

Whitepaper



# IAM für Mitarbeiter: Höhere Sicherheit und Widerstandsfähigkeit für kritische Infrastrukturen

[cpl.thalesgroup.com](http://cpl.thalesgroup.com)

**THALES**  
Building a future we can all trust

# Inhalt

- 3 Einleitung**
- 3 Herausforderungen beim IAM für kritische Infrastrukturen**
  - 3 Einzigartige Komplexität von Systemen und Netzwerken
  - 4 Fokus auf die Einhaltung von Vorschriften und Standards
  - 4 Betriebskontinuität und -stabilität
  - 4 B2B-Anwendungsfälle
- 5 Anforderungen an die IAM-Compliance**
- 6 Bewährte Verfahren für das IAM in kritischen Infrastrukturen**
  - 6 Einsatz von Multi-Faktor-Authentifizierung (MFA)
  - 6 Sichere Kommunikation und Einsatz moderner Protokolle
  - 6 Ausweitung der Nutzung von Public Key Infrastructure (PKI) und Fast Identity Online (FIDO)
  - 6 Plan für Hybrid- und Multi-Cloud-Umgebungen
- 7 Überlegungen zur Umsetzung des IAM**
  - 7 Phishing-sichere Authentifizierung
  - 7 Ausfallsicherheit und Redundanz
  - 7 Risiken durch Dritte
  - 7 Authentifizierungserlebnis für verschiedene Benutzer
- 8 Der Mehrwert von Thales Workforce IAM Solutions**
- 8 Sichere Geschäftskontinuität mit SafeNet Trusted Access Continuum**
- 9 Ein vielschichtiges Unterfangen**

# Einleitung

**Kritische Infrastrukturen wie Stromnetze, Wasseraufbereitungsanlagen, Verkehrssysteme, Öl- und Gasraffinerien und Gesundheitsdienste werden immer vernetzter und digitaler. Moderne Stromnetze nutzen fortschrittliche Sensoren und IoT-Geräte zur Überwachung und Steuerung des Stromflusses und damit zur Steigerung ihrer Effizienz und Zuverlässigkeit. Wasseraufbereitungsanlagen verfügen über automatische Steuerungssysteme, die den Aufbereitungsprozess optimieren und eine sichere Wasserverteilung gewährleisten. Intelligente Verkehrsmanagementsysteme nutzen Echtzeitdaten, um Staus zu reduzieren und die Sicherheit im Straßenverkehr zu erhöhen.**

**All diese Fortschritte bieten erhebliche Effizienzvorteile. Ihre Vernetzung bedeutet jedoch auch, dass sie zunehmend anfällig für Cyberangriffe sind, die zu Ausfallzeiten, Unterbrechungen der Lieferkette, Umweltschäden und sogar zu Bedrohungen für Menschenleben und die nationale Sicherheit führen können.**

**Die Identitäts- und Zugriffsverwaltung (Identity and Access Management – IAM) ist entscheidend für den Schutz kritischer Infrastrukturen, da sie kontrolliert, wer Zugriff auf welche Ressourcen hat, und sicherstellt, dass nur autorisiertes Personal bestimmte Aufgaben ausführen kann.**

**In diesem Whitepaper betrachten wir die Herausforderungen kritischer Infrastruktursektoren bei der Umsetzung von IAM-Lösungen für Mitarbeiter, wie z. B. Compliance-Anforderungen, und stellen bewährte Verfahren zur Erhöhung ihrer Sicherheit und Widerstandsfähigkeit vor.**

## Herausforderungen beim IAM für Mitarbeiter in kritischen Infrastrukturen

Kritische Infrastrukturmgebungen bestehen aus komplexen und heterogenen Systemen, die sich aus den unterschiedlichsten Technologien, Geräten und Anwendungen zusammensetzen. Diese Systeme werden parallel zu herkömmlichen IT- und älteren OT-Umgebungen (Operational Technology) eingesetzt und schaffen so eine vielschichtige und vernetzte Landschaft.

In dieser Landschaft ist die Verwaltung von Identitäten und Zugriffsrechten aufgrund der Verschiedenartigkeit der beteiligten Systeme eine komplexe Herausforderung, da jedes System gegebenenfalls unterschiedliche Protokolle, Sicherheitsmaßnahmen und Verwaltungsansätze erfordert. Diese Komplexität wird durch das Erfordernis zur Einhaltung strenger Sicherheitsstandards und einer reibungslosen Integration unterschiedlicher Komponenten, um kritische Vermögenswerte und Daten vor unbefugtem Zugriff und potenziellen Bedrohungen zu schützen, noch weiter gesteigert.

Im vergangenen Jahr waren verschiedene kritische Systeme wie Energie, Gesundheitswesen, Finanzen, Kommunikation, Fertigung und Transport wiederholt das Ziel von Cyberangriffen. In der Ausgabe Critical Infrastructure des 2024 Thales Data Threat Report berichteten fast 93 % der Befragten aus kritischen Infrastruktursektoren von einer Zunahme dieser Angriffe. Sicherheitslücken in kritischen Infrastrukturen können durch die Unterbrechung wesentlicher Dienste schwerwiegende Folgen haben und sogar Leben gefährden. Eine Gewährleistung der Sicherheit dieser Systeme ist daher wichtiger denn je.

Die Integration all dieser Systeme und die Notwendigkeit ihrer Kompatibilität mit älteren Technologien erfordert spezialisierte IAM-Lösungen.

Kritische Infrastrukturmgebungen integrieren eine Vielzahl verschiedener Systeme und Technologien und zeichnen sich durch Komplexität und Vielschichtigkeit aus. Ihre Komplexität ergibt sich aus mehreren Schlüsselfaktoren:

### Einzigartige Komplexität von Systemen und Netzwerken

Kritische Infrastrukturmgebungen bestehen aus veralteten Technologien, industriellen Kontrollsystemen (Industrial Control Systems – ICS) und den immer verbreiteteren IoT-Geräten. Die Verwaltung von Identitäten und Zugriffsrechten auf diesen verschiedenen Plattformen stellt eine einzigartige Herausforderung dar, die spezialisierte IAM-Lösungen erfordert.

Viele kritische Infrastruktursektoren wie Energie, Transport und Wasserwirtschaft sind in hohem Maße von veralteten OT-Systemen abhängig. Bei der Entwicklung dieser Systeme – oft vor Jahrzehnten – wurden moderne Cybersicherheitsbedrohungen nicht berücksichtigt. Tatsächlich waren viele von ihnen nie für eine Verbindung mit dem Internet ausgelegt. Daher weisen sie von sich aus keine Sicherheitsfunktionen und -protokolle zum Schutz vor den heutigen fortgeschrittenen Bedrohungen auf. Die Aktualisierung oder der Austausch von Altsystemen ist aufgrund der Kosten, des Risikos einer Unterbrechung wesentlicher Dienste oder des Mangels an neueren kompatiblen Technologien nicht möglich.

ICS sind für den Betrieb kritischer Infrastrukturen von entscheidender Bedeutung, da sie physische Prozesse steuern und überwachen. Zu diesen Systemen gehören SCADA-Systeme (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems) und SPS (Speicherprogrammierbare Steuerungen). ICS werden oft in Umgebungen mit strengen Anforderungen an Verfügbarkeit und Zuverlässigkeit eingesetzt. Jede Störung kann schwerwiegende Folgen haben, von Stromausfällen bis hin zu einer Beeinträchtigung der Wasserversorgung.

Die Verbreitung von IoT-Geräten (Internet of Things – Internet der Dinge) in kritischen Infrastrukturmgebungen hat diese Komplexität noch einmal erhöht. IoT-Geräte bieten verbesserte Überwachungs-, Steuerungs- und Automatisierungsfunktionen, dadurch jedoch auch eine größere Angriffsfläche. Viele IoT-Geräte verfügen nur über begrenzte Rechenleistung und Speicherkapazität, was den Einsatz herkömmlicher Sicherheitsmaßnahmen erschwert. Außerdem fand das Thema Sicherheit bei der Entwicklung vieler dieser Geräte keine Berücksichtigung.

### Fokus auf die Einhaltung von Vorschriften und Standards

Kritische Infrastrukturektoren unterliegen strengen regulatorischen Anforderungen und Branchenstandards, die darauf ausgelegt sind, sensible Daten zu schützen, die Betriebsstabilität zu gewährleisten und vor Cyber-Bedrohungen zu schützen. Diese Vorschriften, wie z. B. CISRA oder NIS 2, variieren je nach Sektor und Region und schreiben spezifische Compliance-Verpflichtungen für IAM-Lösungen vor.

IAM-Lösungen müssen an diese regulatorischen Rahmenbedingungen angepasst werden können und für den Nachweis der Compliance robuste Prüfpfade, Zugriffskontrollen und Berichtsmechanismen bereitstellen. Außerdem müssen sie flexibel genug sein, um sektorspezifische Nuancen zu berücksichtigen, und sicherstellen, dass Sicherheitsmaßnahmen die betriebliche Effizienz nicht beeinträchtigen.

### Betriebskontinuität und -stabilität

Der ununterbrochene Betrieb kritischer Infrastrukturen ist entscheidend, da jede Unterbrechung erhebliche wirtschaftliche, soziale und sicherheitsrelevante Auswirkungen haben kann. IAM-Lösungen müssen so konzipiert sein, dass sie die Sicherheit erhöhen, ohne die Agilität und Effizienz dieser so wichtigen Dienste zu beeinträchtigen. Dazu gehört, dass autorisiertem Personal ein nahtloser Zugriff auf die erforderlichen Systeme und Daten ermöglicht wird, während gleichzeitig ein unbefugter Zugriff, der zu Störungen führen könnte, verhindert wird.

Kritische Infrastrukturektoren umfassen viele verschiedene Interessengruppen wie interne Mitarbeiter, Auftragnehmer, Lieferanten und Aufsichtsbehörden. Jede Gruppe hat unterschiedliche Anforderungen an den Zugriff und Sicherheitsüberlegungen, wodurch die Verwaltung aller Identitäten und Zugriffsrechte oft eine Herausforderung darstellt. IAM-Lösungen müssen detaillierte Zugriffskontrollen bieten, um sicherzustellen, dass jeder Benutzer nur über den minimal erforderlichen Zugriff verfügt, um seine Aufgaben zu erfüllen, ohne kritische Systeme unnötigen Risiken auszusetzen. Regelmäßige Audits und Überprüfungen der Zugriffsrechte sind unerlässlich, um eine schleichende Ausweitung von Berechtigungen zu verhindern und sicherzustellen, dass die Zugriffsebenen auch langfristig auf einem angemessenen Niveau bleiben.

Darüber hinaus müssen IAM-Lösungen eine hohe Verfügbarkeit und Redundanz unterstützen, um sicherzustellen, dass die Funktionen der Zugriffsverwaltung auch bei Systemausfällen oder Cyberangriffen funktionsfähig bleiben. Durch ein Gleichgewicht zwischen Sicherheit und Betriebskontinuität kann das IAM dazu beitragen, die Widerstandsfähigkeit kritischer Infrastrukturen angesichts sich immer weiterentwickelnder Bedrohungen aufrechtzuerhalten.

### B2B-Anwendungsfälle

Obwohl der Schwerpunkt dieses Whitepapers auf B2E-Mitarbeitern liegt, darf die Bedeutung von B2B-Identitäten nicht unterschätzt werden. Viele Unternehmen arbeiten heute mit Beratern, Auftragnehmern, Vertriebshändlern, Maklern, Franchisenehmern, Partnern, Lieferanten, Saison- und Gelegenheitsarbeitern und weiteren Dritten zusammen, die nicht unter die traditionelle Definition von „Mitarbeitern“ fallen. Der 2024 Thales Data Threat Report ergab, dass Cloud, Netzwerke und die unternehmenseigenen Geräte häufiger mit externen Identitäten in Kontakt kommen als mit „traditionellen“ Mitarbeitern. Während interne Mitarbeiter die größte Einzelgruppe der Benutzer mit Zugriff auf Unternehmensnetzwerke darstellen (29 %), machen externe Identitäten von Nicht-Kunden fast die Hälfte (48 %) der gesamten Benutzer aus.

Betreiber kritischer Infrastrukturen arbeiten in ihrer Wertschöpfungskette mit einer Reihe von Drittanbietern zusammen. Einerseits stehen sie mit verschiedenen Lieferanten in Kontakt und andererseits können sie mit Vertriebshändlern, Partnern oder Firmenkunden zusammenarbeiten. Der Energiesektor ist dafür ein gutes Beispiel. Als Stromnetzbetreiber stehen in ihrer Wertschöpfungskette Übertragungs- und Erzeugungsunternehmen am oberen Ende und Versorgungsunternehmen am unteren Ende. In unserem digitalen Zeitalter müssen viele Benutzer dieser Drittanbieter auf Ihre Daten und Anwendungen zugreifen können. Bei richtiger Handhabung ist dieser Zugriff für eine reibungslose Zusammenarbeit entscheidend. Bei schlechter Handhabung kann er jedoch auch zu schwerwiegenden Sicherheitsproblemen führen.

Daher muss die sogenannte B2B IAM effektive Lösungen für die Einbindung und Verwaltung dieser unterschiedlichen Unternehmen sowie der damit verbundenen Mitarbeiter und IT-Teams bieten.

### Einzigartige Anforderungen an B2B IAM

- Einbindung externer Identitäten, die nicht Teil eines Verzeichnisses oder HR-Systems des Unternehmens sind
- Remote-Onboarding
- Konsistente Sicherheit für externe Identitätstypen und Anwendungsfälle
- Unterstützung von Entwicklern
- Delegierte Verwaltung: Ermöglicht eine Benutzerverwaltung durch Drittanbieter
- Beziehungsbasierte Autorisierung: Differenzierte Autorisierung auf der Grundlage komplexer und verschachtelter Beziehungen

## Anforderungen an die IAM-Compliance

Gesetze und Vorschriften zur Cybersicherheit in den Vereinigten Staaten und der Europäischen Union ermutigen nationale Unternehmen im Bereich kritische Infrastrukturen, die Einführung von IAM-Kontrollen für einen robusteren allgemeinen Schutz vor Cyberangriffen in Erwägung zu ziehen. Dazu gehören:

**Finanzdienstleistungen:** Der Finanzdienstleistungssektor muss die folgenden Gesetze beachten: [Sarbanes-Oxley Act \(SOX\)](#), [Gramm-Leach-Bliley Act \(GLBA\)](#) und [Digital Operational Resilience Act \(DORA\)](#). Diese Vorschriften erfordern strenge Kontrollen zum Schutz der Finanzdaten von Kunden und zur Abwehr von Bedrohungen. Eine robuste Zugriffsverwaltung ist eine Hauptanforderung für den Schutz sensibler Daten und die Minimierung externer Risiken.

**Stromnetz:** Die Standards der [North American Electric Reliability Corporation Critical Infrastructure Protection \(NERC CIP\)](#) und die Richtlinie über Netz- und Informationssysteme (NIS-2-Richtlinie) regeln das Stromnetz. Diese Vorschriften legen den Schutz kritischer Cyber-Assets, regelmäßige Risikobewertungen und die Incident-Response-Planung fest. Die NERC CIPs enthalten Anforderungen für die Kontrolle privilegierter Zugriffe, die Zugriffsverwaltung per Fernzugriff und die Aufhebung von Zugriffsrechten.

**Gesundheitswesen:** Das [Health Insurance Portability and Accountability Act \(HIPAA\)](#) legt Standards für den Schutz sensibler Patientendaten fest. Die HIPAA Security Rule verpflichtet Unternehmen zur Umsetzung technischer Sicherheitsmaßnahmen für elektronisch geschützte Gesundheitsinformationen (electronic Protected Healthcare Information – ePHI). Diese technischen Schutzmaßnahmen müssen ein Zugriffskontrollsystem enthalten, um sicherzustellen, dass nur autorisierte Personen auf ePHI zugreifen können.

**Zahlungen:** Der [Payment Card Industry Data Security Standard \(PCI DSS\)](#) 4.0 verlangt strenge Sicherheitsmaßnahmen für den Umgang mit Daten von Karteninhabern. PCI DSS 4.0 enthält strikte Anforderungen für den Zugriff und die Authentifizierung. Konkreter verlangen die PCI-DSS-Anforderungen, dass Einzelpersonen nur dann Zugriff auf Daten von privaten Karteninhabern haben sollten, wenn dies für geschäftliche Zwecke erforderlich ist. Um den individuellen Zugriff noch weiter zu regulieren, schreiben die PCI-DSS-Anforderungen den Einsatz der Zwei-Faktor-Authentifizierung vor.

**Bildung:** Das [Family Educational Rights and Privacy Act](#) von 1974 (FERPA) schützt die Privatsphäre der Bildungsdaten von Schülern. Administratoren müssen klare Zugriffskontrollen einrichten, um die Offenlegung von Informationen auf autorisierte Parteien zu beschränken. Diese Zugriffsrechte sollten rollenbasiert sein und klare Verfahren für die Gewährung und den Entzug des Zugriffs auf der Grundlage von Ereignissen wie der Beförderung oder Kündigung von Mitarbeitern vorsehen.

**Datenschutz:** Immer strengere Vorschriften wie die [Datenschutz-Grundverordnung](#) (DSGVO) und das [California's Consumer Privacy Act](#) (CCPA) legen strikte Datenschutz- und Datensicherheitsrichtlinien fest. IAM-Lösungen müssen sicherstellen, dass der Zugriff auf personenbezogene Daten und deren Verarbeitung ausschließlich autorisierten Benutzern vorbehalten ist. Um die Einhaltung der Vorschriften zu gewährleisten, sind eine umfassende Zugriffsverwaltung und Datenzugriffsprotokolle erforderlich.

### Übersicht über die IAM-Compliance-Anforderungen

Sektor	Verordnung, Gesetz, Standard	Anforderung
Finanzdienstleistungen	SOX, GLBA, DORA	Strenge Zugriffskontrollen zum Schutz von Finanzdaten und zur Minderung von Risiken durch Dritte
Stromnetz	NERC CIP, NIS 2	Detaillierte Zugriffskontrollen, privilegierte Zugriffskontrolle, Fernzugriffsverwaltung
Gesundheitswesen	HIPAA (Health Insurance Portability and Accountability Act)	Zugriffskontrollsystem zum Schutz von ePHI
Zahlungen	PCI DSS 4.0	Strenge Anforderungen für den Zugriff nach dem Need-to-know-Prinzip, MFA ist obligatorisch
Bildungswesen	FERPA	Eingeschränkter Zugriff auf Bildungsdaten von Schülern, Audits und Überwachung
Branchenübergreifend	DSGVO, CCPA	Autorisierter Datenzugriff, Zugriffsverwaltung, Datenzugriffsprotokolle

## Anforderungen an die IAM-Compliance

Gesetze und Vorschriften zur Cybersicherheit in den Vereinigten Staaten und der Europäischen Union ermutigen nationale Unternehmen im Bereich kritische Infrastrukturen, die Einführung von IAM-Kontrollen für einen robusteren allgemeinen Schutz vor Cyberangriffen in Erwägung zu ziehen. Dazu gehören:

**Finanzdienstleistungen:** Der Finanzdienstleistungssektor muss die folgenden Gesetze beachten: [Sarbanes-Oxley Act \(SOX\)](#), [Gramm-Leach-Bliley Act \(GLBA\)](#) und [Digital Operational Resilience Act \(DORA\)](#). Diese Vorschriften erfordern strenge Kontrollen zum Schutz der Finanzdaten von Kunden und zur Abwehr von Bedrohungen. Eine robuste Zugriffsverwaltung ist eine Hauptanforderung für den Schutz sensibler Daten und die Minimierung externer Risiken.

**Stromnetz:** Die Standards der [North American Electric Reliability Corporation Critical Infrastructure Protection \(NERC CIP\)](#) und die Richtlinie über Netz- und Informationssysteme (NIS-2-Richtlinie) regeln das Stromnetz. Diese Vorschriften legen den Schutz kritischer Cyber-Assets, regelmäßige Risikobewertungen und die Incident-Response-Planung fest. Die NERC CIPs enthalten Anforderungen für die Kontrolle privilegierter Zugriffe, die Zugriffsverwaltung per Fernzugriff und die Aufhebung von Zugriffsrechten.

**Gesundheitswesen:** Das [Health Insurance Portability and Accountability Act \(HIPAA\)](#) legt Standards für den Schutz sensibler Patientendaten fest. Die HIPAA Security Rule verpflichtet Unternehmen zur Umsetzung technischer Sicherheitsmaßnahmen für elektronisch geschützte Gesundheitsinformationen (electronic Protected Healthcare Information – ePHI). Diese technischen Schutzmaßnahmen müssen ein Zugriffskontrollsystem enthalten, um sicherzustellen, dass nur autorisierte Personen auf ePHI zugreifen können.

**Zahlungen:** Der [Payment Card Industry Data Security Standard \(PCI DSS\)](#) 4.0 verlangt strenge Sicherheitsmaßnahmen für den Umgang mit Daten von Karteninhabern. PCI DSS 4.0 enthält strikte Anforderungen für den Zugriff und die Authentifizierung. Konkreter verlangen die PCI-DSS-Anforderungen, dass Einzelpersonen nur dann Zugriff auf Daten von privaten Karteninhabern haben sollten, wenn dies für geschäftliche Zwecke erforderlich ist. Um den individuellen Zugriff noch weiter zu regulieren, schreiben die PCI-DSS-Anforderungen den Einsatz der Zwei-Faktor-Authentifizierung vor.

**Bildung:** Das [Family Educational Rights and Privacy Act](#) von 1974 (FERPA) schützt die Privatsphäre der Bildungsdaten von Schülern. Administratoren müssen klare Zugriffskontrollen einrichten, um die Offenlegung von Informationen auf autorisierte Parteien zu beschränken. Diese Zugriffsrechte sollten rollenbasiert sein und klare Verfahren für die Gewährung und den Entzug des Zugriffs auf der Grundlage von Ereignissen wie der Beförderung oder Kündigung von Mitarbeitern vorsehen.

**Datenschutz:** Immer strengere Vorschriften wie die [Datenschutz-Grundverordnung](#) (DSGVO) und das [California's Consumer Privacy Act](#) (CCPA) legen strikte Datenschutz- und Datensicherheitsrichtlinien fest. IAM-Lösungen müssen sicherstellen, dass der Zugriff auf personenbezogene Daten und deren Verarbeitung ausschließlich autorisierten Benutzern vorbehalten ist. Um die Einhaltung der Vorschriften zu gewährleisten, sind eine umfassende Zugriffsverwaltung und Datenzugriffsprotokolle erforderlich.

### Übersicht über die IAM-Compliance-Anforderungen

Sektor	Verordnung, Gesetz, Standard	Anforderung
Finanzdienstleistungen	SOX, GLBA, DORA	Strenge Zugriffskontrollen zum Schutz von Finanzdaten und zur Minderung von Risiken durch Dritte
Stromnetz	NERC CIP, NIS 2	Detaillierte Zugriffskontrollen, privilegierte Zugriffskontrolle, Fernzugriffsverwaltung
Gesundheitswesen	HIPAA (Health Insurance Portability and Accountability Act)	Zugriffskontrollsystem zum Schutz von ePHI
Zahlungen	PCI DSS 4.0	Strenge Anforderungen für den Zugriff nach dem Need-to-know-Prinzip, MFA ist obligatorisch
Bildungswesen	FERPA	Eingeschränkter Zugriff auf Bildungsdaten von Schülern, Audits und Überwachung
Branchenübergreifend	DSGVO, CCPA	Autorisierter Datenzugriff, Zugriffsverwaltung, Datenzugriffsprotokolle

## Bewährte Verfahren für das IAM in kritischen Infrastrukturen

In der Ausgabe Critical Infrastructure des [2024 Thales Data Threat Report](#) ist eine spürbare Verschiebung bei der Art und Weise, wie und von wem der Zugriff kontrolliert wird, erkennbar. Fast die Hälfte (49 %) der Befragten stimmt zu, dass Unternehmen die Kontrolle über ihre Zugriffssicherheit behalten sollten, verglichen mit 58 % in der Befragung von 2022, was auf eine leichte Verschiebung hin zur Nutzung externer Anbieter für die Zugriffssicherheit hindeutet.

Darüber hinaus sind 43 % der Meinung, dass Sicherheitslösungen für den Zugriff von einem anbieterunabhängigen Sicherheitsanbieter und nicht von einem Cloud-Dienstleister bereitgestellt werden sollten, und 39 % stimmen zu, dass eine anbieterunabhängige Lösung für die Zugriffsverwaltung für den Schutz von Multi-Cloud-Umgebungen am besten geeignet ist.

In Bezug auf Zero-Trust-Sicherheit waren 36 % der Befragten im Bereich kritische Infrastruktur der Meinung, dass Zugriffsverwaltung und Authentifizierung eine Schlüsselrolle spielen. Der Bericht zeigt außerdem, dass bei mehr als 50 SaaS-Anwendungen eine genauere Betrachtung der Authentifizierungsabläufe erforderlich ist.

Da Unternehmen im Bereich kritische Infrastruktur von Unternehmensmitarbeitern bis hin zu Fabrikarbeitern und Außendiensttechnikern vielfältige Benutzergruppen aufweisen, erfordert die Ermöglichung von Zero Trust flexible Zugriffsrichtlinien. Um Ressourcen zu schützen, ist für Air-Gapped-Umgebungen ebenfalls eine On-premise-Authentifizierungslösung erforderlich.

### Einsatz von Multi-Faktor-Authentifizierung (MFA)

Starke Authentifizierungsmechanismen wie MFA erhöhen die Sicherheit kritischer Infrastruktursysteme, da sie mehr als eine Form der Verifizierung erfordern. Das ist in der Regel etwas, an das sich der Benutzer erinnern muss, wie ein Passwort, etwas, das er bei sich trägt, wie ein biometrisches Merkmal, und etwas, das ihm zugesandt wird, z. B. ein Token oder eine PIN. MFA verringert das Risiko von kompromittierten Anmeldedaten und unbefugten Zugriffsversuchen deutlich, da sie über Benutzernamen und Passwörter hinaus eine zusätzliche Sicherheitsebene schafft.

### Sichere Kommunikation und Einsatz moderner Protokolle

Die in ICS verwendeten Kommunikationsprotokolle wie [Modbus](#), [DNP3](#) usw. sind oft veraltet und verfügen nicht über inhärente Sicherheitsfunktionen, was sie anfällig für Angriffe macht. IAM-Systeme verwenden moderne Protokolle wie SAML, OIDC und SCIM. Überall dort, wo es zu Überschneidungen zwischen IT- und OT-Umgebungen kommt, sollten Unternehmen im Bereich kritische Infrastruktur diese modernen Protokolle zusammen mit spezialisierten OT-Sicherheitslösungen, die Sicherheit für ältere Protokolle bieten, verwenden.

### Ausweitung der Nutzung von Public Key Infrastructure (PKI) und Fast Identity Online (FIDO)

PKI (public key infrastructure, öffentliche Schlüsselinfrastruktur) spielt bei der Sicherung kritischer Infrastrukturmgebungen nach wie vor eine wichtige Rolle. Sie ermöglicht nicht nur Phishing-resistente Authentifizierungsfunktionen, sondern unterstützt auch Verschlüsselung und digitale Signaturen für die Sicherheit und Integrität von Daten. FIDO ist ein moderner Standard, der sich für die Authentifizierung immer mehr durchsetzt. Mit neueren Multi-Protokoll-Authentifizierungsoptionen können Unternehmen beide Technologien in Kombination nutzen und damit sowohl abwärts- als auch aufwärtskompatibel sein.

Durch die Integration von PKI und FIDO erhalten Unternehmen im Bereich kritische Infrastruktur ein starkes Sicherheitskonzept, das vor unbefugtem Zugriff, Datenschutzverletzungen und anderen Cyber-Bedrohungen schützt – und zwar auch vor Bedrohungen, die von der Lieferkette oder von Drittanbietern ausgehen. Dieser Ansatz gewährleistet die Widerstandsfähigkeit und Zuverlässigkeit wichtiger Dienste angesichts sich verändernder Sicherheitsherausforderungen.

### Plan für Hybrid- und Multi-Cloud-Umgebungen

Bei der digitalen Transformation von Unternehmen ist der Wechsel in die Cloud unvermeidlich. Unternehmen im Bereich kritische Infrastruktur müssen dabei jedoch auf ein hybrides und Multi-Cloud-Ökosystem reagieren und ihre Cybersicherheit und Informationssicherheit entsprechend weiterentwickeln. Bei einem Wechsel in die Cloud müssen sich alle Beteiligten ihrer gemeinsamen Verantwortung bewusst sein. Unternehmen im Bereich kritische Infrastruktur können sich aus verschiedenen Gründen für den Einsatz von Hybrid-IAM entscheiden. Erstens verfügen viele Unternehmen im Bereich kritische Infrastruktur über komplexe und geografisch verteilte IT-Umgebungen, die sich oft aus älteren On-premise-Systemen und modernen Cloud-basierten Anwendungen zusammensetzen. Ein Hybrid-IAM-Ansatz ermöglicht es Unternehmen, Benutzeridentitäten und Zugriffsrechte in dieser vielfältigen Infrastruktur zu verwalten und so einen sicheren und konformen Zugriff auf kritische Ressourcen zu gewährleisten.

Zweitens bietet Hybrid-IAM die Flexibilität und Skalierbarkeit für die Anpassung an sich verändernde Sicherheits- und Compliance-Anforderungen. Unternehmen im Bereich kritische Infrastruktur müssen oft strenge gesetzliche Standards einhalten. Eine Hybrid-IAM-Lösung kann dabei helfen, diese Anforderungen zu erfüllen, und ermöglicht den Unternehmen gleichzeitig eine Skalierung gemäß ihren Anforderungen.

Darüber hinaus ermöglicht die anpassungsfähige Natur des Hybrid-IAM Unternehmen im Bereich kritische Infrastruktur die Implementierung starker Authentifizierungs- und Zugriffskontrollen, wodurch das Risiko eines unbefugten Zugriffs auf sensible Systeme und Daten gemindert wird. Insgesamt ermöglicht Hybrid-IAM diesen Unternehmen die effektive Verwaltung ihrer unterschiedlichen IT-Umgebungen, die Stärkung ihrer Sicherheitsmaßnahmen und die kontinuierliche Einhaltung gesetzlicher Standards.

## Überlegungen zur Umsetzung des IAM

Bei der Implementierung von IAM-Lösungen müssen verschiedene Faktoren berücksichtigt werden, um eine robuste Sicherheit, Integration, Skalierbarkeit und Einhaltung gesetzlicher Standards zu gewährleisten.

### Phishing-sichere Authentifizierung

Nicht alle Formen der MFA (Multi-Faktor-Authentifizierung) sind gleich. Weniger sichere MFA-Optionen wie SMS OTP sollten sofort abgeschafft werden. Unternehmen im Bereich kritische Infrastruktur sollten auf einen breiten Einsatz von Phishing-resistenter Authentifizierung achten. In Verbindung mit adaptiven oder risikobasierten Authentifizierungsmechanismen können Unternehmen das richtige Gleichgewicht zwischen Sicherheit und Benutzererfahrung herstellen. Erwägen Sie die Einführung von FIDO-Passkeys und zertifikatbasierter Authentifizierung für robustere Mechanismen.

### Ausfallsicherheit und Redundanz

Die Implementierung redundanter IAM-Mechanismen und Backup-Authentifizierungssysteme verbessert die Widerstandsfähigkeit kritischer Infrastrukturen und stellt sicher, dass die Zugriffskontrollen auch bei einem Systemausfall oder einem Cybersicherheitsvorfall wirksam bleiben. Dies umfasst die Bereitstellung mehrerer Authentifizierungs- und Autorisierungsebenen, die bei Ausfall der Primärsysteme nahtlos übernehmen und dadurch Ausfallzeiten minimieren und einen sicheren Betrieb gewährleisten.

Redundante IAM-Lösungen sollten alternative Zugriffsmethoden umfassen, um eine kontinuierliche Verfügbarkeit und Zuverlässigkeit zu gewährleisten. Regelmäßige Tests und Aktualisierungen dieser redundanten Systeme sind für die Gewährleistung ihrer ordnungsgemäßen Funktion, wenn sie gebraucht werden, unerlässlich. Darüber hinaus können Unternehmen durch die Integration von Notfallwiederherstellungsplänen und automatisierten Reaktionsprotokollen IAM-Dienste schneller wiederherstellen und die Sicherheitsintegrität bei unerwarteten Unterbrechungen aufrechterhalten.

### Risiken durch Dritte

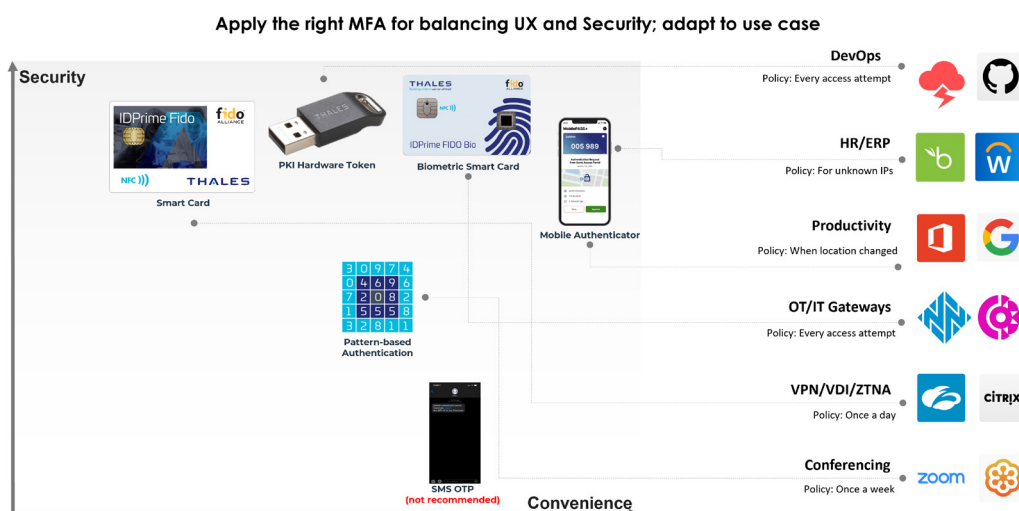
Die meisten Unternehmen im Bereich kritische Infrastruktur müssen sich in einem sehr vielfältigen und komplexen Ökosystem von Drittanbietern zurechtfinden. Dazu gehören unter anderem Lieferanten, Partner und Auftragnehmer. Eine routinierte Zusammenarbeit mit diesen Drittanbietern ist von entscheidender Bedeutung und erfordert den Zugriff auf die Anwendungen und Daten des Unternehmens, das die Plattform bereitstellt. Dies ist ein Grund dafür, dass Verstöße durch Dritte und Angriffe auf die Lieferkette heute immer mehr zunehmen. Unternehmen, die auf Drittanbieter setzen, haben sehr spezifische IAM-Anforderungen, die mit internen oder selbst entwickelten IAM-Systemen nicht immer erfüllt werden können. Solche Unternehmen sollten spezialisierte [B2B-IAM](#)-Lösungen in Erwägung ziehen, da diese für externe Benutzer besser geeignet sind.

### Authentifizierungserlebnis für verschiedene Benutzer

Bei einer so vielfältigen Gruppe interner und externer Benutzer können sich Unternehmen im Bereich kritische Infrastruktur die Forcierung eines einheitlichen Authentifizierungsansatzes nicht leisten. Sie sollten für ihre unterschiedlichen Anforderungen vielmehr verschiedene Authentifizierungsmechanismen mit adaptiven Authentifizierungskontrollen nutzen. Um den richtigen Authentifizierungsweg für verschiedene Benutzergruppen zu identifizieren, müssen die Empfindlichkeit der Zielanwendung oder -daten und der Gesamtkontext des jeweiligen Benutzers berücksichtigt werden.

Doch Unternehmen sollten sogar noch einen Schritt weiter gehen und Mechanismen zur passwortlosen Authentifizierung für interne und externe Benutzer einführen. Nutzen Sie einen Ansatz wie [Passwordless 360°](#), der eine vollständige Palette von Tools für eine Vielzahl verschiedener Benutzer und Anwendungen bietet.

Eine robuste IAM-Lösung sollte rollenbasierte Zugriffskontrollen, Multi-Faktor-Authentifizierung und starke Verschlüsselung unterstützen, um sensible Informationen zu schützen und gleichzeitig sicherzustellen, dass die richtigen Personen zum richtigen Zeitpunkt Zugriff auf die benötigten Daten haben. Darüber hinaus sollten IAM-Systeme Prüfprotokolle und Überwachungsfunktionen enthalten, um unbefugten Zugriff zu erkennen und darauf zu reagieren und so die Integrität und Vertraulichkeit der gemeinsam genutzten Daten zu gewährleisten.



## Der Mehrwert von Thales Workforce IAM Solutions

Die Lösungen von Thales für die Identitäts- und Zugriffsverwaltung bieten mit SafeNet Trusted Access und SAS PCE einen soliden Rahmen für die Sicherung kritischer Infrastrukturen. Diese Lösungen sind darauf ausgelegt, die einzigartigen Herausforderungen und regulatorischen Anforderungen des Bereichs kritische Infrastruktur zu bewältigen.

Funktion	SafeNet Trusted Access	SAS PCE Enterprise (on-premises)
<b>Starke Authentifizierung: Multi-Faktor-Authentifizierung (MFA)</b>	✓ SafeNet Trusted Access bietet mehrstufige Authentifizierung für eine zusätzliche Sicherheitsebene über Benutzernamen und Passwörter hinaus. Durch die Anforderung von zwei oder mehr Verifizierungsformen, wie z. B. einem Passwort und einem biometrischen Scan oder einem einmaligen Passcode, reduziert die MFA das Risiko eines unbefugten Zugriffs durch kompromittierte Anmeldedaten deutlich.	✓ SAS PCE bietet eine MFA mit unterschiedlichen Verifizierungsformen und erhöht damit die Sicherheit. Dieser mehrschichtige Ansatz reduziert das Risiko eines unbefugten Zugriffs deutlich und stellt sicher, dass nur authentifizierte Benutzer Zugriff auf sensible Systeme und Daten erhalten.
<b>Einhaltung von gesetzlichen Vorgaben</b>	✓ SafeNet Trusted Access gewährleistet die Einhaltung von bewährten Verfahren bei verschiedenen Vorschriften, einschließlich DSGVO, CCPA, HIPAA, PCI DSS usw. Dies wird durch strenge Zugriffskontrollen, kontinuierliche Überwachung und detaillierte Prüfprotokolle erreicht und unterstützt Unternehmen dabei, gesetzliche Anforderungen zu erfüllen und Strafen zu vermeiden.	✓ SAS PCE ist für die Einhaltung der Vorgaben von SOX, GLBA, NERC CIP, NIS 2 und weiteren Verordnungen konzipiert. Die Lösung bietet detaillierte Prüfprotokolle und strenge Authentifizierungskontrollen zur Erfüllung gesetzlicher Standards und der Unterstützung von Compliance-Initiativen.
<b>Risikobewertung und Richtlinienkonfiguration</b>	✓ Leistungsstarke Richtlinienkonfiguration, Risikobewertung und Risikobeurteilungen für Endgeräte stellen sicher, dass Sie die passenden Zugriffsrichtlinien für Ihre Anwendungen und Benutzer durchsetzen und die Integrität aller Authentifizierungen wahren.	
<b>Datengestützte Einblicke</b>	✓ Ein vollständiger protokollierter Zugriff sowie der automatische Protokollexport und die nahtlose Integration mit SIEM-Systemen gewährleisten eine kontinuierliche Überwachung und Compliance.	✓ Zeigt Informationen über die Authentifizierung von Benutzern, die Aktivität von Bedienern und andere Faktoren, die für interne und externe Sicherheitsprüfer wichtig sind, an.
<b>Integration mit OT</b>	✓ SafeNet Trusted Access lässt sich in spezialisierte Systeme wie Nozomi Networks Guardian und Claroty SRA (Secure Access) integrieren und ermöglicht so eine nahtlose Integration in OT-Umgebungen (Operational Technology), einschließlich industrieller Steuerungssysteme (ICS) und SCADA-Netzwerke. Dadurch wird sichergestellt, dass Sicherheitsmaßnahmen den Betrieb kritischer Infrastrukturen nicht stören, während gleichzeitig solide Zugriffskontrollen aufrechterhalten werden.	✓ In Verbindung mit dem spezialisierten OT-Gateway unterstützt SAS PCE die nahtlose Integration in SCADA- und ICS-Umgebungen und stellt so sicher, dass Sicherheitsmaßnahmen über IT- und OT-Domains hinweg durchgesetzt werden. Diese Integration ist für die Aufrechterhaltung einheitlicher Richtlinien und den Schutz kritischer Infrastrukturen vor Cybersicherheitsbedrohungen von entscheidender Bedeutung.
<b>Ausfallsicherheit und Redundanz: Hohe Verfügbarkeit, Redundanz und Notfallwiederherstellungsfunktionen</b>	✓ SafeNet Trusted Access kann im Falle einer Dienstunterbrechung auf SAS PCE zurückgreifen. Dies wird über das Modul SafeNet Access Exchange verwaltet.	✓ SAS PCE wurde mit hoher Verfügbarkeit, Redundanz und Notfallwiederherstellungsfunktionen entwickelt und stellt sicher, dass die IAM-Funktionen bei Systemausfällen oder Cybersicherheitsvorfällen betriebsbereit bleiben. Diese Widerstandsfähigkeit ist für die Aufrechterhaltung einer kontinuierlichen Zugriffskontrolle und Sicherheit in kritischen Infrastrukturmgebungen unerlässlich.

## Sichern Sie Ihre Geschäftskontinuität mit STA Hybrid-Zugriffsverwaltung

Aufgrund der Natur kritischer Infrastrukturen ist eine kontinuierliche Dienstverfügbarkeit für den Zugriff auf kritische Ressourcen von entscheidender Bedeutung. Diese Branche wird von Regierungen und Behörden reguliert, um die Dienstverfügbarkeit für die Benutzer durchzusetzen und dabei die Datenhoheit und On-premise-Fallback-Optionen z. B. bei folgenden Ereignissen zu berücksichtigen:

- Nichtverfügbarkeit der Internetverbindung aufgrund eines Cyberangriffs, eines Krieges oder einer anderen Katastrophe.
- Gezielte Trennung des STA vom Internet, um Cyberangriffen vorzubeugen und lange Wartungsfenster zu ermöglichen.

Diese geschäftlichen Anforderungen unterstreichen die Notwendigkeit einer robusten Lösung für die Geschäftskontinuität. Eine solche Lösung sollte die nahtlose Authentifizierung wichtiger Prozesse vor, während und nach der Nichtverfügbarkeit des Internets sicherstellen.

SafeNet Trusted Access (STA) Hybrid ist eine umfassende Lösung für die Identitäts- und Zugriffsverwaltung, die die Vorteile von On-premise- und Cloud-basierter IAM kombiniert. Der hybride Ansatz ermöglicht Unternehmen den nahtlosen Schutz ihrer Benutzeridentitäten und die Verwaltung von Zugriffsrechten in verschiedenen IT-Umgebungen, einschließlich On-premise-Anwendungen und Cloud-basierten Diensten.

STA Hybrid erfüllt darüber hinaus die Compliance-Anforderungen durch die erforderliche Flexibilität und Kontrolle zur Gewährleistung eines sicheren Zugriffs auf kritische Ressourcen. Mit seinen adaptiven Authentifizierungs- und Single-Sign-on-Funktionen bietet SafeNet Trusted Access Hybrid ein nahtloses Benutzererlebnis ohne Kompromisse bei der Sicherheit.

STA Hybrid Access Management wird kann auf den kontinuierlichen Zugriff, d. h. eine Kontinuität der Dienste für die geschützten Ressourcen, erweitert werden. In dieser

Lösung fungiert SafeNet Access Exchange (SAE) als Zugriffsvermittler und koordiniert den Datenfluss zu STA oder SAS PCE. STA bietet eine anpassungsfähige Zugriffsverwaltung und MFA für Cloud-Ressourcen, während SAS PCE als alternative MFA bei einem Ausfall bereitsteht.

Dieses hybride Bereitstellungsmodell ermöglicht den Schutz von Anwendungen mit STA in der Cloud ebenso wie eine sichere On-premise-Authentifizierung durch SAS PCE. Alle vorhandenen On-premise- oder Cloud-basierten Anwendungen funktionieren wie gewohnt mit SAS PCE und STA und Benutzer können für alle Anwendungen denselben Authentifikator verwenden.

Im Falle eines Internetausfalls bietet STA Hybrid einen integrierten Failover-Mechanismus und Funktionen für den Offline-Zugriff zur Gewährleistung eines kontinuierlichen Schutzes und der Aufrechterhaltung der Zugriffskontrollen. Diese Redundanz trägt dazu bei, die Auswirkungen von Internetausfällen auf die Sicherheit und Verfügbarkeit der Identitäts- und Zugriffsverwaltung zu minimieren.

## Ein vielschichtiges Unterfangen

Der Schutz kritischer Infrastruktursysteme ist ein vielschichtiges Unterfangen, das einen ganzheitlichen Ansatz für Sicherheit, Widerstandsfähigkeit und Betriebskontinuität erfordert. Durch die Priorisierung robuster IAM-Strategien, die auf die spezifischen Bedürfnisse kritischer Infrastrukturen zugeschnitten sind, können Unternehmen in diesem Bereich ihre Abwehrmaßnahmen gegen neu auftretende Cyberbedrohungen verbessern, die Einhaltung gesetzlicher Vorschriften sicherstellen und die ununterbrochene Bereitstellung grundlegender Dienste gewährleisten.

IAM spielt in kritischen Infrastrukturen eine entscheidende Rolle. Durch die zunehmende Digitalisierung ihrer Dienste müssen auch die Sicherheitsmaßnahmen zum Schutz dieser kritischen Systeme weiterentwickelt werden. Starke Authentifizierungsmethoden bieten zuverlässige Sicherheit zum Schutz vor modernen Cyberbedrohungen.

Durch die Priorisierung von IAM und die Implementierung fortschrittlicher Authentifizierungsmethoden können Unternehmen im Bereich kritische Infrastrukturen ihre Betriebsabläufe schützen und die Sicherheit der für unsere Gesellschaft so wichtigen Dienste gewährleisten.

Sind Sie bereit, den Schutz Ihrer Dienste zu stärken?

Greifen Sie jetzt auf die vollständige Ausgabe [2024 Thales Data Threat Report](#) – The Critical Infrastructure zu, um sich eingehender mit den Daten zu befassen und zu erfahren, wie IAM Ihre Abläufe vor modernen Cyber-Bedrohungen schützen kann.

Weitere Informationen zu den neuesten IAM-Themen finden Sie im [IAM 360 Magazine](#), einer Publikation, die sich der Erforschung aller Aspekte der Identitäts- und Zugriffsverwaltung (IAM) widmet. In jeder Ausgabe finden Sie neue Perspektiven, praktische IAM-Ratschläge sowie die neuesten Nachrichten und Trends im Bereich der Identitäts- und Zugriffsverwaltung.

Weitere Informationen zu B2B und zur Berücksichtigung der Anforderungen an Drittanbieter-Identitäten finden Sie im Analystenbericht [B2B IAM – The Hidden Value of Third-Party Identities](#).

## Über Thales

Unternehmen und Behörden sind heute auf die Cloud, Daten und Software angewiesen, um vertrauenswürdige digitale Dienste bereitzustellen. Daher vertrauen die angesehensten Marken und Unternehmen weltweit auf Thales, wenn es darum geht, sensible Daten und Software zu schützen – unabhängig davon, wo diese erstellt oder gespeichert werden bzw. von wo aus auf sie zugegriffen wird – von der Cloud über Rechenzentren bis hin zu Geräten und ganzen Netzwerken. Als weltweit führender Anbieter für Datensicherheit und Software-Lizenzierung unterstützen wir Unternehmen durch unsere Lösungen dabei, sicher in die Cloud zu migrieren, zuverlässig Vorschriften einzuhalten, einen Mehrwert aus ihrer Software zu ziehen und Millionen von Verbrauchern täglich eine nahtlose, digitale Erfahrung bereitzustellen.



### Kontakt

Alle Bürostandorte und Kontaktinformationen  
finden Sie auf [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

