

sayFUSE HCI

LÖSUNG UND ARCHITEKTUR

Ganzheitliche resiliente IT-Infrastrukturplattform und Secure Private Cloud

Die sayFUSE Betriebsplattform

Resilienz beginnt mit einer beherrschbaren IT-Infrastruktur

Souverän | Hochsicher | Wiederherstellbar

Inhalt

Executive Summary

1. Ausgangslage und Architekturziel
 2. Das Dreibein der ganzheitlichen IT-Infrastruktur
 3. sayFUSE HCI als Betriebsplattform
 - 3.1. sayFUSE HCI als ganzheitliche IT-Infrastruktur-Appliance
 - 3.2. Verfügbarkeit durch Auslegung und Betrieb
 - 3.3. Virtualisierung und Workloads
 - 3.4 Speicher nach Anwendungsprofil
 4. Souveräne Private Cloud und kontrollierte Netze
 - 4.1. Network as a Service als mittlere Schutzebene
 - 4.2. Zugriff auf Anwendungen statt pauschale Netzteilnahme
 - 4.3. Security by Design und Betriebsmodelle
 5. Arbeitsplätze und Software als definierter Sollzustand
 - 5.1 VDI & Digital Workspace – automatisierte Bereitstellung und Softwareverteilung
 6. Drei unterschiedliche Wege zur Wiederherstellung
 - 6.1 sayFUSE Backup und getrennte Sicherungsgenerationen
 - 6.2 Medienbruch als letzte Wiederherstellungsinstanz
 - 6.3 Live-Migration auf die neue Infrastruktur
 - 6.4 Live-Synchronisation für die Betriebsfortführung
 7. Migrationspfad aus bestehenden Umgebungen
 8. Architekturbeispiel für eine kritische Organisation
 9. Anforderungen an Planung und Nachweis
- Fazit
- Ergänzende technische Unterlagen

Executive Summary

sayFUSE HCI verbindet Betrieb, Zugriffssicherheit und Wiederherstellung innerhalb einer ganzheitlichen IT-Infrastruktur. Mehrere Technologien greifen ineinander: sayFUSE HCI stellt Anwendungen, Daten und Arbeitsplätze bereit; sayTRUST UZE steuert den Zugriff über Autorisierung, geprüfte Identitäten und freigegebene Anwendungen; sayFUSE Backup hält getrennte Sicherungsstände vor. NaaS kapselt Kommunikationsräume, LiveSync ergänzt die Fortführung kritischer Dienste auf einer zweiten Infrastruktur. Die Infrastruktur besteht aus mehreren All-in-One-Appliances. Eine All-in-One-Appliance bilden eine vollständige Funktionsbasis für Compute, Virtualisierung, Storage und Netzwerkdienste sowie integrierte Sicherheits-, Cloud- und Sicherungsfunktionen. Weitere Appliances erweitern Kapazität und Leistung und ermöglichen im passend ausgelegten Cluster die Übernahme von Diensten. Automatisierte VDI-Bereitstellung und Softwareverteilung schaffen reproduzierbare Arbeitsplätze statt manueller Einzelkonfigurationen.

sayFUSE HCI - die ganzheitlich resiliente IT-Infrastrukturplattform und Secure Private Cloud

Souveräner Betrieb, kontrollierter Zugriff und belastbare Wiederherstellung

Eine hyperkonvergente Plattform kann Compute, Virtualisierung, Speicher und virtuelle Netzwerke zusammenführen. Resilienz entsteht aber erst, wenn Sicherheitszonen, Zugriff, Sicherung, Auslagerung und Wiederanlauf als zusammenhängende Architektur geplant und regelmäßig überprüft werden. Dieses Whitepaper beschreibt den Funktionsumfang von sayFUSE HCI – dem Zusammenspiel von sayTRUST UZE, sayFUSE Backup und ergänzende Dienste.

1. Ausgangslage und Architekturziel

Viele IT-Landschaften wachsen als Folge bestimmter Bedarfe und einzelner Beschaffungsentscheidungen: Compute, SAN, Virtualisierung, Netzwerk, Backup, Arbeitsplatzmanagement und Fernzugriff werden getrennt betrieben. Schnittstellen erhöhen den Abstimmungsaufwand, während Fehler und Angriffe mehrere Ebenen gleichzeitig betreffen können. Entscheidend ist deshalb ein Betriebsmodell, das Abhängigkeiten sichtbar macht und die Wiederherstellung von Anfang an einplant. Das Zielbild verbindet drei Aufgaben: produktive Dienste auf einer skalierbaren Infrastruktur bereitstellen, Kommunikationswege und Zuständigkeiten kontrollieren und regeln sowie einen überprüfbaren Wiederherstellungspfad für Ausfälle und kompromittierte Umgebungen sicherstellen.

Ebene	Aufgabe	Bausteine
<i>Betrieb</i>	Workloads und Daten bereitstellen	sayFUSE HCI, Virtualisierung, Storage, Private Cloud, S3
<i>Schutz</i>	Mandanten, Zonen und Zugriffe begrenzen	NaaS, Firewall und Gateway, sayTRUST UZE
<i>Fortführung</i>	Sichern, getrennt vorhalten und wiederanlaufen	sayFUSE Backup, Medienbruch, LiveSync, Disaster Recovery

Die sayFUSE-Technologie verbindet getrennte IT-Bereiche zu einer gemeinsamen, skalierbaren Architektur. Die Funktionen bleiben stets modular, werden jedoch aus einer Hand konzipiert, integriert und in einem einheitlichen Betriebsmodell gesteuert und betrieben. Dieser Ansatz senkt Kosten, erhöht die Sicherheit und reduziert die Komplexität.

2. Das Dreiein der ganzheitlichen IT-Infrastruktur

Drei eigenständige sayTEC-Technologien tragen die Gesamtarchitektur. Jedes Standbein übernimmt eine eigene Aufgabe: sayFUSE HCI hält Infrastruktur, Anwendungen und Daten verfügbar, sayTRUST UZE kontrolliert den Zugriff, und sayFUSE Backup ermöglicht die Wiederherstellung aus getrennten Sicherungsständen. Gemeinsam decken sie den Weg von der Zugriffsfreigabe über den produktiven Betrieb bis zum Wiederanlauf ab.



Abb. 1: Drei Standbeine – eine gemeinsame Schutz- und Betriebsarchitektur

1. sayFUSE HCI

Betrieb und Verfügbarkeit

Die hyperkonvergente Plattform vereint Compute, Storage, Virtualisierung und softwaredefinierte Netzwerke in einer gemeinsamen Architektur. Sie bildet die Grundlage für Anwendungen, virtuelle Desktops (VDI) und Cloud-Dienste. Zusätzliche Nodes erweitern die verfügbaren Ressourcen und erhöhen die Redundanz.

2. sayTRUST UZE

Identität und kontrollierter Zugriff

Unified Post-Zero-Trust Exchange prüft Identität, Client und Policy vor der Freigabe. User erreichen autorisierte Anwendungen und Arbeitsplätze über kontrollierte Kommunikationswege. Der Zugriff wird auf die freigegebenen Beziehungen begrenzt.

3. sayFUSE Backup

Sicherung und Wiederherstellung

Die eigenständige Backup- und Restore-Plattform verbindet Sicherungsgenerationen, Backup Library und Medienmanagement. Jobgesteuert abgeschaltete, entnehmbare und ausgelagerte Medien schaffen getrennte Stände für Restore, Archivierung und Wiederanlauf.

Einzeln stark. Gemeinsam cyberresilient. Jede Lösung kann eigenständig betrieben werden und erfüllt eine klar definierte Aufgabe. Zusammen erzeugen sie Zugriffsschutz, Plattformverfügbarkeit und Wiederherstellung: Ein berechtigter Zugriff führt in eine abgegrenzte Betriebsumgebung; deren Daten werden über getrennte Sicherungspfade geschützt. LiveSync ergänzt diese Architektur für die Fortführung ausgewählter kritischer Dienste an einem zweiten Standort.

3. sayFUSE HCI als Betriebsplattform

Hyperkonvergenz vereint Rechenleistung, Speicher und Virtualisierung in einem Cluster aus Nodes. Die Ressourcen stehen gemeinsam zur Verfügung und lassen sich durch weitere Nodes oder – je nach Systemauslegung – zusätzliche Laufwerke erweitern. Die einheitliche Plattform vereinfacht die Zuweisung von Ressourcen an virtuelle Maschinen, virtuelle Arbeitsplatzumgebungen und interne Cloud-Dienste.

3.1. sayFUSE HCI als ganzheitliche IT-Infrastruktur-Appliance

Jede sayFUSE-HCI-Appliance ist als vollständiger Infrastrukturbaukasten konzipiert. Sie vereint Rechenleistung, Storage, Virtualisierung und Netzwerkfunktionen mit integrierten Zugriffs-, Cloud- und Sicherungsdiensten. Damit stellt jede Node eine einheitliche Funktionsbasis bereit, die die grundlegenden Infrastrukturaufgaben auf einer gemeinsamen Betriebsplattform zusammenführt.

Im Cluster ergänzt jede weitere Appliance den vorhandenen Verbund vollwertig. Sie erweitert Kapazität und Leistung und stellt zugleich Ressourcen für die Übernahme von Workloads und Diensten anderer Nodes bereit. Bei Wartung oder dem Ausfall einer Appliance können die verbleibenden Nodes deren Aufgaben übernehmen, sofern Datenredundanz, Quorum, Netzwerkpfade und ausreichende Reservekapazität dafür ausgelegt sind. Die vollständige Funktionsbasis ist dabei von der konkret aktivierten Ausstattung und den vereinbarten Diensten zu unterscheiden.

Für den Betreiber bedeutet das: Ausbau, Wartung und Ersatz erfolgen innerhalb derselben Architektur, ohne dass für jeden Funktionsbereich eine neue separate Plattform erforderlich wird. Ziel ist es, alle benötigten Services auch bei einem definierten Node-Ausfall im verbleibenden Verbund bereitzustellen. Welche Dienste automatisch fortgeführt, neu gestartet oder kontrolliert umgeschaltet werden, wird während der Konfiguration festgelegt und durch Ausfalltests nachgewiesen. Bei einer physischen Auslagerung werden Medienrotation und Verwahrung als eigenständige Betriebsaufgaben geführt.

3.2. Verfügbarkeit durch Auslegung und Betrieb

Redundante Komponenten und verteilte Ressourcen können den Weiterbetrieb beim Ausfall einzelner Komponenten oder Nodes unterstützen. Die konkrete Toleranz ergibt sich aus Clustergröße, Quorum, Datenverteilung, Reservekapazität, Netzwerkpfaden und Wartungszustand. Sie ist für jede Konfiguration zu planen und durch Ausfalltests nachzuweisen. Hochverfügbarkeit innerhalb eines Clusters schützt insbesondere vor lokalen Komponentenfehlern; ein Standortverlust erfordert eine getrennte Umgebung und einen eigenen Wiederanlaufplan.

3.3. Virtualisierung und Workloads

Auf der HCI-Plattform können virtuelle Server, VDI-Arbeitsplätze und Dienste der Private Cloud betrieben werden. In die Architektur ist Virtuozzo als Virtualisierungs- und Cloud-Betriebsschicht integriert. Rollen, Quoten, Ressourcenprofile und Administrationsgrenzen werden je Umgebung festgelegt. Live-Migration zwischen geeigneten Hosts unterstützt Wartung und Betrieb.

3.4 Speicher nach Anwendungsprofil

Block- und File-Dienste wie iSCSI und NFS decken klassische Server- und Anwendungsanforderungen ab. S3 Object Storage bietet einen anderen Zugriffspfad für große unstrukturierte Datenbestände, Backup-Ziele,

Archive oder Data-Lake-Szenarien. Kapazität, Redundanzschema und Leistungsziele werden je Datenklasse getrennt geplant. S3 ist dabei ein Speicherbaustein und ersetzt weder Sicherungsgenerationen noch unabhängige Wiederherstellungskopien.

Leistungsbeispiel aus dem produktiven S3-Betrieb

Unser S3-Whitepaper dokumentiert eine Kundenkonfiguration mit 35 Nodes und jeweils 200 Gbit/s interner sowie externer Kommunikation. Für diese Umgebung werden S3-Spitzendurchsätze von über 160 GB/s beim Lesen und über 90 GB/s beim Schreiben ausgewiesen. Separat zeigt das Monitoring 9,46 Millionen Disk IOPS und 632,44 GB/s aggregierten Datenträgerdurchsatz; diese Disk-Werte sind nicht mit dem S3-Anwendungsdurchsatz gleichzusetzen. Im dargestellten Ausbau umfasst der Cluster 25 PB Rohkapazität. Freie Laufwerksslots ermöglichen einen Ausbau auf bis zu 50 PB Rohkapazität mit den vorhandenen 35 Nodes; darüber hinaus können weitere Nodes hinzukommen. Die Werte gelten für die dokumentierte Konfiguration und den jeweiligen Messzeitpunkt. Objektgröße, Parallelität, Laufwerksbestückung, Netzwerk und Redundanzschema bestimmen die tatsächlich erreichbare Leistung.

4. Souveräne Private Cloud und kontrollierte Netze

Souveränität ist eine Betriebsentscheidung:

- Wo befinden sich die Systeme und Daten?
- Wer administriert sie?
- Wer und welche Stellen können auf Metadaten, Schlüssel, Backups und Managementebenen zugreifen?

sayFUSE Secure Private Cloud kann im eigenen Rechenzentrum oder in einer vertraglich und technisch kontrollierten Betriebsumgebung bereitgestellt werden. Mandanten, Quoten, Rollen und externe Anbindungen werden entsprechend dem Schutzbedarf definiert.

4.1. Network as a Service als mittlere Schutzebene

NaaS stellt logisch getrennte Netze für Mandanten, Anwendungen und Sicherheitszonen auf einer gemeinsamen physischen Infrastruktur bereit. Virtuelle Router, DHCP, NAT, Firewalls, VPN-Übergänge und Load Balancer können je Bereich zugeordnet werden. Ein gemeinsames Cluster bedeutet dadurch keinen gemeinsamen Kommunikationsraum. Verbindungen zwischen VDI, Fachverfahren, Datenbanken, Backup und Management benötigen ausdrückliche Regeln und dokumentierte Freigaben. Die Trennung begrenzt potenzielle laterale Bewegungen, sofern Regeln und Administrationsrechte tatsächlich konsequent umgesetzt werden. Gerade für kritische Umgebungen empfiehlt sich eine eigene Zone für Management und Sicherung sowie eine klare Trennung von Produktions-, Test- und Migrationsnetzen.

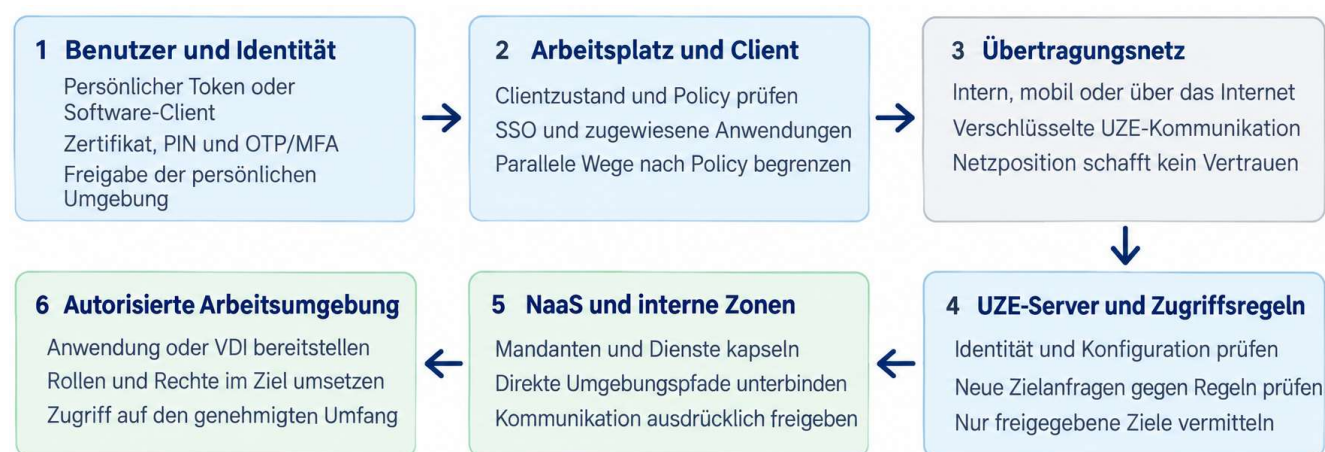
4.2. Zugriff auf Anwendungen statt pauschaler Netzteilnahme

sayTRUST UZE verbindet den zentralen UZE-Server mit dem persönlichen Hardware-Token oder gerätegebundenen Software-Clients. Die Freigabe (Autorisierung) richtet sich nach Identität, Client, Zertifikat und anwendungsbezogener Policy. Der Nutzer erhält ausschließlich die autorisierte Kommunikationsbeziehung zu einer Anwendung oder einem virtuellen Arbeitsplatz. NaaS begrenzt die Kommunikation zwischen den internen Zonen; UZE steuert den Zugriff aus dem Arbeitsplatz in diese Zonen. Identifikation und Aktivierung. Persönliche Zertifikate aus einer PKI, PIN, Hardware- beziehungsweise Gerätebindung und OTP/MFA sichern den Zugang. In der biometrischen Token-Variante aktiviert der berechtigte Nutzer den geschützten Tokenbereich per Fingerabdruck. Die verschlüsselte SSO-Datenbank wird mit ihrem Passwort

geöffnet und stellt das zugewiesene Anwendungsmenü bereit. Client und Kommunikationskontrolle. Policy- und Posture-Prüfungen berücksichtigen die festgelegten Voraussetzungen am Endgerät. Je nach Client und Policy können nicht benötigte parallele Kommunikationswege für die Sitzung eingeschränkt werden. Der native UZE-Kommunikationsmodus nutzt gegenseitige TLS-1.3-Authentisierung. Der Server prüft neue TCP- und UDP-Zielanfragen gegen die geladenen Freigaberegeln; eine erfolgreiche Anmeldung gewährt damit keine pauschale Erreichbarkeit weiterer Systeme. Sitzung und Berechtigungen. Das Zero-Footprint-Prinzip zielt darauf, sicherheitsrelevante Sitzungsinformationen nicht dauerhaft auf dem Arbeitsplatz abzulegen. Rollen- und zielbezogene Freigaben begrenzen auch administrative Kommunikationswege.

Interne und mobile Arbeitsplätze folgen derselben Logik. Die Position im Unternehmensnetz ersetzt eine Identitäts- und Zugriffsprüfung nicht. UZE-Ziele können nur über freigegebene Kommunikationswege erreicht werden; direkte, umgehende Zugriffe sind im Zielnetz zu unterbinden. So wird die Gefahr von Scans, unkontrollierten Quersugriffen und lateralen Bewegungen aus Endgerätebereichen reduziert. Ein internes Arbeitsplatznetz muss dafür ebenso konsequent von geschützten Server- und Managementzonen getrennt werden - wie ein externer Zugang.

Kontrollierte Strecke vom Nutzer bis zur Anwendung



Eine Sicherheitslogik für interne und externe Arbeitsplätze

Kein allgemeiner Zugang zu geschützten Netzen – nur ausdrücklich freigegebene Beziehungen.

Abb. 2: Durchgängige UZE-Zugriffsstrecke. Die Topologie verbindet geprüfte Identitäten und Clients mit zielbezogenen Freigaben und gekapselten NaaS-Zonen.

4.3. Security by Design und Betriebsmodelle

Die Sicherheitsarchitektur basiert auf Ringzonen und wird bereits bei der Installation angelegt. Der äußere Ring kontrolliert die User-Identität, Client und Anwendungszugriff über sayTRUST UZE. Der mittlere Ring verbindet die resiliente HCI-Betriebsplattform mit gekapselten NaaS-Kommunikationsräumen. Der innere Ring (Kern) schützt Daten und Wiederherstellung über getrennte Sicherungsbereiche und bei entsprechender Auslegung über abgeschaltete oder ausgelagerte Medien. Ein „Tresor im Tresor“ Prinzip führt Zugriffsschutz, Betriebsfähigkeit und unabhängige Wiederherstellung von Beginn an zusammen. Die Architektur kann zentral, über mehrere Standorte oder innerhalb eines Unternehmens für einzelne Abteilungen eingesetzt werden. Jeder Mandant erhält einen abgegrenzten Kommunikations- und Berechtigungsbereich. UZE und die internen NaaS-Regeln schützen gemeinsam die freigegebenen Wege und unterstützen die Kontrolle über das eigene digitale Hoheitsgebiet.

Für Managed Service Provider (MSP) bildet die Plattform die Grundlage, um Infrastruktur, virtuelle Arbeitsplätze, Anwendungsbereitstellung, sicheren Zugriff, Backup und Wiederherstellung als zusammenhängende Dienste bedarfsgerecht anzubieten. Kunden können über ihren persönlichen Token und die zugehörige Client-Umgebung auf autorisierte Arbeitsplätze und Anwendungen zugreifen. Bei vollständig europäischer Bereitstellung einschließlich Sicherung, Administration und vereinbarter Betriebsleistungen können Daten in Europa und in getrennten Mandantenbereichen verbleiben.

Die Architektur ist für zentrale Umgebungen, mehrere Standorte, getrennte Abteilungen und MSP-Dienste nutzbar. Der Betreiber behält die Kontrolle über Datenstandort, Administration und Berechtigungen. Weniger getrennte Plattformen, gemeinsame Ressourcen und automatisierte Abläufe reduzieren den Betriebsaufwand. Verfügbarkeit und Wiederherstellung werden durch definierte Ausfalltoleranzen und getestete Prozesse abgesichert.

Betrieb und Infrastruktur	Arbeitsplätze und Wiederherstellung	Identität und Zugriffsschutz
• Compute und Servervirtualisierung • Kubernetes • NFS-, iSCSI- und S3-Storage • Private Cloud und Cloud-Dienste • Router, Firewall und Load Balancer • VPN und Floating IPs • Mandantentrennung und gekapselte Netze	• Automatisierte VDI und Digital Workplace • Privileged Access Workstation (PAW) • Anwendungsbereitstellung • Softwareverteilung und Updates • LiveSync und Live-Migration • Mehrstufiges Backup und Restore • Medienbruch und physische Auslagerung	• Identitätsgebundene Post-Zero-Trust-Kommunikation • Anwendungsbezogene Freigaben • Client- und Policy-Prüfung • Zero Footprint • Single Sign-on (SSO) • Zertifikatsbasierte Identifikation (PKI) • OTP und Multifaktor-authentifizierung

Kunden profitieren von zentral bereitgestellten Diensten, deutlich weniger lokaler Betriebsaufwand und gemeinsam genutzten Ressourcen bei kontrollierter Mandantentrennung. Für Dienstleister entstehen skalierbare, wiederkehrende Serviceangebote. Der wirtschaftliche Vorteil, die planbare hohe Verfügbarkeit und eine belastbare Wiederherstellung sind das Ergebnis. Servicevereinbarungen und regelmäßige Tests sichern die zugesagte Qualität ab.

Mehrstufige Isolationsarchitektur der ganzheitlichen IT-Infrastruktur mit physischer und logischer Separation

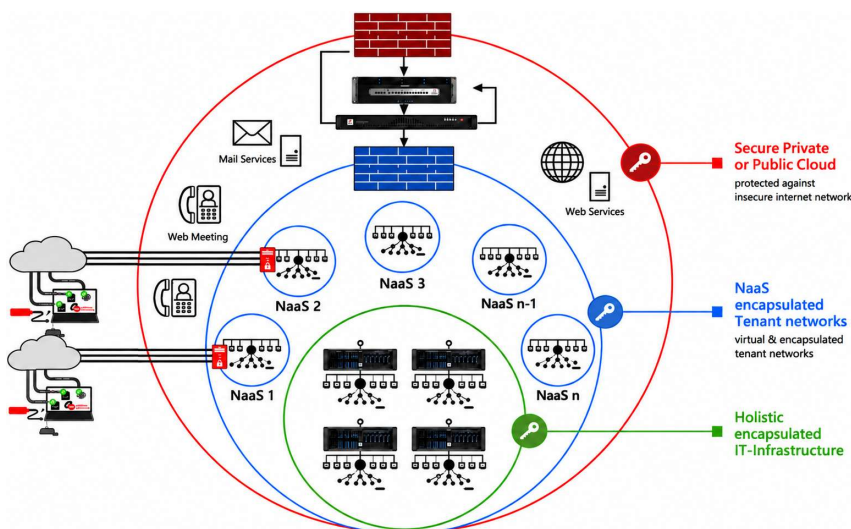


Abb. 3: Isolationsarchitektur der ganzheitlichen IT-Infrastruktur

Integrierte modulare Dienste

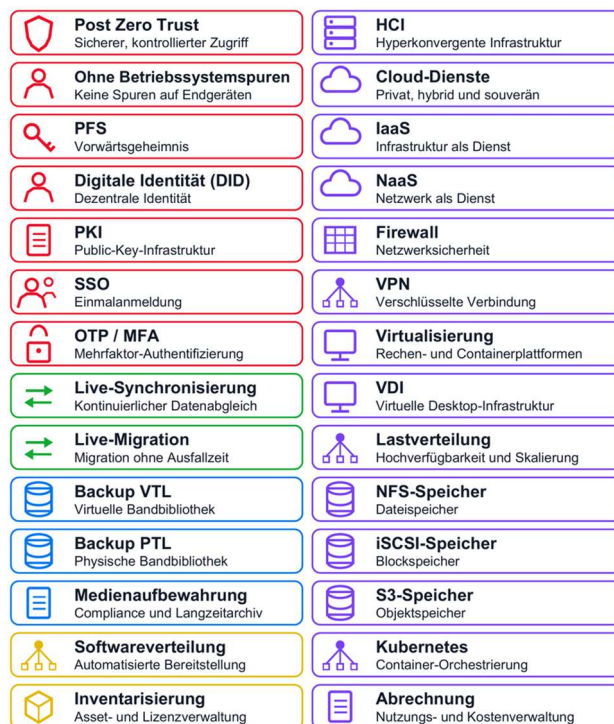


Abb. 4: Funktionsübersicht und gekapselte Gesamtarchitektur. Die Grafik zeigt das Zielbild; der konkrete Funktionsumfang richtet sich nach der Projektkonfiguration.

5. Arbeitsplätze und Software als definierter Sollzustand

VDI stellt nutzerbezogene Arbeitsplätze zentral bereit. Für privilegierte Tätigkeiten können gesondert gehärtete Privileged Access Workstations (PAW) eingerichtet werden. Der Prozess beginnt mit dem geschützten Zugang über sayTRUST UZE und der Domänenanmeldung. Rolle und Gruppenzugehörigkeit bestimmen anschließend das freigegebene Golden Image, Ressourcenprofil und die zugehörige Netzwerkzone.

Die VDI-Orchestrierung erzeugt oder weist die passende Instanz zu, nimmt sie in die Domäne auf und registriert sie beim Unified Endpoint Management (UEM). Matrix42 UEM/Empirum verteilt die zugeordneten Basispakete, Sicherheitsrichtlinien und Updates automatisch und meldet Status oder Fehler. Nach erfolgreicher Umsetzung der verpflichtenden Baseline steht der Arbeitsplatz für die produktive Nutzung zur Verfügung. Die Erzeugung der VDI und die Softwareverteilung bleiben dabei klar zugeordnete Aufgaben innerhalb derselben Prozesskette.

5.1 VDI & Digital Workspace – automatisierte Bereitstellung und Softwareverteilung

Die Arbeitsplätze werden standardisiert, automatisch, einheitlich, sicher und jederzeit reproduzierbar bereitgestellt. Zusatzanwendungen werden über Self Service angefordert und nach fachlicher, lizenzbezogener und gegebenenfalls sicherheitsbezogener Freigabe automatisiert zugewiesen. Nach Entzug wird die Software entfernt und die Lizenz entsprechend der Lizenzlogik wieder frei verfügbar. Beim Neuaufbau wird der genehmigte Sollzustand erneut hergestellt. Derselbe UEM-Grundprozess kann physische Windows-Arbeitsplätze einbeziehen; Images, Pakete, Rollen und Wartungsregeln werden zentral gepflegt.

Der Prozess für die automatische Bereitstellung von Arbeitsplätzen und Softwareverteilung wird in nachfolgende Grafik veranschaulicht.

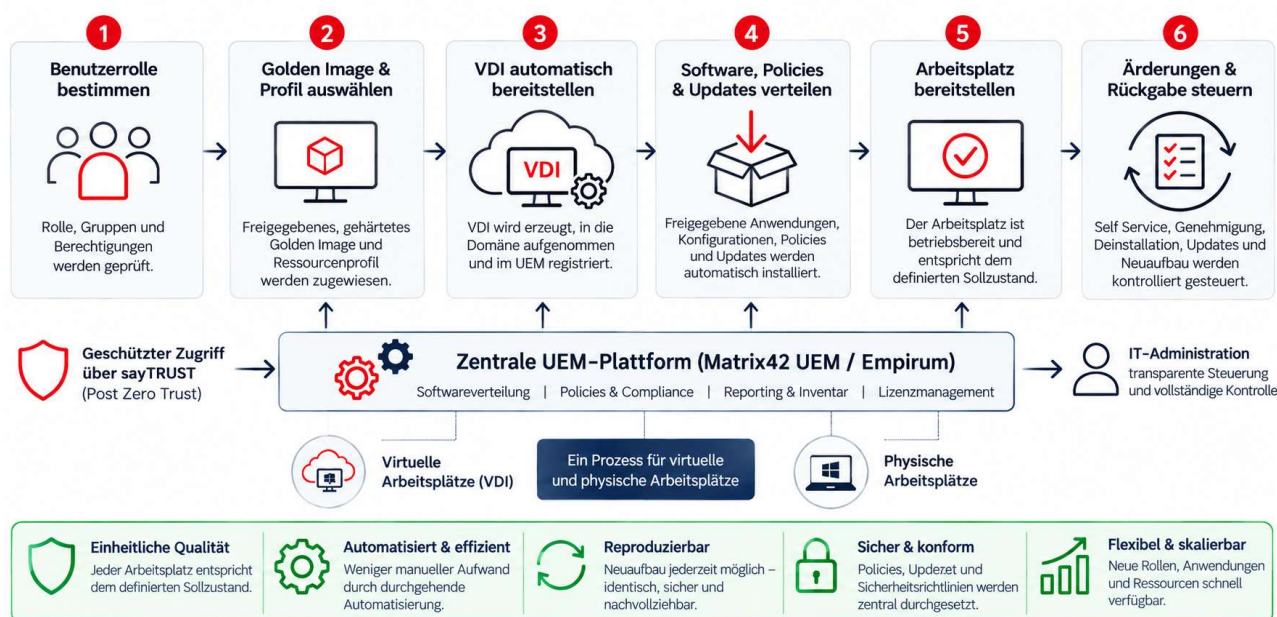


Abb. 5: Automatisierte Arbeitsplatzbereitstellung vom geprüften Benutzer und Rollenprofil bis zur betriebsbereiten VDI sowie zur kontrollierten Änderung und Rückgabe.

6. Drei unterschiedliche Wege zur Wiederherstellung

Verfügbarkeit, Datensicherung und Live-Synchronisation lösen verschiedene Probleme. Sie müssen zusammen geplant und prozessiert werden, weil ein synchronisierter Fehler oder eine Verschlüsselung auch die zweite laufende Umgebung treffen kann, während eine isolierte Sicherung allein noch keinen sofort betriebsbereiten Ersatzstandort schafft.

Maßnahme	Typischer Zweck	Planungsfrage
Clusterverfügbarkeit	Ausfall einzelner Komponenten überbrücken	Welche Fehlerdomänen sind redundant?
LiveSync und DR	Kritische Dienste an getrenntem Standort fortführen	Wie wird umgeschaltet und zurückgeführt?
Backup, Archivierung und Medienbruch	Frühere, getrennte Stände wiederherstellen	Welche Kopie bleibt nach einem Angriff nutzbar?

6.1 sayFUSE Backup und getrennte Sicherungsgenerationen

sayFUSE Backup verbindet Backup-/Dedup-Storage, parallele Sicherungsströme, Backup Library, Medienmanagement und Restore.

- Die erste Stufe sichert produktive Daten auf den zentralen Backup-Storage.
- Anschließend werden definierte Stände automatisiert auf getrennte Medien übertragen und zu Tages-, Wochen-, Monats- oder Jahressätzen zusammengeführt. Ausgewählte vollständige Sicherungsgenerationen lassen sich entnehmen und geschützt auslagern.
- Jobgesteuerte Laufwerke: Einem Sicherungsjob zugeordnete Backup-Laufwerke werden bedarfsgerecht ein- und ausgeschaltet. Für einen vorgesehenen Sicherungslauf wird das benötigte Laufwerk eingeschaltet und nach erfolgreichem Abschluss wieder abgeschaltet. So stehen Sicherungsmedien nicht dauerhaft im aktiven Datenpfad. Medienkatalog, Rotation und die Prüfung des Sicherungsergebnisses gehören zum automatisierten Ablauf und zum Betriebsprozess.

- **Sicherungsleistung bis zu 30 TB/h.** In einer entsprechend dimensionierten Konfiguration kann sayFUSE Backup mit parallelen Sicherungsströmen einen Sicherungsdurchsatz von bis zu 30 Terabyte pro Stunde erreichen. Maßgeblich sind Quellsysteme, Netzwerk, Medienbestückung, Datenprofil und Sicherungssoftware. Der Durchsatz der anschließenden Übertragung auf Auslagerungsmedien wird separat dimensioniert; die Kennzahl ist keine pauschale Zusage für jede Sicherungsstufe oder einen vollständigen System-Restore.
- Beim B6S16-Konzept können sechs Backup-Laufwerke einzeln jobgesteuert ein- und ausgeschaltet werden. Mit Medien von bis zu 40 TB ergeben sich rechnerisch bis zu 240 TB über sechs Medien. Nutzbare Kapazität, Rotation und Laufzeit richten sich nach dem konkreten Profil. Die integrierten Sicherungsfunktionen der HCI-Umgebung und eine eigenständige sayFUSE-Backup-Plattform werden so kombiniert, dass die für den Wiederanlauf benötigten Kopien ausreichend unabhängig von der produktiven Fehlerdomäne bleiben.

6.2 Medienbruch als letzte Wiederherstellungsinstanz

Ein abgeschaltetes oder entnommenes Medium liegt außerhalb des dauerhaft aktiven Datenpfads. Der Schutz wird erst belastbar, wenn auch Berechtigungen, Medienkatalog, Transport, physische Verwahrung und ein getesteter Restore geregelt sind. Die Auslagerung in einen anderen Brandabschnitt oder Standort adressiert zusätzlich physische Ereignisse. Ein Air Gap ist daher ein konkreter Betriebsprozess mit technischem Anteil, kein bloßes Etikett für eine zweite Online-Kopie.

6.3 Live-Migration auf die neue Infrastruktur

Live-Migration dient der erstmaligen oder projektbezogenen Übertragung bestehender physischer und virtueller Systeme auf die ganzheitliche sayFUSE-Infrastruktur. Die Quellsysteme bleiben während der initialen Übertragung produktiv; zwischenzeitliche Änderungen werden nachgeführt. In einer isolierten Zielumgebung werden Anwendungen, Daten und Kommunikationsbeziehungen geprüft. Erst nach der letzten Synchronisation und erfolgreichen Abnahme erfolgt die geplante Umschaltung. Das Quellsystem wird anschließend gemäß dem vereinbarten Rückfallverfahren außer Betrieb genommen. Eine Live-Migration ist damit ein zeitlich begrenztes Plattformwechselprojekt. Die fortlaufende Absicherung gegen einen späteren Ausfall ist eine separate Aufgabe der Live-Synchronisation.

6.4 Live-Synchronisation für die Betriebsfortführung

Eine Live-Synchronisation hält ausgewählte kritische Systeme dauerhaft auf einer zweiten, getrennten Betriebsplattform aktuell. Nach der initialen Übertragung werden fortlaufend Änderungen nachgeführt. Fällt ein System oder der Primärstandort aus, wird die vorbereitete Umgebung nach der definierten Prüfung und Umschaltung produktiv.

Bei entsprechender Auslegung können priorisierte Dienste innerhalb weniger Minuten auf Basis des zuletzt erfolgreich synchronisierten, konsistenten Datenstands wieder bereitstehen. Während die Benutzer auf der LiveSync-Ersatzumgebung weiterarbeiten, werden defekte Systeme repariert, ersetzt oder aus einer Sicherung wiederhergestellt. Alle im laufenden Betrieb entstehenden Änderungen werden weiterhin auf der LiveSync-Umgebung erfasst.

Nach erfolgreicher Prüfung der wiederhergestellten Plattform werden Änderungen kontrolliert zurücksynchronisiert. Erst danach erfolgt die Rückumschaltung (Failback). Anschließend wird die reguläre Synchronisationsrichtung wieder aktiviert.

RTO und RPO werden je Dienst anhand von Replikationsintervall, Datenkonsistenz, Netz, Abhängigkeiten und Umschaltprozess festgelegt und gemessen. Ein Fehler oder kompromittierter Zustand kann ebenfalls synchronisiert werden. Für solche Fälle bleiben unabhängige Backup-Generationen und ein kontrollierter Wiederanlauf aus einem geprüften Sicherungsstand erforderlich.

7. Migrationspfad aus bestehenden Umgebungen

Ein Plattformwechsel gelingt nur mit einer sauberen Zielarchitektur. Vor der Übertragung werden Workloads inventarisiert, Zielnetze, Abhängigkeiten und Schutzbedarf zugeordnet sowie Test- und Rückfallkriterien festgelegt. Die technische Synchronisation kann während des laufenden Betriebs erfolgen; die endgültige Umschaltung benötigt ein festzulegendes Zeitfenster und eine fachliche Abnahme.

- Inventar und Abhängigkeiten der Quellsysteme erfassen; Zielnetze und Berechtigungen festlegen.
- Initiale Übertragung und laufende Synchronisation in die neue sayFUSE-Umgebung durchführen.
- Technische und fachliche Tests der Anwendung, Datenkonsistenz und Kommunikationsregeln durchführen.
- Letzte Synchronisation, Umschaltung und kontrollierte Beobachtungsphase durchführen.
- Kritische Dienste bei Bedarf in ein gesondertes LiveSync- und DR-Konzept übernehmen.

Das ergänzende Whitepaper „KRITIS Infrastruktur für ganzheitliche resiliente IT-Infrastruktur“ beschreibt diesen Ablauf anhand einer VMware-/ESXi-Quellumgebung mit Hystax LiveSync.

8. Architekturbeispiel für eine kritische Organisation

Ein Mitarbeiter meldet sich intern oder mobil über seinen persönlichen UZE-Client an. Identität, Zertifikat, zusätzliche Authentifizierung und Freigaben bestimmen, welche Arbeitsumgebung er erreichen darf. Die geschützte Verbindung führt ausschließlich zur autorisierten VDI oder Anwendung; NaaS trennt Arbeitsplatz-, Anwendungs-, Datenbank-, Management- und Backup-Zonen. Die zugewiesene VDI erhält ihr Rollenprofil sowie die genehmigte Software automatisch.

Die Dienste laufen auf dem sayFUSE-HCI-Verbund. Zusätzliche Appliances erweitern Ressourcen und Redundanz; S3 stellt große Objektdatenbestände bereit. Produktive Daten werden zunächst auf Backup-Storage gesichert und anschließend auf jobgesteuerte Medien übertragen. Getrennte Generationen und ausgelagerte Kopien sichern die Rückkehr zu einem geeigneten Datenstand. LiveSync hält die priorisierten Dienste zusätzlich an einer zweiten Betriebsumgebung vor.

Bei einem Node-Ausfall übernehmen verbleibende Clusterressourcen die vorgesehenen Aufgaben. Bei einem Standortausfall werden kritische Dienste auf der LiveSync-Umgebung fortgeführt, während die ursprüngliche Plattform wiederhergestellt wird. Bei beschädigten oder kompromittierten Daten wird ein geprüfter Sicherungsstand genutzt. Zugriff, Arbeitsplatzbereitstellung, Betrieb und Wiederherstellung bilden damit einen nachvollziehbaren Gesamtprozess.

9. Anforderungen an Planung und Nachweis

Eine ganzheitliche Plattform entsteht durch technische Integration und klare Betriebsentscheidungen. Ohne definierte Verantwortlichkeiten, Schutzklassen und regelmäßige Wiederanlauf-tests bleiben Zusagen zur Resilienz unvollständig.

Entscheidung	Nachweis im Betrieb
<i>Schutzbedarf, RTO und RPO je Dienst</i>	Abgestimmte Ziele und gemessene Wiederanlaufzeiten
<i>Redundanz und Fehlerdomänen</i>	Ausfalltests für Node, Netzwerkpfad und Standort
<i>Mandanten und Zonen</i>	Freigegebene Kommunikationsmatrix und Regelprüfung
<i>Rollen und Administrationsgrenzen</i>	Berechtigungskonzept, Protokollierung und Review
<i>Backup und Auslagerung</i>	Sicherungskatalog, Medienrotation und Restore-Tests
<i>Migration und Rückfall</i>	Testprotokolle, Abnahme und Rückschaltverfahren

Fazit

sayFUSE HCI liefert die skalierbare Grundlage für Rechenleistung, Virtualisierung, Speicher und Private Cloud. Die ganzheitliche IT-Infrastruktur entsteht durch die kontrollierte Verbindung dieser Grundlage mit Netztrennung, identitätsbezogenem Zugriff, reproduzierbaren Arbeitsplätzen und mehreren Wiederherstellungspfaden. Souveränität folgt aus der Kontrolle über Betriebsort, Rollen, Daten und Abhängigkeiten. Cyberresilienz zeigt sich im nachgewiesenen Weiterbetrieb und in einer funktionierenden Wiederherstellung.

Der nächste Schritt für eine konkrete Organisation ist ein überprüfbares Zielbild: Dienste und Abhängigkeiten erfassen, RTO und RPO festlegen, Zonen und Rollen entwerfen, Backup- und DR-Pfade dimensionieren und den vollständigen Ablauf praktisch testen.