

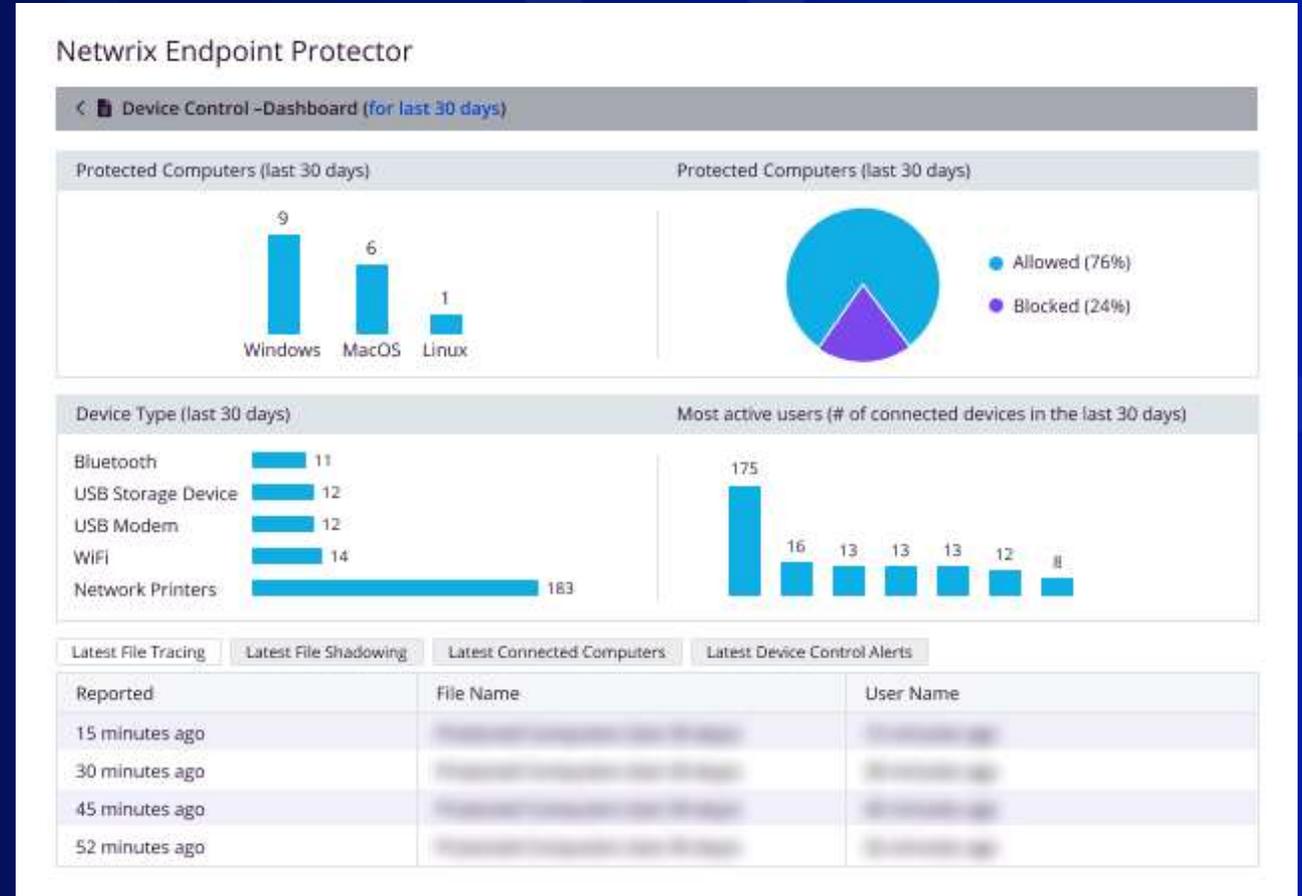
Data Loss Prevention

Funktionen & Anforderungen für Compliance und Risikomanagement (NIS2)

Data Loss Prevention

Grundlegendes und Ziel

Überwachen, kontrollieren und blockieren Sie die Exfiltration sensibler Daten von den Endpunkten der Mitarbeiter. Verhindern Sie Betriebsunterbrechungen, regulatorische Probleme und Reputationsschäden, die aus Datenschutzverletzungen resultieren.



Data Loss Prevention – Aufgaben



**IDENTIFYING
SENSITIVE DATA**



**END USER FRICTION
& PRODUCTIVITY
CONCERNS**



**REMOTE TEAMS
AND OFFLINE
ENDPOINTS**



**CONSISTENT POLICY
ENFORCEMENT
ACROSS MULTI-OS**



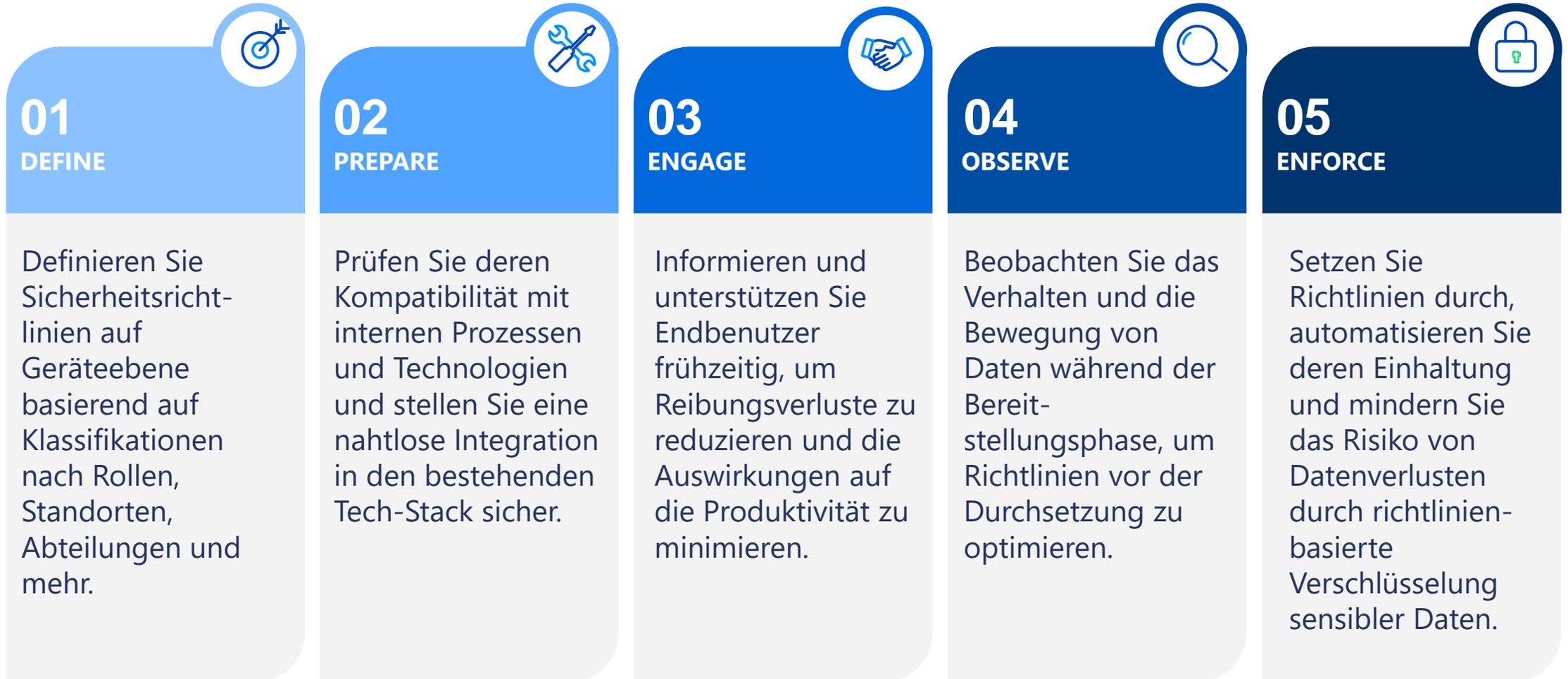
**COMPLIANCE
REQUIREMENTS**



“70% of all data breach incidents occur via the endpoint”.

-IBM Cost of a Data Breach Report 2023

Data Loss Prevention – WIE?



Data Loss Prevention – Anwendungsbeispiele

| ANWENDUNG | REDUZIERTES RISIKO | ERHÖHTE SICHERHEIT | ZEITERSPARNIS | KOSTEN-ERSPARNIS | COMPLIANCE |
|--|--------------------|--------------------|---------------|------------------|------------|
| Verhindern von Datenlecks durch externe Speichergeräte | X | X | | | X |
| Verhindern von Datenübertragungen in Cloud-Speicher | X | X | | | X |
| Verhindern von Datenlecks per E-Mail | X | X | | | X |
| Verwaltung von Endpunktrichtlinien für mehrere Betriebssysteme | X | X | X | X | X |
| Insider Threat Detection und Response | X | X | | X | |
| Data Discovery & Classification | X | X | | | X |

netwrix

Data Loss Prevention

DANKE, Sie finden uns in Halle 7A am Stand 425