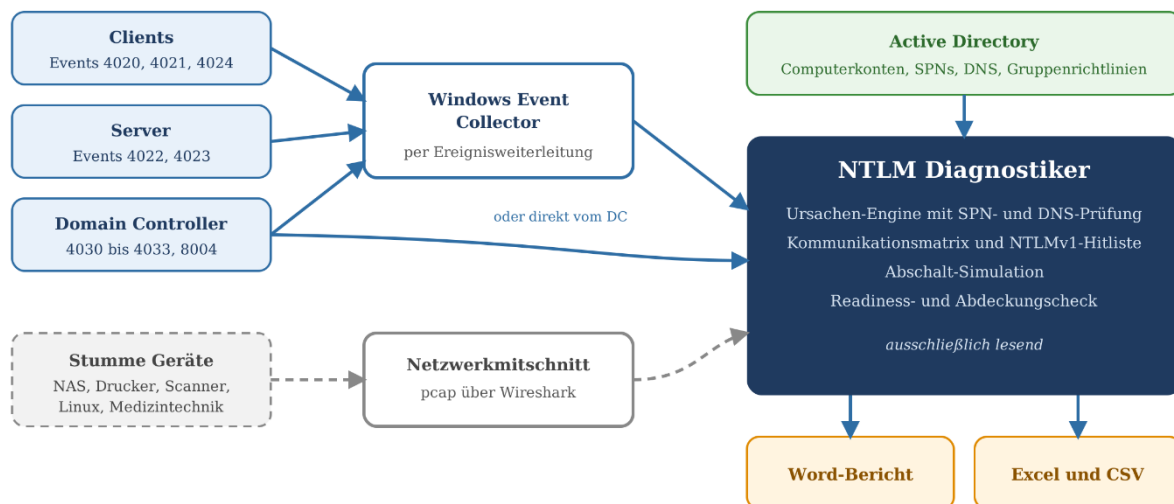
Die Liste der Reason-IDs stammt aus Microsofts [Übersicht zum erweiterten NTLM-Auditing](#). Der Diagnostiker hält sie aktuell, falls Microsoft weitere Gründe ergänzt.

So arbeitet der NTLM Diagnostiker

Der Diagnostiker ist eine Windows-Anwendung, die du auf einem Admin-Arbeitsplatz oder Server startest. Er zieht seine Daten aus drei Richtungen zusammen und hält sie in einer lokalen Datenbank, sodass du über Wochen hinweg sammeln und jederzeit auswerten kannst.

So kommen die Daten in den NTLM Diagnostiker

Nur lesen, nichts verändern: Ereignisse, Mitschnitte und das Active Directory



Der Mitschnitt findet die Geräte, die kein Windows-Ereignisprotokoll schreiben

Skizze 2: Ereignisse, Mitschnitte und Active Directory fließen im Diagnostiker zusammen

Datenquellen

- **Domain Controller direkt:** Für den schnellen Überblick liest der Diagnostiker die NTLM-Ereignisse der DCs. Ganz ohne Vorbereitung, ideal für den ersten Befund.
- **Windows Event Collector:** Für die vollständige Bestandsaufnahme leiten Clients und Server ihre NTLM-Ereignisse per Ereignisweiterleitung an einen Sammelserver. Der Diagnostiker liest dort ein einziges Protokoll, statt Tausende Maschinen einzeln abzufragen.
- **Direktabfrage einzelner Server:** Für kleine Umgebungen oder gezielte Nachfragen bei einzelnen Servern.
- **Netzwerkmitschnitte:** Für Geräte, die gar kein Windows-Ereignisprotokoll schreiben.
- **Active Directory:** Computerkonten, SPNs, DNS und Gruppenrichtlinien, um jede Verbindung gegenzuprüfen.

Welche Ereignisse ausgewertet werden

Ereignis	Quelle	Bedeutung
4020, 4021	Client	Ausgehende NTLM-Anmeldung mit Reason-ID; 4021 als Warnung bei geschwächter Sicherheit, etwa NTLMv1
4022, 4023	Server	Eingehende NTLM-Anmeldung mit Ergebnis; 4023 als Warnung
4024, 4025	Client	NTLMv1 bei der einfachen Anmeldung überwacht (4024) oder blockiert (4025)
4030 bis 4033	Domain Controller	Domänenweite NTLM-Anmeldungen, auch domänenübergreifend
8001 bis 8004	Client, Server, DC	Klassische Restrict-NTLM-Überwachung, auch auf älteren Systemen ohne erweitertes Auditing

Nur lesen, nichts anfassen

Der NTLM Diagnostiker verändert nichts an deiner Umgebung: keine Gruppenrichtlinien, keine Registrierungswerte, keine Konten. Wo eine Einstellung fehlt, zeigt er sie dir an und liefert auf

Wunsch das passende Skript. Ausführen tust du es selbst. Das macht die Freigabe beim CISO deutlich einfacher.

Die Funktionen im Detail

Readiness-Ampel

Bevor du auswertest, musst du wissen, ob die Daten überhaupt vollständig sind. Die Readiness-Ampel prüft, ob das NTLM-Auditing aktiv ist, ob die Domain Controller die erweiterten Ereignisse liefern, welche Restrict-NTLM-Einstellungen gesetzt sind, wie LmCompatibilityLevel und BlockNtlmv1SSO stehen und ob sich Gruppenrichtlinien gegenseitig widersprechen. Rot heißt: erst nachbessern, dann auswerten.

Abdeckungsmonitor und OS-Landkarte

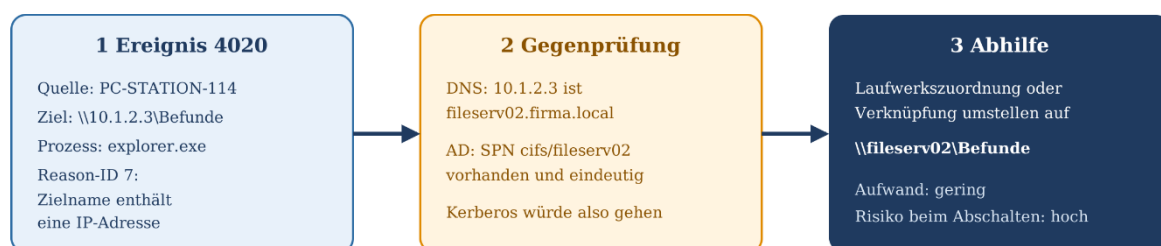
Eine Auswertung ist nur so gut wie die Zahl der Maschinen, die tatsächlich liefern. Der Abdeckungsmonitor zeigt, welche Rechner Ereignisse schicken und welche schweigen, zum Beispiel „1.840 von 2.100 Rechnern liefern, 260 nicht, davon 190 aus der OU Medizintechnik“. Die OS-Landkarte ergänzt, welche Maschinen die erweiterten Ereignisse mit Reason-ID liefern können und welche nur die klassischen. Dazu prüft ein Pipeline-Test, ob WinRM läuft, die Subscription aktiv ist und das Weiterleitungsprotokoll auf dem Collector nicht überläuft.

Ursachen-Engine mit SPN- und DNS-Prüfung

Das Herzstück. Für jede NTLM-Verbindung wertet die Ursachen-Engine die Reason-ID aus und prüft gegen: Gibt es zum Ziel einen DNS-Namen? Existiert der passende SPN, und ist er eindeutig? Wird der Server per IP-Adresse angesprochen? Läuft der Dienst unter einem lokalen Konto? Heraus kommt eine Diagnose mit konkreter Abhilfe, Aufwand und Risiko.

Vom Ereignis zur Abhilfe

Die Ursachen-Engine an einem typischen Fall



Aus „irgendwer macht NTLM“ wird eine konkrete Aufgabe mit Adresse

Skizze 3: Aus einem Ereignis wird eine konkrete Aufgabe

NTLMv1-Hitliste

NTLMv1 gehört ganz nach oben auf die Liste, weil es kryptografisch am schwächsten ist und weil Microsoft hier bereits blockiert. Die Hitliste zeigt alle Quellen, die noch NTLMv1 sprechen, samt Konto, Ziel und Prozess. Rot hinterlegt, damit niemand behaupten kann, er hätte es nicht gesehen.

Kommunikationsmatrix und Konten-Sicht

Wer spricht mit wem per NTLM, mit welchem Konto, aus welchem Prozess und wie oft? Die Kommunikationsmatrix ist filterbar nach Quelle, Ziel, Konto, Protokoll und Reason-ID. Die Konten-

Sicht dreht die Perspektive um: Welche Dienstkonten machen wie viel NTLM und gegen welche Ziele? Dienstkonten sind erfahrungsgemäß die Hauptverdächtigen.

Sicherheitsflaggen

Nicht jede NTLM-Anmeldung ist gleich gefährlich. Fehlt die Nachrichtenintegritätsprüfung (MIC), gibt es keine Kanalbindung oder keinen Sitzungsschlüssel, ist die Verbindung ein Kandidat für Relay-Angriffe. Der Diagnostiker markiert diese Fälle eigens. Das interessiert den CISO auch dann, wenn die vollständige Ablösung noch eine Weile dauert.

Wireshark-Import für stumme Geräte

Ausgerechnet die Geräte, an denen eine Abschaltung später scheitert, schreiben keine Windows-Ereignisse: NAS-Systeme, Drucker und Scanner, Linux-Server, Medizintechnik. Deshalb liest der Diagnostiker Netzwerkmitschnitte im pcap- und pcapng-Format ein. Er nutzt dafür tshark aus einer vorhandenen Wireshark-Installation und filtert die NTLMSSP-Anmeldungen aus SMB, HTTP, LDAP und RPC heraus.

- Die Treffer landen in derselben Kommunikationsmatrix wie die Ereignisse, gekennzeichnet als Quelle „Mitschnitt“.
- Besonders aufschlussreich ist die Liste der Verbindungen, die **nur** im Mitschnitt auftauchen: genau die Geräte, die im Ereignisprotokoll unsichtbar sind.
- NTLMv1 erkennt der Diagnostiker auch im Mitschnitt und setzt es direkt auf die Hitliste.

Datenschutz beim Mitschnitt

Ein Mitschnitt enthält mehr als nur Anmeldungen. Der Diagnostiker übernimmt ausschließlich die NTLM-Metadaten (Quelle, Ziel, Konto, Protokoll, Version) und speichert die Mitschnittdatei selbst weder als Kopie noch in seiner Datenbank.

Verschlüsselte Verbindungen wie HTTPS, LDAPS oder RDP mit TLS kann kein Mitschnitt einsehen. Für SMB klappt es dagegen, weil die Anmeldung vor der Verschlüsselung stattfindet.

Abschalt-Simulation

Die Frage, vor der jeder Admin Angst hat: Was passiert, wenn wir NTLM hier abschalten? Die Abschalt-Simulation beantwortet sie auf Basis deiner gesammelten Daten. Du wählst eine OU, eine Servergruppe oder die ganze Domäne aus und siehst, welche Verbindungen der letzten Wochen betroffen wären, wer sie verursacht und ob es für sie schon eine Abhilfe gibt. „Wenn wir OU Verwaltung blockieren, trifft es 14 Verbindungen, 11 davon sind mit einem DNS-Namen erledigt“ ist eine Aussage, mit der man in eine Änderungsbesprechung gehen kann.

Bericht und Export

Der Word-Bericht fasst die Ergebnisse so zusammen, dass Geschäftsführung, CISO und IT-Leitung damit arbeiten können: Ampel, Kennzahlen, NTLMv1-Befund, die wichtigsten Ursachen, Ergebnis der Abschalt-Simulation und Empfehlungen. Alle Rohdaten gehen zusätzlich als Excel- und CSV-Export raus, etwa für das Ticketsystem.

Lizenzanforderung

Der Diagnostiker zählt die aktiven Computerkonten deiner Domänen und erzeugt daraus die Lizenzanforderung. So steht der Preis fest, bevor wir überhaupt miteinander gesprochen haben.

Ausbaustufen

Einige Funktionen kommen nach der ersten Version. Termine nennen wir bewusst nicht, nur die Richtung:

- **Anwendungserkennung:** Ein mitwachsender Katalog bekannter NTLM-Verursacher macht aus „svchost.exe auf SRV-X“ eine Vermutung wie „vermutlich die Druckerwarteschlange“.
- **Ausnahmelisten-Generator:** Vorschläge für die Server-Ausnahmen der Restrict-NTLM-Richtlinien, abgeleitet aus den tatsächlich beobachteten Verbindungen.
- **Skript-Generator:** SPN-Korrekturen und Gruppenrichtlinien-Einstellungen als fertiges Paket zum Prüfen und Ausführen.
- **Phasenplan pro OU:** Audit, Ausnahmen festziehen, blockieren, beobachten, jeweils mit Erfolgskriterium und Rückfallweg.
- **Kerberos-Gegencheck:** Wenn NTLM wegfällt, muss Kerberos tragen. Zeitabweichungen, DNS, Verschlüsselungstypen und Delegierungen werden mitgeprüft.
- **Verlauf über mehrere Erfassungen:** Die NTLM-Quote sinkt von 34 auf 6 Prozent, und zwar sichtbar.
- **Zuständigkeiten und Status** je Befund sowie Vorlagen für Anfragen an Hersteller.
- **Phase-3-Bereitschaft:** Welche Verbindungen profitieren von IAKerb und lokalem KDC, sobald Microsoft sie ausliefert?

Datenschutz und Mitbestimmung

NTLM-Ereignisse enthalten Benutzernamen, Rechnernamen und Uhrzeiten. Das sind personenbezogene Daten, und in vielen Häusern will der Betriebs- oder Personalrat wissen, wofür sie verwendet werden. Der Diagnostiker ist dafür gebaut, diese Fragen leicht zu beantworten:

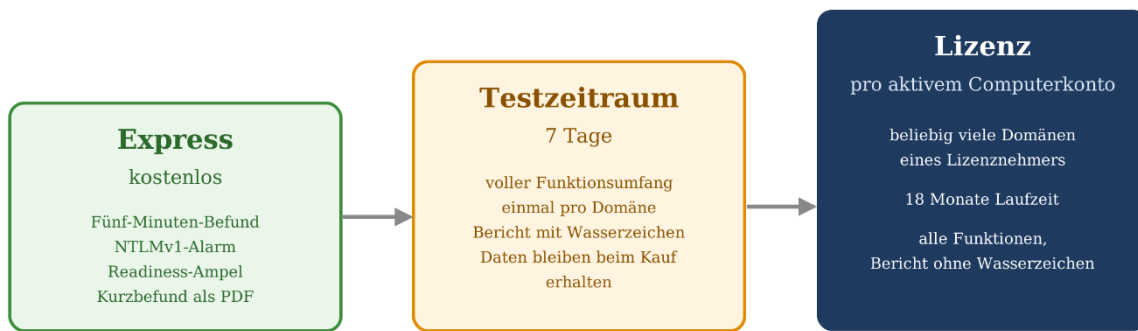
- **Zweck:** Ausgewertet wird, welche Systeme und Dienste NTLM benötigen. Eine Auswertung von Arbeitsverhalten ist weder vorgesehen noch sinnvoll.
- **Alles bleibt im Haus:** Die Daten liegen in einer lokalen Datenbank bei dir. Die Lizenzprüfung läuft offline.
- **Domänenkennung nur als Fingerabdruck:** Für die Lizenz wird die Domänen-SID ausschließlich als nicht umkehrbarer Hash übermittelt, zusammen mit der Zahl der Computerkonten. Sonst nichts.
- **Mitschnitte:** Nur NTLM-Metadaten werden übernommen, die Mitschnittdatei selbst nicht gespeichert.

Editionen, Preise und Testzeitraum

Eine NTLM-Ablösung ist ein Projekt mit Anfang und Ende. Wenn NTLM weg ist, braucht niemand mehr ein Werkzeug, das NTLM sucht. Deshalb gibt es kein Abo und keine Wartungsgebühr für die Ewigkeit, sondern eine Lizenz für die Dauer des Projekts, berechnet nach der Größe der Baustelle.

Erst sehen, dann testen, dann ablösen

Bezahlt wird nur das Projekt, nicht ein Abo für die Ewigkeit



Optional dazu: Servicepaket mit Beratung, Premium-Report und Workshop

Skizze 4: Express, Testzeitraum und Lizenz

Funktion	Express	Testzeitraum	Lizenz
Fünf-Minuten-Befund (DC-Ereignisse der letzten Tage)	ja	ja	ja
Readiness-Ampel	ja	ja	ja
NTLMv1-Alarm	Anzahl und Top 5	vollständige Hitliste	vollständige Hitliste
Hinweise auf doppelte SPNs und Zugriffe per IP	nur Anzahl	mit Details	mit Details
Kurzbefund als PDF	ja	ja	ja
Kontenzählung und Lizenzanforderung	ja	ja	ja
Dauerhafte Erfassung über Event Collector	–	ja	ja
Abdeckungsmonitor und OS-Landkarte	–	ja	ja
Ursachen-Engine mit SPN- und DNS-Prüfung	–	ja	ja
Kommunikationsmatrix und Konten-Sicht	–	ja	ja
Sicherheitsflaggen	–	ja	ja
Wireshark-Import	–	ja	ja
Abschalt-Simulation	–	ja	ja
Word-Bericht	–	mit Wasserzeichen	ja
Excel- und CSV-Export	–	ja	ja
Laufzeit	unbegrenzt	7 Tage, einmal pro Domäne	18 Monate
Preis	kostenlos	kostenlos	pro aktivem Computerkonto

Express: der Fünf-Minuten-Befund

Express braucht keinen Collector und keine Gruppenrichtlinie. Er liest die NTLM-Ereignisse der letzten Tage direkt von deinen Domain Controllern und sagt dir nach ein paar Minuten, wie es um deine Domäne steht, zum Beispiel: „3.412 NTLM-Anmeldungen gegen 87 Server, davon 41 mit NTLMv1“. Dazu die Readiness-Ampel, die Zahl der aktiven und der verwaisten Computerkonten und ein einseitiger Kurzbefund als PDF, den du direkt an die IT-Leitung weitergeben kannst.

Express zeigt dir, **dass** es ein Problem gibt und **wie groß** es ist. Warum es im Einzelnen auftritt und was zu tun ist, zeigen Testzeitraum und Lizenz.

Testzeitraum: sieben Tage mit vollem Funktionsumfang

Im Testzeitraum kannst du alles ausprobieren, auch Ursachen-Engine, Wireshark-Import und Abschalt-Simulation. Nur der Word-Bericht trägt ein Wasserzeichen.

- Die sieben Tage beginnen mit der ersten Aktivierung, nicht mit dem Download.
- Der Testzeitraum gilt einmal pro Domäne.
- Was du in den sieben Tagen gesammelt hast, bleibt beim Kauf erhalten. Die Erfassung läuft einfach weiter.

Warum sieben Tage nicht reichen

Sieben Tage zeigen dir, dass der Diagnostiker funktioniert. Für eine belastbare Bestandsaufnahme sind sie zu kurz, weil Monatsabschlüsse, Quartalsjobs und Wartungsfenster darin nicht vorkommen. Für die eigentliche Inventur solltest du mindestens 30 Tage erfassen.

Die Lizenz: pro aktivem Computerkonto

Bezahlt wird nach der Größe deiner Umgebung, gemessen an den aktiven Computerkonten. So zahlt der Klinikverbund mehr als das Steuerbüro, und beide zahlen einen fairen Preis.

- **Was zählt:** aktivierte Computerkonten mit einer Anmeldung in den letzten 90 Tagen, also Clients, Server und Domain Controller. Verwaiste Konten zählen nicht mit, und der Diagnostiker zeigt sie dir gleich als Nebenbefund an. Geräte ohne Computerkonto, etwa ein NAS aus dem Mitschnitt, zählen ebenfalls nicht.
- **Beliebig viele Domänen:** Eine Lizenz kann alle Domänen und Gesamtstrukturen eines Lizenznehmers umfassen. Die Staffel gilt für die Summe aller Konten, nicht je Domäne.
- **Lizenznehmer:** eine Organisation oder ein Konzernverbund. Alle Domänen einer Lizenz gehören diesem Lizenznehmer, sein Name steht im Bericht.
- **Wachstum:** Die Kontenzahl wird beim Aktivieren festgeschrieben. Bis zu 10 Prozent Zuwachs sind abgedeckt, darüber gibt es einen Hinweis, aber keine Sperre.
- **Domäne vergessen?** Neue Lizenzanforderung erzeugen, berechnet werden nur die zusätzlichen Konten. Die Laufzeit bleibt beim ursprünglichen Ablaufdatum.
- **Laufzeit:** 18 Monate. Das reicht für eine realistische Ablösung einschließlich Phase 3. Wer länger braucht, spricht uns an.

Aktive Computerkonten	Preis pro Konto (netto)
bis 500	Preis folgt
501 bis 2.000	Preis folgt

Aktive Computerkonten	Preis pro Konto (netto)
ab 2.001	Preis folgt
Mindestpreis je Lizenz	Preis folgt

Alle Preise verstehen sich netto zuzüglich der gesetzlichen Mehrwertsteuer.

Servicepaket: Beratung, Premium-Report und Workshop

Du willst die Ergebnisse nicht allein interpretieren? Das Servicepaket zum Festpreis von **Preis folgt** enthält eine Initial-Beratung, einen ausführlichen Premium-Report und einen Ergebnis-Workshop, in dem wir den Phasenplan für deine Umgebung festlegen. Wer das ganze Projekt begleitet haben möchte, findet alles Weitere unter [Beratung zur NTLM-Ablösung](#).

Für Systemhäuser

Du betreust mehrere Kunden, die alle vor der NTLM-Ablösung stehen? Für die eigene Domäne und zum Kennenlernen bekommst du den Diagnostiker kostenlos. Für Kundeneinsätze erhält jeder Kunde seine eigene Lizenz, in der du als betreuender Partner vermerkt bist. Sprich uns an: [Kontakt über die Beratung](#).

Kostenlos vorab: das Audit-GPO-Skript

Bevor du NTLM auswerten kannst, muss es protokolliert und eingesammelt werden. Dafür gibt es ein kostenloses PowerShell-Skript. Es legt ein Gruppenrichtlinienobjekt mit allen nötigen Audit-Einstellungen und der Ereignisweiterleitung an und erzeugt die passende Subscription-Datei für den Collector. Es blockiert nichts und verknüpft das GPO nicht. Das entscheidest du selbst.

Download und Anleitung: [Audit-GPO-Skript für die NTLM-Ablösung](#)

Systemvoraussetzungen

Welche Systeme welche Ereignisse liefern

System	Erweiterte Ereignisse mit Reason-ID	Klassische Ereignisse 8001 bis 8004
Windows 11 ab 24H2	ja (4020 bis 4025)	ja
Windows Server 2025	ja (4020 bis 4025, DC: 4030 bis 4033)	ja
Windows Server 2022 und 2019	ja, mit Updates ab 13.10.2026 (ohne 4024 und 4025)	ja
Windows 10, Windows Server 2016 und älter	nein	ja

Ältere Systeme liefern also nur, **dass** sie NTLM sprechen, nicht **warum**. Der Diagnostiker kennzeichnet diese Fälle und grenzt die Ursache über Ziel, Konto und Active Directory weiter ein. Ein aktueller Domain Controller sieht die Anmeldungen alter Systeme ohnehin.

Für den Diagnostiker selbst

- Windows-Arbeitsplatz oder -Server in der Domäne, **Version und Laufzeitumgebung folgen**
- Lesender Zugriff auf das Active Directory, ein normales Domänenkonto genügt

- Lesezugriff auf die Ereignisprotokolle der Domain Controller beziehungsweise des Collectors, zum Beispiel über die Gruppe „Ereignisprotokollleser“
- Für den Mitschnitt-Import: eine Wireshark-Installation mit tshark

Beratung und Schulung rund um die Ablösung

Ein Werkzeug findet die Ursachen. Abschalten musst du trotzdem selbst, und genau da kommen die Fragen, bei denen Erfahrung hilft: Wie überzeuge ich den Hersteller der Laborsoftware? Was mache ich mit dem Dienst, der hart auf NTLM programmiert ist? In welcher Reihenfolge schalte ich ab, damit montags keiner anruft?

- **Beratung:** von der Bestandsaufnahme über den Phasenplan bis zur Begleitung der Abschaltung. [Beratung zur NTLM-Ablösung](#)
- **Schulung:** Kerberos statt NTLM, SPNs, Delegierung und Fehlersuche, für Admins und Systemhäuser. [Schulungsangebot](#)
- **Wissen:** Hintergründe zu Kerberos, SPNs und dem NTLM-Rückfall im [Kompetenzbereich Kerberos](#).

Häufige Fragen

Verändert der NTLM Diagnostiker etwas an meiner Umgebung?

Nein. Er liest ausschließlich. Fehlende Einstellungen zeigt er dir an und liefert auf Wunsch das passende Skript, ausführen tust du es selbst.

Brauche ich unbedingt einen Windows Event Collector?

Für den ersten Befund nicht, der Diagnostiker liest dann direkt von den Domain Controllern. Für die vollständige Bestandsaufnahme aller Clients und Server ist ein Collector der bequemste Weg. Das kostenlose Audit-GPO-Skript richtet die Weiterleitung ein.

Wie lange sollte ich Daten sammeln?

Mindestens 30 Tage, besser einen vollen Monatszyklus plus Puffer. Sonst fehlen Monatsabschlüsse, Quartalsjobs und Wartungsfenster, und genau die melden sich dann am Tag nach der Abschaltung.

Was ist mit Geräten ohne Windows?

Dafür gibt es den Wireshark-Import. Ein Mitschnitt an einem zentralen Punkt, etwa am Fileserver oder Domain Controller, zeigt auch NAS, Drucker, Scanner und Linux-Systeme, die NTLM sprechen.

Erkennt der Diagnostiker NTLM in verschlüsselten Verbindungen?

Im Mitschnitt nicht, HTTPS, LDAPS und RDP mit TLS sind dafür undurchsichtig. Laufen diese Anmeldungen gegen Windows-Server, tauchen sie aber in deren Ereignisprotokoll auf.

Warum kein Abo?

Weil NTLM-Ablösung ein Projekt mit Ende ist. Du zahlst einmal für 18 Monate, nach der Größe deiner Umgebung, und danach brauchst du das Werkzeug idealerweise nicht mehr.

Was zählt als aktives Computerkonto?

Ein aktiviertes Computerkonto mit Anmeldung in den letzten 90 Tagen. Verwaiste Konten zählen nicht, ebenso wenig Geräte ohne Computerkonto.

Wir haben mehrere Domänen. Brauchen wir mehrere Lizenzen?

Nein. Eine Lizenz umfasst beliebig viele Domänen desselben Lizenznehmers, die Staffel gilt für die Summe aller Konten.

Werden Daten an boddenberg.de übertragen?

Nein. Alles bleibt in deiner Umgebung. Für die Lizenz bekommen wir nur einen nicht umkehrbaren Fingerabdruck der Domänen-SID und die Zahl der Computerkonten.

Was kostet der NTLM Diagnostiker konkret?

Das hängt von der Zahl der aktiven Computerkonten ab, die Staffel steht weiter oben. Der kostenlose Express zählt deine Konten und erzeugt die Lizenzanforderung, damit kennst du den Preis sofort.

Jetzt anfangen

Starte mit dem kostenlosen Express und sieh dir in fünf Minuten an, wie viel NTLM in deiner Domäne steckt. Wenn du Unterstützung beim Weg danach willst, melde dich: [Beratung zur NTLM-Ablösung](#).