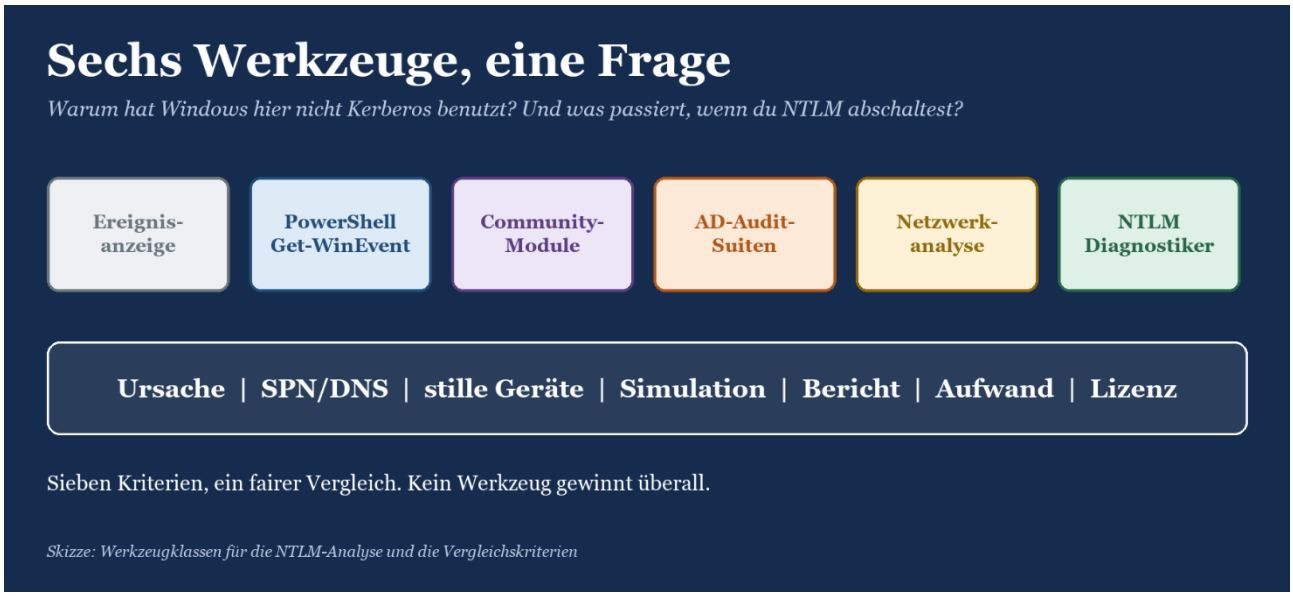
NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker



Skizze: Werkzeugklassen für die NTLM-Analyse und die Vergleichskriterien

WISSEN
Was der NTLM Diagnostiker rein lesend über die NTLM-Nutzung in deiner Domäne herausfindet.
› **NTLM Diagnostiker**

BERATUNG
Werkzeugauswahl, Erfassung und Abschaltplan gemeinsam mit erfahrenen Kerberos-Leuten.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Ereignisse lesen, Ursachen deuten, Berichte erstellen: praxisnah für dein Team.
› **Schulung zum NTLM Diagnostiker**

Irgendwann in jeder NTLM-Ablösung kommt die Werkzeugfrage. Meist dann, wenn du zum dritten Mal eine Ereignisanzeige mit 40.000 Einträgen nach Zeit sortiert hast und feststellst, dass du immer noch nicht weißt, warum der Buchhaltungsserver seit 2014 per NTLM mit dem Dateiserver redet. Dann beginnt die Suche: ein Skript aus dem Netz, ein Modul aus der Community, die Audit-Suite, die ohnehin schon lizenziert ist, Wireshark, oder doch ein spezialisiertes ntlm analyse tool?

Dieser Beitrag schließt die Serie zur NTLM-Ablösung ab und vergleicht die Optionen fair. Fair heißt: Bordmittel bekommen ihre Ehre, wo sie sie verdienen, und das ist in sehr kleinen Umgebungen ziemlich oft der Fall. Fair heißt aber auch: Wer 600 Rechner, drei Standorte und ein Labor voller Geräte mit Firmware aus der Bronzezeit betreut, sollte sich nicht einreden, dass er das mit einer gut gemeinten PowerShell-Schleife erledigt. Der Tod kommt bekanntlich nicht überraschend. Die Abschaltung von NTLM auch nicht.

Der Zeitplan steht nämlich: Seit dem Windows-Update vom 13.10.2026 ist NTLMv1 für Single Sign-on auf Windows 11 ab 24H2 und Windows Server 2025 standardmäßig blockiert, gesteuert über den Registrierungswert BlockNtlmv1SSO und sichtbar in den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM in Phase 3 standardmäßig abgeschaltet. Details findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

FAKTEN · Was jedes Werkzeug lesen können muss

Microsoft beschreibt das erweiterte NTLM-Auditing in KB5064479. Alle Ereignisse landen im Protokoll Microsoft-Windows-NTLM/Operational: 4020 und 4021 für ausgehende NTLM-

Anmeldungen auf dem Client, 4022 und 4023 für eingehende auf dem Server, 4030 bis 4033 auf Domänencontrollern. Die jeweils zweite Nummer ist eine Warnung, etwa bei NTLMv1.

Jedes dieser Ereignisse trägt eine Reason ID von 0 bis 11, zum Beispiel 2 für ein lokales Konto, 6 für einen nicht auflösbaren Zielnamen, 7 für eine IP-Adresse als Ziel, 8 für einen doppelten Eintrag im Active Directory und 9 für fehlende Sichtverbindung zum Domänencontroller.

Verfügbar ist das 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.

Die Kriterien: woran sich ein ntlm analyse tool messen lassen muss

Bevor wir Werkzeuge vergleichen, brauchen wir einen Maßstab. „Zeigt NTLM an“ ist keiner, denn das kann die Ereignisanzeige auch. Die eigentliche Arbeit beginnt nach dem Anzeigen. Die folgenden sieben Kriterien stammen aus genau den Stellen, an denen Projekte in der Praxis hängen bleiben. Wie du die Arbeit grundsätzlich angehst, steht in NTLM-Nutzung ermitteln: der komplette Leitfaden.

Kriterium	Die Frage dahinter	Warum es weh tut, wenn es fehlt
Ursache je Verbindung	Warum hat Windows bei genau dieser Verbindung nicht Kerberos benutzt?	Ohne Ursache hast du eine Liste, keinen Plan. Jede Zeile wird zur Detektivarbeit.
SPN- und DNS-Gegenprüfung	Stimmt die Ursache, oder fehlt einfach ein SPN oder ein DNS-Eintrag?	Die Reason ID sagt, was Windows dachte. Ob es stimmt, zeigt erst der Abgleich mit AD und DNS.
Stille Geräte	Welche Rechner und Geräte liefern gar keine Ereignisse?	Schweigen sieht aus wie Sauberkeit. Bis zum Abschalttag.
Simulation	Was bricht, wenn ich NTLM für diese OU oder Servergruppe verweigere?	Ohne Simulation ist jeder Abschaltschritt ein Feldversuch am lebenden Betrieb.
Bericht	Kann ich das Ergebnis Geschäftsführung, CISO oder Prüfern vorlegen?	Ohne Bericht bleibt die Analyse im Kopf eines Administrators. Der hat auch mal Urlaub.
Aufwand	Wie viel Arbeit kostet Einrichtung und laufende Pflege?	Selbstgebautes ist kostenlos, bis man die eigenen Stunden zählt.
Lizenzmodell	Was kostet es, und wonach wird gezählt?	Pro Benutzer, pro Server, pro Datenvolumen: Jedes Modell passt zu einer anderen Umgebung.

Zwei Kriterien fehlen bewusst: „schöne Oberfläche“ und „Echtzeit-Dashboard“. Beides ist nett, aber NTLM-Ablösung ist kein Leitstand, sondern ein Projekt mit Anfang und Ende. Wer vier Wochen lang auf ein blinkendes Dashboard starrt, hat danach vor allem trockene Augen.

Warum gerade die Ursache das Kriterium Nummer eins ist

Eine NTLM-Verbindung an sich ist kein Problem, sie ist ein Symptom. Ob du sie durch einen DNS-Namen statt einer IP-Adresse behebst, durch einen SPN, durch das Umstellen eines lokalen Kontos oder durch eine Herstelleranfrage, hängt allein an der Ursache. Die Reason IDs liefern dafür einen guten Startpunkt, aber eben nur auf den Systemen, die das erweiterte Auditing beherrschen. Die Bedeutung aller zwölf Werte erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

WICHTIG · Reason ID ist ein Hinweis, kein Urteil

Reason ID 6 heißt, dass der Zielname nicht aufgelöst werden konnte. Ob das an einem fehlenden SPN, an einem Tippfehler im Skript oder an einem DNS-Alias liegt, sagt das Ereignis nicht. Genau deshalb ist die Gegenprüfung gegen Active Directory und DNS ein eigenes Kriterium. Mehr dazu in Reason-ID 6: wenn der Zielname nicht auflösbar ist.

Bordmittel und Skripte: ehrlich, kostenlos, begrenzt

Windows bringt alles mit, um NTLM zu sehen. Was es nicht mitbringt, ist jemand, der die Ereignisse für dich zusammensetzt. Schauen wir uns die Bordmittel der Reihe nach an.

Ereignisanzeige: der ehrliche Einstieg

Unter Anwendungs- und Dienstprotokolle, Microsoft, Windows, NTLM, Operational liegen die Ereignisse. Ein Doppelklick zeigt im Meldungstext Felder wie „Reason ID“, „Target Machine“ oder „NTLM Version“. Für einen ersten Blick auf einem einzelnen Server ist das ideal: keine Installation, keine Freigabe, kein Risiko. Benutzerdefinierte Ansichten mit Filter auf Ereignis-IDs machen das Ganze erträglicher.

Die Grenze kommt schnell. Die Ereignisanzeige zeigt einen Rechner gleichzeitig, sie aggregiert nicht, und sie korreliert nichts. Wenn ein Domänencontroller am Tag 30.000 Ereignisse 4032 schreibt, ist Scrollen keine Analysemethode, sondern eine Bußübung. Welche Felder die DC-Ereignisse tragen, steht in NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

PowerShell mit Get-WinEvent und wevtutil

Der nächste Schritt ist fast immer PowerShell. Get-WinEvent filtert performant per FilterHashtable oder XPath, wevtutil exportiert ganze Protokolle. Mit ein paar Zeilen hast du eine erste Hitliste nach Zielrechner:

```
# NTLM-Ereignisse der letzten 7 Tage auf diesem Server, gruppiert nach Ereignis-ID
$ev = Get-WinEvent -FilterHashtable @{
  LogName   = 'Microsoft-Windows-NTLM/Operational'
  Id        = 4020,4021,4022,4023
  StartTime = (Get-Date).AddDays(-7) }
$ev | Group-Object Id | Sort-Object Count -Descending | Select-Object Count, Name

# Protokoll für die spätere Auswertung sichern
wevtutil epl Microsoft-Windows-NTLM/Operational C:\Temp\ntlm-op.evtx

# Gegenprüfung: doppelte SPNs in der Gesamtstruktur
setspn -X -F
```

Das ist solide Handarbeit. Problematisch wird es an drei Stellen. Erstens musst du den Meldungstext zerlegen, um an Felder wie „Reason ID“ oder „Target Machine“ zu kommen, und das Format unterscheidet sich zwischen Client-, Server- und DC-Ereignissen. Zweitens läuft das Skript auf einem Rechner; für 300 Rechner brauchst du WinRM, Fehlerbehandlung, Zeitüberschreitungen und eine Ablage. Drittens ist die Gegenprüfung gegen SPNs und DNS ein eigenes Skript, das du mit dem ersten verheiraten musst. Wie das systematisch geht, zeigen Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen und Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern.

TIPP · Zentral sammeln statt herumfahren

Bevor du Skripte auf hundert Rechner verteilst, leite die Ereignisse per Windows Event Forwarding an einen Sammelserver. Dann fragt dein Skript nur noch ein Protokoll ab. Die Anleitung steht in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding. Die Audit-Einstellungen selbst verteilst du per Gruppenrichtlinie, zum Beispiel mit dem NTLM-Audit-GPO-Skript; Schritt für Schritt

erklärt es Erweitertes NTLM-Auditing einschalten: Schritt für Schritt.

Community-Module und Skriptsammlungen

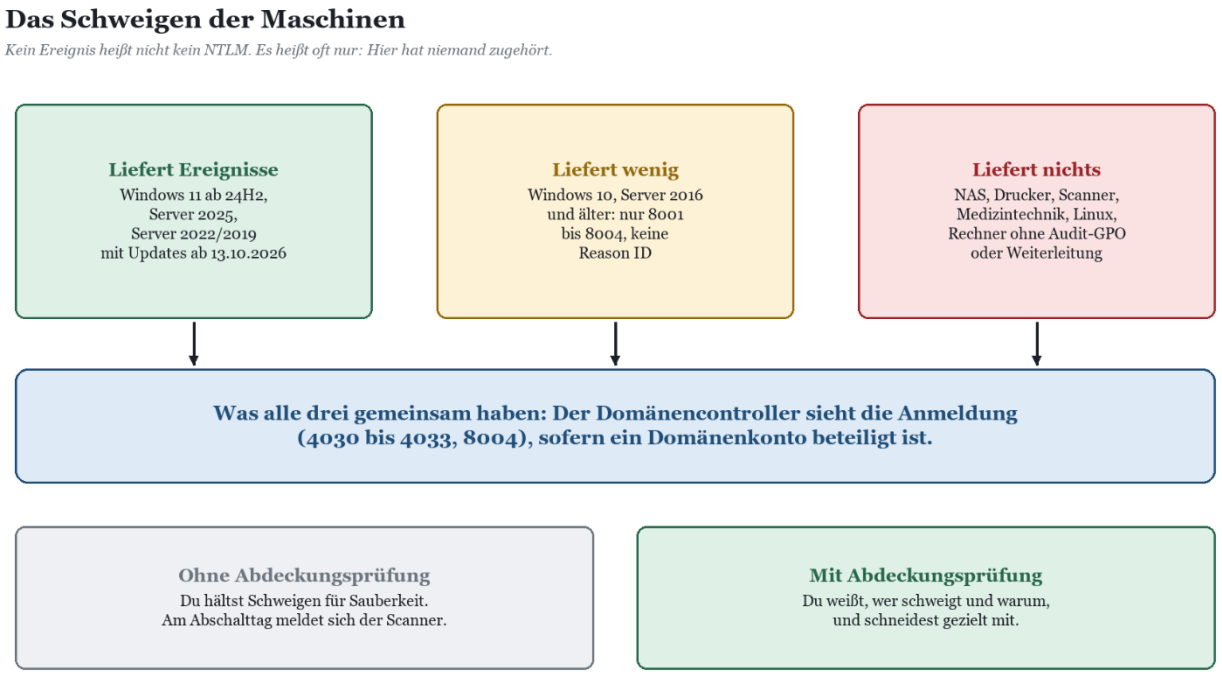
Im Netz kursieren zahlreiche PowerShell-Module und Skripte, die NTLM-Ereignisse einsammeln, in CSV schreiben oder als Tabelle aufbereiten. Viele davon sind gut gemacht und ein sinnvoller Startpunkt, vor allem für die klassischen Ereignisse 8001 bis 8004. Drei Dinge solltest du trotzdem prüfen: ob das Modul die neuen Ereignisse 4020 bis 4033 mit Reason ID überhaupt kennt, wer es pflegt, wenn Microsoft am Format dreht, und ob du Code aus dem Netz mit Leserechten auf die Protokolle deiner Domänencontroller laufen lassen möchtest.

WARNUNG · Das Skript, das nur einer versteht

In fast jeder Umgebung gibt es das eine Auswerteskript, das ein Kollege 2019 geschrieben hat. Es funktioniert. Niemand weiß genau, warum. Der Kollege ist inzwischen bei der Konkurrenz. Wenn deine NTLM-Analyse an so einem Skript hängt, hast du kein Werkzeug, sondern eine Wette.

Netzwerkanalyse mit Wireshark

Für Geräte ohne Windows-Ereignisprotokoll ist der Mitschnitt oft die einzige Wahrheit. Der Filter ntlmssp zeigt NTLM in SMB, HTTP, LDAP und RPC, inklusive Version, Domäne, Benutzer und Zielrechner. Das ist präzise und unbestechlich. Es ist aber auch punktuell: Du siehst nur, was über die Leitung lief, an der du gerade mitgeschnitten hast, und nur in dem Zeitraum, in dem du dabei warst. Für die Fläche ist das nichts, für den Einzelfall unschlagbar. Wie du gezielt mitschneidest, beschreiben NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen und NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.



Skizze: Ereignisabdeckung nach Gerätetyp und Betriebssystem

AD-Audit-Suiten und der NTLM Diagnostiker

Zwischen Selbstbau und Spezialwerkzeug liegen die großen Audit- und SIEM-Lösungen. Und dann gibt es Werkzeuge, die genau eine Frage beantworten wollen: Wie kommt diese Domäne ohne NTLM aus?

AD-Audit-Suiten und SIEM: breit aufgestellt

Viele Häuser haben bereits eine Audit-Suite für Active Directory oder ein SIEM im Einsatz. Diese Lösungen sind stark im zentralen Sammeln, im Aufbewahren, in Alarmierung und in Compliance-Berichten über viele Themen hinweg. Wenn deine Ereignisse dort ohnehin ankommen, ist es naheliegend, auch NTLM dort zu suchen, und für Fragen wie „wer meldet sich wo an“ ist das eine gute Quelle.

Für die NTLM-Ablösung sind die Stärken aber oft an der falschen Stelle. Eine Suite sammelt, sie diagnostiziert in der Regel nicht die Ursache je Verbindung, sie gleicht die Reason ID nicht von sich aus mit SPNs und DNS ab, und eine Abschalt-Simulation für eine OU ist kein typischer Bestandteil. Dazu kommen Lizenzmodelle, die sich häufig nach Benutzern, Servern oder Datenvolumen richten. Das ist kein Mangel dieser Produkte, sie sind schlicht für eine andere Aufgabe gebaut. Wer eine Suite hat, sollte sie als Datenquelle nutzen und prüfen, ob die fehlenden Schritte mit vertretbarem Aufwand ergänzt werden können.

NTLM Diagnostiker: gebaut für genau diese Ablösung

Der NTLM Diagnostiker ist ein Werkzeug, das nur eine Aufgabe hat: zu zeigen, wo in deiner Domäne NTLM läuft, warum, und was passiert, wenn du es abschaltest. Er arbeitet ausschließlich lesend. Er ändert keine Gruppenrichtlinien, keine Registrierungswerte und keine Konten, ein normales Domänenkonto mit Lesezugriff auf das Active Directory und die Ereignisprotokolle genügt. Einstellungen schlägt er vor, umsetzen tust du sie selbst.

Als Ereignisquellen nutzt er die Domänencontroller direkt, einen Windows Event Collector oder die Direktabfrage einzelner Server. Er liest die Ereignisse 4020 bis 4025, 4030 bis 4033 und 8001 bis 8004 und kann Wireshark-Mitschnitte importieren, um stille Geräte einzubeziehen. Bei den Kriterien aus dem ersten Abschnitt sieht das so aus:

- **Ursache je Verbindung:** Die Ursachen-Engine wertet die Reason ID aus und prüft gegen SPNs und DNS. Heraus kommt eine Diagnose mit Abhilfe, Aufwand und Risiko.
- **Stille Geräte:** Abdeckungsmonitor und OS-Landkarte zeigen, welche Rechner Ereignisse liefern und welche nicht, inklusive Test der Weiterleitungskette.
- **Simulation:** Die Abschalt-Simulation zeigt für eine OU, eine Servergruppe oder die Domäne, welche Verbindungen betroffen wären.
- **Bericht:** Word-Bericht für Management, CISO und IT-Leitung, Excel- und CSV-Export der Rohdaten.
- **Weitere Sichten:** Readiness-Ampel, NTLMv1-Hitliste mit Konto, Ziel und Prozess, Kommunikationsmatrix, Konten-Sicht und Sicherheitsflaggen für Verbindungen ohne MIC, Kanalbindung oder Sitzungsschlüssel.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Vom Express-Befund zur Abschaltentscheidung

1. Express starten: Die kostenlose Edition liefert in rund fünf Minuten einen Befund aus den DC-Ereignissen der letzten Tage, mit Readiness-Ampel, NTLMv1-Anzahl samt Top 5 und Kontenzählung. Kein Collector nötig.

2. Ampel ernst nehmen: Zeigt die Readiness-Ampel Rot, fehlen Daten. Erst die Abdeckung nachbessern, dann auswerten. Der Abdeckungsmonitor sagt dir, welche Rechner schweigen.

3. Ursachen lesen: In der Kommunikationsmatrix filterst du nach Quelle, Ziel, Konto, Protokoll und Reason ID. Die Ursachen-Engine liefert die Abhilfe gleich mit, die NTLMv1-Hitliste die dringendsten Fälle.

4. Stille Geräte ergänzen: Mitschnitte von Drucker- oder Labornetz per Wireshark-Import einlesen. Übernommen werden nur NTLM-Metadaten.

5. Simulieren und berichten: Abschalt-Simulation für die erste OU, dann Word-Bericht für die Entscheidung. Den vollen Umfang testest du 7 Tage lang; lizenziert wird pro aktivem Computerkonto.

Was der Diagnostiker heute nicht kann, gehört auch in einen fairen Vergleich. Ein Katalog bekannter NTLM-Anwendungen, ein Generator für Ausnahmelisten und Skripte, ein Phasenplan pro OU, ein Kerberos-Gegencheck und ein Verlauf über mehrere Erfassungen sind geplant, aber noch nicht verfügbar. Bis dahin sind das Aufgaben für dich, für die Serie und gegebenenfalls für die Beratung zur NTLM-Ablösung.



Grün: liefert das Werkzeug selbst. Gelb: geht, wenn du Skripte schreibst und pflegst. Rot: nicht vorgesehen.

Skizze: Arbeitsschritte der NTLM-Analyse und ihre Abdeckung, vereinfacht

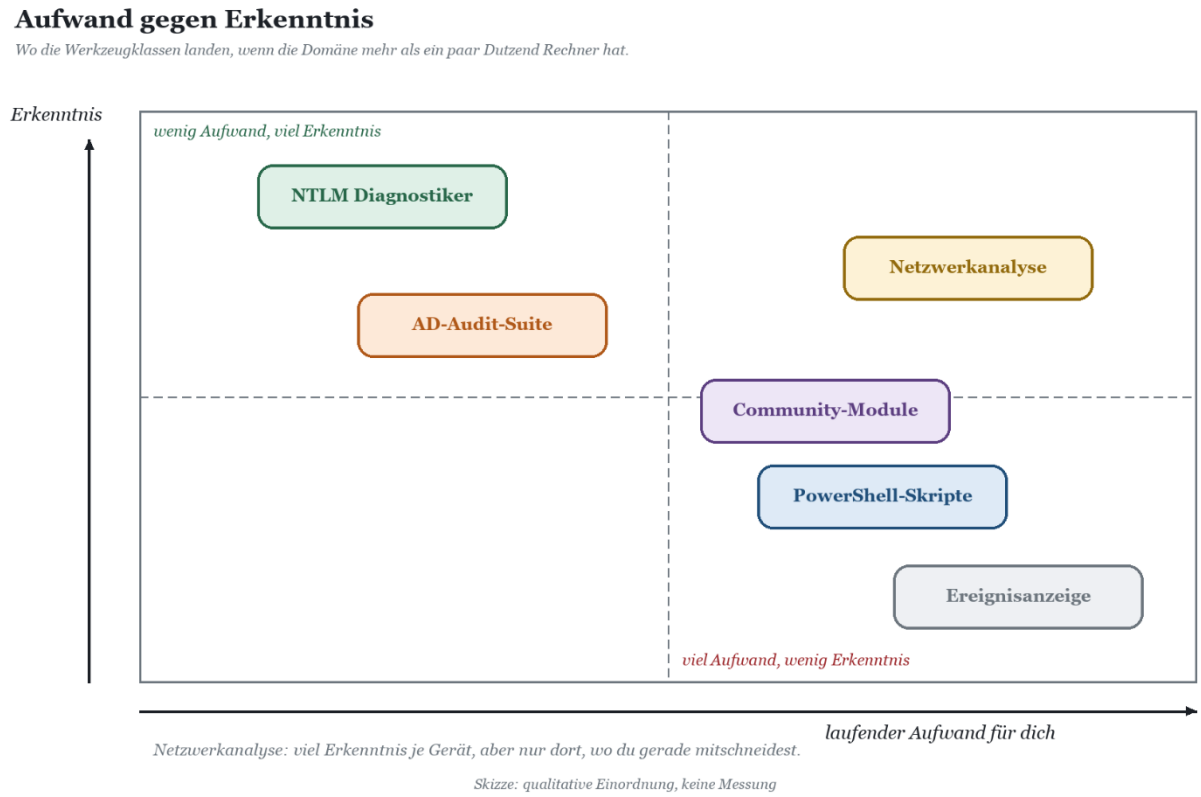
Der Vergleich: alle Werkzeuge in einer Tabelle

Jetzt die Übersicht. Die Bewertung ist bewusst grob: „ja“ heißt, das Werkzeug liefert es selbst; „Handarbeit“ heißt, es geht, wenn du Skripte schreibst oder Daten zusammenführst; „nein“ heißt, nicht vorgesehen. Bei AD-Audit-Suiten hängt vieles vom konkreten Produkt ab, die Spalte beschreibt den typischen Fall.

Kriterium	Ereignisanzeige	PowerShell	Community-Module	AD-Audit-Suite	Netzwerkanalyse	NTLM Diagnostiker
Ursache je Verbindung	Reason ID ablesen, je Ereignis	Handarbeit	teilweise	meist nur Rohdaten	Version, Ziel, kein Grund	ja, mit Abhilfe
SPN/DNS-Gegenprüfung	nein	Handarbeit mit setspn	selten	selten	nein	ja

Stille Geräte	nein	Handarbeit	selten	teilweise, je Agent	ja, punktuell	Abdeckungsmonitor plus Mitschnitt-Import
Simulation	nein	nein	nein	selten	nein	ja, je OU, Servergruppe, Domäne
Bericht	nein	Handarbeit	CSV	ja, allgemein	nein	Word-Bericht, Excel/CSV
Aufwand	gering, skaliert nicht	mittel bis hoch, laufend	mittel, Pflegerisiko	hoch bei Einführung	hoch je Fall	gering, Express in Minuten
Lizenzmodell	kostenlos	kostenlos	meist kostenlos	nach Benutzern, Servern oder Volumen	kostenlos	Express kostenlos, sonst pro aktivem Computerkonto

Zwei Dinge fallen auf. Erstens: Kein Werkzeug ist überflüssig. Die Netzwerkanalyse bleibt für Geräte ohne Protokoll unverzichtbar, PowerShell für schnelle Einzelfragen, die Audit-Suite für Aufbewahrung und Alarmierung. Zweitens: Die Spalten Ursache, Gegenprüfung, Simulation und Bericht sind genau die, die über Erfolg oder Misserfolg der Ablösung entscheiden, und genau dort trennen sich die Werkzeuge.



Was Handarbeit in echten Zahlen bedeutet

AUS DER PRAXIS · Musterwerk GmbH, 420 Rechner, drei Standorte

Das Team der Musterwerk GmbH hat zunächst mit PowerShell begonnen. Nach zwei Wochen gab es

ein Skript, das die Ereignisse von zwei Domänencontrollern einsammelt und nach Zielrechner gruppiert. Ergebnis: 1,8 Millionen Ereignisse im Monat, 230 Quell-Ziel-Paare, davon gut 60 mit Reason ID 7.

Offen blieb: Welche der 60 IP-Zugriffe stammen aus Anmeldeskripten, welche aus Maschinen in der Fertigung? Welche Rechner fehlen ganz, weil die Audit-GPO dort nie angekommen ist? Und was passiert, wenn die OU Verwaltung NTLM verweigert? Für jede dieser Fragen wäre ein weiteres Skript nötig gewesen. Die Werkzeugfrage hat sich dann recht schnell von selbst beantwortet.

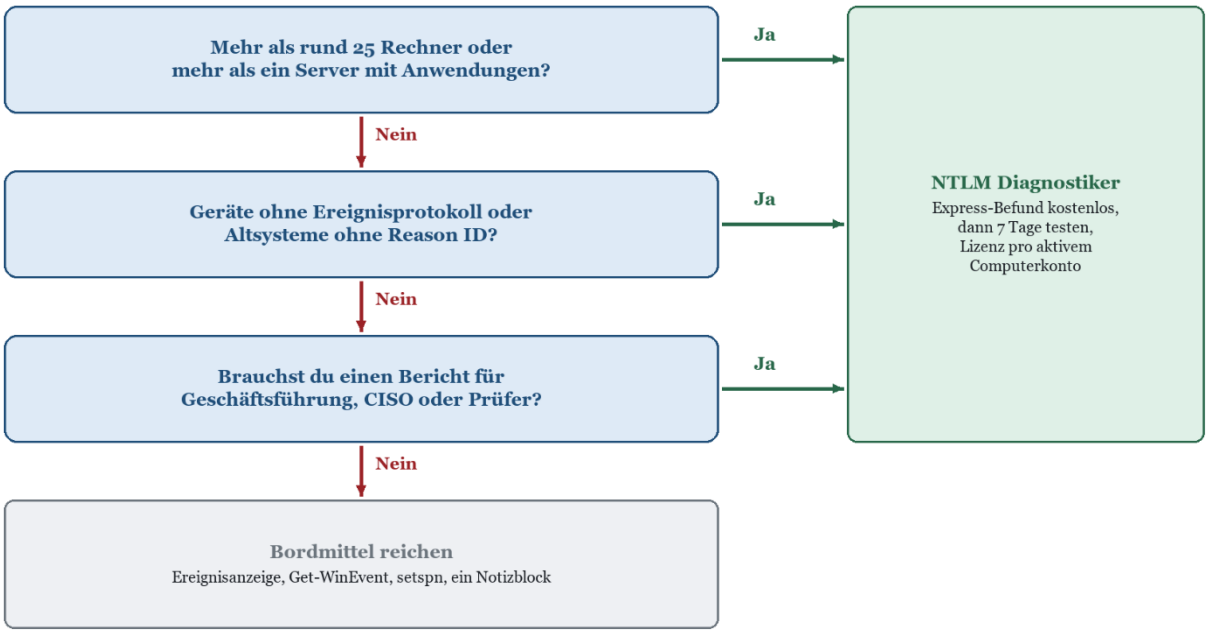
Die Kosten der Handarbeit stehen nicht auf einer Rechnung, sie stehen im Kalender. Wer ehrlich zählt, kommt bei mittleren Umgebungen schnell auf mehrere Personentage für Skripte, Fehlersuche und das Zusammenführen von Tabellen, und zwar bei jeder neuen Erfassung wieder. Wie du den Gesamtaufwand realistisch planst, steht in NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand.

Wann Bordmittel wirklich reichen

Jetzt der ehrliche Teil. Bordmittel reichen, wenn die Umgebung sehr klein ist: ein Domänencontroller, eine Handvoll Server, wenige Dutzend Clients, alles auf aktuellen Betriebssystemen mit erweitertem Auditing, kein Labor, keine Produktion, keine Geräte mit eigenem Kopf. Die Sparfuchs & Partner Steuerberatungs GmbH mit 20 Arbeitsplätzen ist so ein Fall. Dort schaust du dir die Ereignisse auf dem Domänencontroller an, behebst zwei IP-Pfade und einen Multifunktionsdrucker und bist fertig. Ein Bericht? Eine E-Mail an die Partner genügt.

Reichen Bordmittel? Der ehrliche Entscheidungsbaum

Drei Fragen. Wenn du alle mit Nein beantwortest, spar dir das Geld.



Skizze: Entscheidungshilfe, Schwellenwerte als Faustregel

Sobald eine der drei Fragen aus der Skizze mit Ja beantwortet wird, kippt die Rechnung. Ab dann ist der Diagnostiker die naheliegende Wahl: nicht, weil Bordmittel schlecht wären, sondern weil er genau die Schritte erledigt, die du sonst selbst baust. Und weil der Express-Befund kostenlos ist, kannst du diese Entscheidung auf Basis deiner eigenen Daten treffen statt auf Basis eines Bauchgefühls.

TIPP · Kombinieren statt ersetzen

Die sinnvollste Werkzeugkette in mittleren Umgebungen: Audit-Einstellungen per Gruppenrichtlinie, Ereignisse per Windows Event Forwarding sammeln, Auswertung im Diagnostiker, Mitschnitte für stille Geräte, PowerShell für schnelle Rückfragen. Eine vorhandene Audit-Suite bleibt für Aufbewahrung und Alarmierung zuständig.

Sonderfälle: Kliniken, Systemhäuser und Sicherheitsfragen

Kliniken und Verwaltungen

In Kliniken ist das Verhältnis von Windows-Rechnern zu stillen Geräten besonders ungünstig. Medizintechnik, Laborgeräte und Fachanwendungen schreiben keine Ereignisse, laufen aber oft mit Dienstkonten oder lokalen Konten gegen Windows-Server. Hier entscheidet das Kriterium „stille Geräte“ über alles. Hintergründe stehen in NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen, zu Konten in Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen und Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden.

Systemhäuser mit vielen Kunden

Wer die Analyse nicht einmal, sondern bei vielen Kunden macht, braucht Wiederholbarkeit. Ein Skript, das bei Kunde A funktioniert, scheitert bei Kunde B an einem anderen Sprachpaket im Meldungstext oder an einer fehlenden WinRM-Freigabe. Ein fest definiertes Werkzeug mit gleichem Bericht spart hier am meisten. Das Vorgehen beschreibt NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

Relay-Risiken und NTLMv1

Nicht jede NTLM-Verbindung ist gleich gefährlich. NTLMv1 ist seit Oktober 2026 ohnehin auf dem Rückzug, siehe NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht und BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme. Verbindungen ohne MIC oder Kanalbindung sind Kandidaten für Relay-Angriffe. Mit Bordmitteln findest du NTLMv1 über die Ereignisse 4024 und 4025 (Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen), für die Relay-Bewertung brauchst du Mitschnitte oder ein Werkzeug, das diese Merkmale auswertet. Wie du dich schützt, steht in NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

WICHTIG · Datenschutz gilt für jedes Werkzeug

Egal ob Ereignisanzeige, Skript, Suite oder Diagnostiker: Ein NTLM-Audit verarbeitet Konten- und Rechnernamen. Kläre Zweck, Speicherdauer und gegebenenfalls die Beteiligung des Betriebsrats, bevor du sammelst. Einzelheiten findest du in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

FAQ: NTLM-Analyse-Werkzeuge im Vergleich

Reicht die Ereignisanzeige für eine NTLM-Analyse?

Für einen einzelnen Server oder eine sehr kleine Domäne ja. Sobald du mehrere Rechner, ältere Systeme ohne Reason ID oder Geräte ohne Ereignisprotokoll hast, fehlen Aggregation, Abdeckung und Gegenprüfung.

Kann ich mit PowerShell alles nachbauen, was ein Spezialwerkzeug kann?

Grundsätzlich ja, PowerShell kann alles lesen, was Windows protokolliert. Die Frage ist, ob du Sammeln, Parsen, SPN- und DNS-Abgleich, Abdeckungsprüfung, Simulation und Bericht selbst bauen und dauerhaft pflegen willst.

Unsere AD-Audit-Suite sammelt bereits alle Ereignisse. Brauchen wir trotzdem etwas anderes?

Nicht unbedingt für das Sammeln. Prüfe, ob die Suite die Ereignisse 4020 bis 4033 mit Reason ID auswertet, Ursachen gegen SPNs und DNS abgleicht und eine Abschalt-Simulation bietet. Fehlt das, ergänzt ein spezialisiertes Werkzeug die Suite, statt sie zu ersetzen.

Ändert der NTLM Diagnostiker etwas in meiner Domäne?

Nein. Er arbeitet ausschließlich lesend und verändert weder Gruppenrichtlinien noch Registrierungswerte noch Konten. Die Audit-Einstellungen verteilst du selbst, etwa mit dem separaten NTLM-Audit-GPO-Skript.

Was kostet der Einstieg?

Die Edition Express ist kostenlos und liefert einen Fünf-Minuten-Befund aus den DC-Ereignissen. Den vollen Funktionsumfang kannst du 7 Tage testen. Lizenziert wird pro aktivem Computerkonto.

Wie finde ich NTLM bei Druckern und NAS-Systemen?

Diese Geräte schreiben kein Windows-Ereignisprotokoll. Du siehst sie indirekt auf dem Server oder Domänencontroller, gegen den sie sich anmelden, oder direkt im Netzwerkmitschnitt. Der Diagnostiker kann solche Mitschnitte importieren.

Was ist mit Windows 10 und Windows Server 2016?

Diese Systeme liefern nur die klassischen Ereignisse 8001 bis 8004 ohne Reason ID. Die Ursache musst du dort aus dem Zusammenhang erschließen, etwa über die DC-Ereignisse oder einen Mitschnitt. Für die Kerberos-Seite lohnt ein Blick auf Microsoft Kerberos.

Wer hilft, wenn wir das nicht allein stemmen wollen?

Die Beratung zur NTLM-Ablösung unterstützt bei Werkzeugauswahl, Erfassung und Abschaltplan, die Schulung zum NTLM Diagnostiker bringt dein Team auf Stand.

Fazit: das richtige Werkzeug für die letzte Meile

Die NTLM-Analyse scheitert selten am Sehen, sondern fast immer am Verstehen. Ereignisanzeige und PowerShell zeigen dir zuverlässig, dass NTLM läuft. Netzwerkanalyse zeigt dir, was bei stillen Geräten passiert. Audit-Suiten bewahren alles brav auf. Die Fragen, die über eine erfolgreiche Abschaltung entscheiden, nämlich warum, wer schweigt und was bricht, beantwortet keine dieser Lösungen von sich aus.

In sehr kleinen Umgebungen beantwortest du sie im Kopf, und das ist völlig in Ordnung. Ab einer gewissen Größe brauchst du ein Werkzeug, das Ursache, Gegenprüfung, Abdeckung, Simulation und Bericht zusammenbringt, und das ist der NTLM Diagnostiker. Ein Express-Befund kostet dich fünf Minuten und nichts sonst. Das ist billiger als der Montag nach der Abschaltung, an dem der Scanner im Keller beschließt, dass er nie wieder scannen wird. Danach geht es mit NTLM schrittweise abschalten, ohne dass etwas ausfällt und Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern an die Umsetzung.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet

› NTLM-Nutzung ermitteln: der komplette Leitfaden

› NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten
› Keine Sichtverbindung zum DC: Reason-ID 9, IAKerb und lokales KDC
› NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen
› NTLM schrittweise abschalten, ohne dass etwas ausfällt