sonio.

Ihr Digital Workplace brennt.

Und Ihre IT löscht Feuer, statt Fundamente zu bauen.

Digital Workplace im Blindflug.

Warum überstürzte Tool-Entscheidungen aus der Pandemie heute IT-Teams lähmen.

In der IT vieler Unternehmen hat sich ein Muster etabliert, das niemand bewusst wollte: Ein Konto funktioniert nicht, ein Gerät streikt, ein Zugriff fehlt. Also wird gelöscht, geflickt, improvisiert. Tag für Tag stapeln sich die Tickets, und für strategische Arbeit bleibt schlicht keine Zeit. Das ist kein Versagen einzelner IT-Teams. Es ist die logische Konsequenz einer Entwicklung, die vor wenigen Jahren mit einer globalen Krise begann. COVID-19 hat die Digitalisierung nicht beschleunigt, sie hat sie erzwungen. Innert Wochen mussten Unternehmen remote-arbeitsfähig werden. Videokonferenzen, Cloud-Speicher, Chat-Plattformen, VPN-Zugänge: Jedes Tool löste ein dringendes Problem, und die Entscheidungen mussten überstürzt getroffen werden. Was damals Pragmatismus war, ist heute ein Flickenteppich. Und dieser Flickenteppich produziert genau die Brände, die Ihre IT täglich löschen muss. In der Praxis sehen wir es regelmässig: Fünf bis zehn sich überschneidende Lösungen sind der Normalfall, nicht die Ausnahme.

Die Offerte liegt im OneDrive. Die Projektdatei beim externen Partner in Dropbox. Die Baupäne auf dem lokalen NAS. Drei Speicherorte, ein Dokument, das niemand auf Anhieb findet. Die Freigabe dazu läuft parallel über Teams, den inoffiziellen Slack-Kanal der Fachabteilung – und wenn es wirklich schnell gehen muss, landet die Nachricht in einer WhatsApp-

ZUSAMMENFASSUNG

Kennen Sie das? Die Tickets stapeln sich, das IT-Team ist im Dauerstress und Mitarbeitende verlieren Stunden mit Warten auf den Support. Statt Motivation herrscht Frust. Und während Ihre IT ein Feuer nach dem anderen löscht, bleibt keine Zeit für das, was den Brand eigentlich verursacht.

Was 2020 als Notlösung begann, ist heute strukturelles Problem: Unter enormem Druck der COVID-19-Pandemie mussten Unternehmen innerhalb von Wochen remote-fähig werden. Tool um Tool wurde eingeführt, Entscheidungen mussten überstürzt getroffen werden, um den Betrieb aufrechtzuerhalten. Jetzt, Jahre später, muss dieses Fundament sauber aufgearbeitet werden. Das Resultat dieser Notmassnahmen: fragmentierte Identitäten, Schatten-IT, ein aufgelöster Sicherheitsperimeter und Lizenzkosten, von denen rund die Hälfte verpufft.

Dieses White Paper zeigt, was das konkret kostet, warum mehr Software das Problem nicht löst und wie ein tragfähiges Fundament aufgebaut wird. Mit Schweizer Regulierungskontext, konkreten Kennzahlen und Handlungsempfehlungen für drei Zeithorizonte.

Gruppe. Aufgaben verwaltet jede Abteilung für sich: Führungskräfte in Planner, das Projektmanagement in Asana, die IT in Jira, der Vertrieb in Salesforce. Vier Systeme, kein gemeinsames Bild.
Das ist kein Extrembeispiel. Das ist Montag.

Ein beachtlicher Teil dieser Anwendungen wurde nie von der IT freigegeben, sondern per Kreditkarte in der Fachabteilung gebucht. Fragt man, wer den Überblick hat, erntet man Schweigen.

Was der Wildwuchs wirklich kostet

Die Zahlen sind kein Schönheitsfehler, sondern ein Alarmsignal. Ein mittelständisches Unternehmen betreibt heute im Durchschnitt rund 275 SaaS-Anwendungen. Etwa ein Drittel davon kennt die IT-Abteilung nicht einmal – sie laufen als Schatten-IT vollständig unter dem Radar. Rund 70 % der Software-Ausgaben werden mittlerweile von Fachabteilungen kontrolliert, nicht von der IT (Zylo SaaS Management Index 2025). Für die Schweiz zeigt der SWICO ICT Index, dass trotz Kostendruck die IT-Ausgaben weiter steigen – ohne dass die Effizienz proportional mitwächst. Noch unbequemer: Rund die Hälfte aller gekauften Software-Lizenzen bleibt ungenutzt. Gemäss Flexera verschwinden im Schnitt 27 % der Cloud-Ausgaben in ungenutzten Lizenzen

> „Statt Motivation herrscht Frust.
> Sonio AG, Digital Workplace Praxis

und redundanten Tools (Flexera State of the Cloud 2025). Bei einem SaaS-Budget von einer Million Franken sind das über 250‘000 Franken pro Jahr, die niemandem etwas bringen. Ein weiterer Nutzen, der selten beziffert wird: Mitarbeitende, deren Werkzeuge einfach funktionieren, arbeiten lieber – und bleiben länger. In der Schweiz kostet die Rekrutierung einer Fachkraft je nach Rolle CHF 15’000–40’000. Ein reibungsloser Digital Workplace als Employer-Branding-Argument ist daher keine weiche Kennzahl, sondern eine harte.

RECHENBEISPIEL: Was der Flickenteppich ein KMU kostet

Ausgangslage: Unternehmen mit 150 Mitarbeitenden

Support-Tickets:	Ø 60/Monat × 45 Min. × CHF 120 Stundenkosten = **CHF 54‘000/Jahr**
Ungenutzte Lizenzen:	150 User × CHF 80/Monat × 50 % Nichtnutzung = **CHF 72‘000/Jahr**
Onboarding-Verzögerung:	15 MA/Jahr × 3 Tage × CHF 600 Tagessatz = **CHF 27‘000/Jahr**

Total vermeidbarer Aufwand: ≈ CHF 153‘000/Jahr

Diese Zahlen sind konservativ gerechnet und berücksichtigen weder Sicherheitsvorfälle noch Reputationsschäden.

Vier Brandherde in Ihrem Digital Workplace

FRAGMENTIERTE IDENTITÄTEN:
Mitarbeitende haben Konten in Dutzenden Systemen. Wer wo Zugriff hat, weiss niemand verlässlich. Beim Austritt bleiben Zugänge oft monatelang aktiv. Ein Einfallstor mit Ansage.

SCHATTEN-IT:
Fachabteilungen buchen Tools an der IT vorbei. Unternehmensdaten landen in Systemen, die nie jemand geprüft hat. Sowohl ein Sicherheits- als auch ein Compliance-Risiko.

AUFGELÖSTER PERIMETER:
Gearbeitet wird aus Büro, Homeoffice und unterwegs. Konzepte, die auf das Firmennetzwerk ausgelegt sind, greifen schlicht nicht mehr.

SCHATTEN-KI:
Mitarbeitende kippen Firmendaten in private ChatGPT- oder andere KI-Konten, ohne dass dies irgendjemand kontrolliert. Dies ist die neue, gefährlichste Form der Schatten-IT und derzeit einer der meistgenannten Schmerzpunkte bei Schweizer CISOs.

Quelle: Zylo SaaS Management Index 2025. Für die Schweiz zeigt der SWICO ICT Index, dass trotz Kostendruck die IT-Ausgaben weiter steigen – ohne dass die Effizienz proportional mitwächst. HR Today / Kienbaum Vergütungsreport Schweiz 2025: hrtoday.ch

Die Firewall reicht nicht mehr.

Die Firewall schützt den Rand. Doch den gibt es so nicht mehr. Sicherheit muss heute dort greifen, wo auf Daten zugegriffen wird.

Früher war die Sache einfach: Innerhalb des Firmennetzwerks galt Vertrauen, ausserhalb Misstrauen. Die Firewall war die Stadtmauer. Dieses Modell ist tot – nicht weil es schlecht konzipiert war, sondern weil sich die Arbeitswelt fundamental verändert hat. Das Unbequeme: Viele Unternehmen sichern noch immer eine Welt ab, die es nicht mehr gibt.

Hybrides Arbeiten ist der Normalfall, nicht das Sonderszenario

Mitarbeitende arbeiten heute aus dem Büro, dem Homeoffice, dem Zug und dem Café. Sie nutzen sowohl Firmengeräte als auch private Geräte. Die Daten liegen in der Cloud, auf lokalen Servern und in SaaS-Anwendungen, oft alles gleichzeitig. Ein Innen und Aussen gibt es nicht mehr. Es gibt nur noch Zugriffe – und jeder davon ist eine Vertrauensentscheidung. Wer diese Entscheidung dem Zufall überlässt, hat bereits verloren.

Der Angreifer hackt nicht mehr. Er meldet sich an.

Die Angreifer haben den Wandel längst verstanden. Gemäss dem Verizon Data Breach Investigations Report 2025 gehen 80 % der Datenpannen auf kompromittierte oder gestohlene Anmeldedaten zurück (verizon.com/business/resources/reports/dbir). Microsoft blockiert inzwischen über 7'000 passwortbasierte Angriffe pro Sekunde – ein Anstieg von 75 % gegenüber dem Vorjahr. Angriffe auf Geschäfts-E-Mail-Konten (BEC) nahmen 2025 um 34 % zu (Microsoft Digital Defense Report 2025: microsoft.com/security/blog). KI-generierte Phishing-Mails sind von echten kaum noch zu unterscheiden. Der ENISA

> Hybrides Arbeiten ohne Zero-Trust-Architektur ist ein Sicherheitsversprechen ohne Substanz.
>
> Sonio AG, Digital Workplace Praxis

Threat Landscape 2025 bestätigt: Identitäten sind das primäre Einfallstor für Angreifer in europäischen Unternehmen (enisa.europa.eu/publications/enisa-threat-landscape-2025).

Die Konsequenz: Wenn ein Konto kompromittiert ist, gilt der Angreifer in den meisten Fällen aus Systemsicht als legitimer Mitarbeiter – mit allen Zugriffen dieses Kontos. In einem Flickenteppich mit fragmentierten Identitäten kann das bedeuten: Vollzugriff, unbemerkt, über Wochen. Multi-Faktor-Authentifizierung war der erste wichtige Schritt zum Schutz von Identitäten. Der nächste Schritt sind Passkeys und Passwordless-Architekturen:
Sie eliminieren das Passwort als Angriffsfläche

vollständig, sind phishing-resistent und machen Identitäten auch dann sicher, wenn Anmeldedaten aus anderen Quellen bekannt werden.

Schweizer Regulierungskontext: Was jetzt gilt

Für Schweizer Unternehmen steigt der regulatorische Druck auf mehreren Ebenen gleichzeitig:

- **revDSG (revidiertes Datenschutzgesetz):** In Kraft seit September 2023. Unternehmen müssen nachweisen können, welche Daten sie zu welchem Zweck bearbeiten und wer darauf Zugriff hatte. Bei Verletzung der Datensicherheit besteht Meldepflicht gegenüber dem EDÖB. Die Folgen bei Verstoss: Bussen bis CHF 250‘000 für verantwortliche Personen, Reputationsschäden und zivilrechtliche Haftung gegenüber betroffenen Personen. PwC Switzerland schätzt, dass ein Grossteil der Schweizer KMU die Anforderungen noch nicht vollständig erfüllt.

- **ISG (Informationssicherheitsgesetz):** Für Betreiber kritischer Infrastrukturen gilt ab 2025 die Meldepflicht für erhebliche Cyberangriffe an das NCSC innerhalb von 24 Stunden. Bei Nichteinhaltung drohen Bussen bis CHF 100‘000. Der NCSC-Halbjahresbericht 2025/2 zeigt: Phishing und Ransomware bleiben die dominanten Angriffsvektoren in der Schweiz.

- **FINMA-Anforderungen:** Finanzinstitute unterliegen strengen Vorgaben zu Zugriffskontrollen, Audit-Trails und Datensouveränität. Verstösse können Lizenzentzug, Bussen und persönliche Haftung der Geschäftsleitung zur Folge haben. Ein Digital Workplace ohne lückenlose Nachvollziehbarkeit ist für regulierte Unternehmen kein Betriebsmodell, sondern ein direktes Haftungsrisiko.

- **US Cloud Act & Datensouveränität:** Wer Public-Cloud-Dienste amerikanischer Anbieter nutzt, muss wissen: US-Behörden können unter dem Cloud Act auf diese Daten zugreifen, unabhängig vom physischen Serverstandort. Für Schweizer Unternehmen mit sensitiven Kundendaten ist ein Deployment-Modell in der Schweiz keine Kür, sondern Pflicht.

Das Fundament entscheidet.

Eine integrierte Workplace-Architektur reduziert Komplexität und erhöht die Sicherheit.

Wenn im Digital Workplace etwas nicht funktioniert, ist der Reflex fast immer derselbe: ein neues Tool. Die Zusammenarbeit hakt? Ein Collaboration-Tool. Die Dateien sind verstreut? Eine neue Speicherlösung. Der Support ertrinkt? Ein Ticket-System. Jede dieser Entscheidungen war verständlich – und hat das Problem strukturell verschlimmert.

> Wer oben bei den Tools statt unten bei der Identität beginnt, baut auf Sand. Das mag Jahre gutgehen. Bis zum ersten Sicherheitsvorfall.
>
> Sonio AG, Digital Workplace Praxis

Denn dieser Reflex behandelt Symptome, nicht Ursachen. Jedes zusätzliche Tool ohne architektonisches Fundament vergrössert die Komplexität, die es reduzieren sollte. Das Ergebnis: mehr Tickets, mehr Schatten-IT, mehr Sicherheitslücken – und höhere Kosten. Sie kaufen also nicht die Lösung, sondern das nächste Problem.

Die Erkenntnis aus Dutzenden Workplace-Projekten: Der Digital Workplace funktioniert nicht als Tool-Sammlung, sondern als Architektur. Produktivität, Sicherheit und Zufriedenheit entstehen durch ein durchdachtes, integriertes Fundament aus Identität, Endgeräte-Management und Zugriffssteuerung. Struktur entscheidet. Nicht die Tools. Sie bestimmt, ob ein neues Tool in Tagen oder erst in Monaten produktiv ist. Und ob ein kompromittiertes Passwort ein Ärgernis bleibt oder zum Vollzugriff auf das Unternehmen wird.

Wer beim Tool beginnt, baut verkehrt.

Identität, Sicherheit, Endgeräte und Integration bilden die Basis für einen Digital Workplace, der sicher, skalierbar und bereit für KI ist.

Ein tragfähiger Digital Workplace ist wie ein Gebäude aufgebaut: von unten nach oben. Die sichtbaren Tools, mit denen Mitarbeitende täglich arbeiten, sind das oberste Stockwerk. Darunter liegen vier tragende Schichten. Über allem steht Governance und Compliance als Rahmen. Wer das Gebäude vom Dach her baut, braucht sich über einstürzende Wände nicht zu wundern. Die Reihenfolge ist entscheidend. Wer zuerst die Identitätsschicht in Ordnung bringt, kann Tools später fast beliebig austauschen.

SCHICHT	WAS SIE LEISTET
Governance & Compliance	Der Rahmen über allem: Nachvollziehbarkeit, Datensouveränität (revDSG, Cloud Act), klare Regeln, wer was darf und wo Daten liegen.
Sichtbare Tools + KI	Collaboration, Kommunikation, Fachanwendungen, KI-Assistenten. Das, was Mitarbeitende sehen. Wichtig, aber nur sicher wenn das Fundament steht.
4. Integration	Cloud und On-Premises verbinden, Datenflüsse steuern, Insellösungen vermeiden. Ein Workplace, nicht zehn.
3. Verwaltete Endgeräte	Unified Endpoint Management für Windows, macOS, iOS und Android. Jedes Gerät bekannt, konform und im Ernstfall aus der Ferne sperrbar.
2. Sicherheit / Zero Trust	Kein impliziter Vertrauensvorschuss. Jeder Zugriff wird geprüft: Wer, von wo, mit welchem Gerät. Passkeys/ Passwordless als nächste Ausbaustufe.
1. Identität	Das Fundament. Eine zentrale, saubere Identität pro Person. Ein Eintritt, ein Austritt, ein Berechtigungsmodell. Hier beginnt sowohl Sicherheit als auch KI-Readiness.

Das Fundament-Modell: gelesen von unten nach oben. Die Tools stehen zuoberst, weil sie auf allem anderen aufbauen.

Wer zuerst Tools kauft, zementiert das Chaos – und bezahlt es doppelt: einmal beim Kauf, einmal beim täglichen Firefighting. Und noch ein Gedanke, der

> KI-Readiness beginnt nicht beim KI-Tool. Sie beginnt bei der Frage, wer heute worauf Zugriff hat.
>
> Sonio AG, Digital Workplace Praxis

heute immer wichtiger wird: KI-Readiness beginnt nicht beim KI-Tool. Sie beginnt genau hier – bei einer sauberen Identitätsstruktur, klaren Berechtigungsmodellen und einem Fundament, das kontrolliert, wer auf was zugreifen darf. Wer dieses Fundament hat, kann KI-Systeme sicher und sinnvoll einsetzen. Wer es nicht hat, macht sein Unternehmen durch KI schneller angreifbar.

Weniger Aufwand. Mehr Wirkung.

Ein durchdachter Digital Workplace senkt Kosten und Risiken, entlastet die IT und macht Mitarbeitende vom ersten Tag an produktiver.

Ein sauber gebauter Digital Workplace verändert den Alltag messbar, auf fünf Dimensionen:

- **Sicherheit:** Identität und Zero Trust statt offenem Perimeter. Da 80 % der Datenpannen bei kompromittierten Anmeldedaten beginnen, ist eine zentrale Identität mit phishing-resistenter MFA (Passkeys) der wirksamste einzelne Sicherheitshebel. Kein anderes Investment bringt mehr Schutz pro Franken.

- **Kosten:** Konsolidierung überschneidender Lizenzen. Wenn rund die Hälfte der Lizenzen ungenutzt bleibt und gut ein Viertel der Cloud-Ausgaben verpufft, liegt bei einem 150-Personen-Unternehmen ein jährliches Sparpotenzial von CHF 70‘000–150‘000 allein durch Lizenzbereinigung.

- **Geschwindigkeit:** Neue Mitarbeitende erhalten am ersten Tag ein fertig konfiguriertes Gerät mit allen Zugriffen, statt tagelang auf Freischaltungen zu warten. Beim Austritt werden sämtliche Zugänge zentral und sofort entzogen. In Minuten, nicht in Wochen.

- **Kontrolle & Compliance:** Wer hat wann worauf zugegriffen? Wo liegen welche Daten? Mit sauberer Architektur sind das Reports auf Knopfdruck – und kein Thema mehr bei revDSG-Audits oder FINMA-Prüfungen.

- **Entlastung der IT:** Standardisierte, verwaltete Geräte erzeugen deutlich weniger Tickets. In begleiteten Projekten konnten Support-Tickets nach vollständigem Fundament-Aufbau um 35–50 % reduziert werden. Ihre IT gewinnt Zeit für Strategie statt Firefighting.

Ein weiterer Nutzen, der selten beziffert wird: Mitarbeitende, deren Werkzeuge einfach funktionieren, arbeiten lieber – und bleiben länger. In der Schweiz kostet die Rekrutierung einer Fachkraft je nach Rolle CHF 15‘000–40‘000 (Stelleninserat, Recruiting, Einarbeitung). Ein reibungsloser Digital Workplace als Employer-Branding-Argument ist daher keine weiche Kennzahl, sondern eine harte.

Spätestens im Ernstfall zählt die Architektur.

Verlorene Geräte, unklare Zugriffe und unnötige Support-Tickets zeigen, was ein fehlendes Fundament tatsächlich kostet.

Zwei Szenarien aus der Praxis zeigen, was der Unterschied zwischen Tool-Denken und Architektur-Denken im Alltag bedeutet.

Das verlorene Gerät – und keine Antwort auf die Frage «Was war drauf?»

Ein Unternehmen mit rund 200 Mitarbeitenden stattet seine Teams für hybrides Arbeiten mit neuen Notebooks aus. Die Geräte sind modern, die Mitarbeitenden zufrieden – das Projekt gilt intern als Erfolg. Was jedoch niemand gebaut hat,

> Die teuersten IT-Probleme entstehen nicht durch schlechte Tools. Sie entstehen durch fehlende Architektur – und werden sichtbar, wenn es zu spät ist.
>
> Sonio AG, Digital Workplace Praxis

ist die Architektur dahinter: kein zentrales Endgeräte-Management, keine Zugriffssteuerung, keine Geräteverschlüsselung mit zentralem Schlüsselmanagement. Als ein Notebook im Zug verloren geht, kann niemand sagen, welche Daten darauf lagen, und niemand kann es aus der Ferne sperren oder löschen. Das Gerät landet irgendwo – mit potenziellem Zugriff auf Firmen-E-Mails, SharePoint und interne Tools. Ergebnis: IT-Notfall, anwaltliche Abklärung, Meldepflicht nach revDSG. Neue Geräte kaufen ist einfach. Eine Architektur bauen, die sie sicher macht, ist die eigentliche Aufgabe.

40 % weniger Tickets nach Fundament-Aufbau

Ein Unternehmen im Dienstleistungssektor (ca. 120 Mitarbeitende) stellte fest, dass das IT-Team monatlich über 80 Tickets bearbeitete, von denen mehr als die Hälfte auf Zugriffsprobleme, fehlende Konfigurationen und unklare Gerätezustände zurückzuführen waren. Nach strukturiertem Aufbau von zentralem Identitätsmanagement, Endpoint Management und sauberem Onboarding-Prozess: Rückgang der monatlichen Tickets auf unter 50 innerhalb von drei Monaten – eine Reduktion von rund 40 %. (Quelle: Anonymisiertes Sonio-Kundenprojekt, Q1 2026.) Die IT konnte in dieser Zeit erstmals an einer Sicherheits-Roadmap arbeiten, statt täglich Feuer zu löschen.

Die Reihenfolge macht den Unterschied.

Erst verstehen, dann strukturieren, integrieren und konsolidieren – so entsteht ein Digital Workplace, der langfristig funktioniert.

Wie kommt man vom Löschen zum Bauen? Aus unserer Projekterfahrung hat sich ein fünfstufiges Vorgehen bewährt. Die Reihenfolge ist dabei kein Vorschlag, sondern der Kern der Methode.
Das ist kein Big-Bang-Projekt, sondern ein Weg mit Zwischenerfolgen. Schon die Bestandsaufnahme deckt ungenutzte Lizenzen und riskante Zugänge auf, die sofort bereinigt werden können. Wer strukturiert vorgeht, finanziert die Architekturarbeit oft aus den Einsparungen der ersten Monate.

Das 5-Schritte-Vorgehen zum tragfähigen Digital Workplace

SCHRITT 1
Bestandsaufnahme:
Welche Tools, Identitäten, Geräte und Zugriffe existieren wirklich? Inklusive Schatten-IT und Schatten-KI. Diese Inventur ist ernüchternd, aber unverzichtbar.

SCHRITT 2
Fundament definieren: Identitäts- und Zugriffsmodell festlegen, Zero-Trust-Prinzipien verankern, Roadmap zu Passkeys/Passwordless planen. Eine Identität pro Person, Zugriff nach minimalen Rechten.

SCHRITT 3
Geräte- und Integrationsschicht aufbauen: Unified Endpoint Management einführen, Cloud- und On-Premises-Systeme sauber verbinden, Datensouveränität sicherstellen.

SCHRITT 4
Governance verankern:
Klare Regeln für neue Tools, Datenablage, KI-Nutzung und Zugriffe. Leichtgewichtig genug, dass sie gelebt werden. Verbindlich genug, dass Wildwuchs nicht zurückkehrt.

SCHRITT 5
Tools konsolidieren und befähigen:
Redundante Lösungen ablösen, verbleibende Tools sauber integrieren, Mitarbeitende schulen und begleiten.

Kein weiterer Tool-Anbieter. Ein Partner fürs Ganze.

Sonio begleitet den Digital Workplace ganzheitlich – von Identität und Sicherheit über Integration und Governance bis zum laufenden Betrieb.

Die meisten Unternehmen haben weder das Spezialwissen noch die freien Kapazitäten, eine Workplace-Architektur neben dem Tagesgeschäft aufzubauen.

> Erfolg entsteht durch Struktur – nicht durch Software. Und durch einen Partner, der die Situation versteht, bevor er empfiehlt.
>
> Sonio AG

Was sie brauchen, ist kein weiterer Softwareverkäufer, sondern ein Partner, der sich die Zeit nimmt, ihre Situation zu verstehen – und die Architektur dann umsetzt und im Betrieb Verantwortung übernimmt. Genau das ist die Rolle von Sonio. Unser Fokus liegt auf der Strategie, dem technischen Fundament und der Begleitung des Digital Workplace:

- **Identity & Access Management:** Eine zentrale, saubere Identitätsschicht als Basis für Sicherheit, Compliance und KI-Readiness.
- **Modernes Endgeräte-Management:** Unified Endpoint Management über alle Plattformen, inklusive Rollout Services vom Staging bis zur Vor-Ort-Begleitung und Schulung der Mitarbeitenden.
- **Zero-Trust-Security & Passwordless:** Endpoint Security, Zugriffssteuerung, Passkeys und auf Wunsch Anbindung an ein Security Operations Center. Proaktiv statt reaktiv.
- **Integration von Cloud und On-Premises:** Sichere Konnektivität statt Insellösungen, abgestimmt auf die bestehende Infrastruktur und Datensouveränitätsanforderungen.
- **Governance, Compliance und Datensouveränität:** Nachvollziehbare Strukturen, Betrieb in der Schweiz, revDSG- und ISG-konform.
- **Change Management und Befähigung:** Mitarbeitende müssen mit neuen Werkzeugen produktiv werden. Wir begleiten diesen Prozess: von der Schulung am ersten Tag bis zur kontinuierlichen Weiterentwicklung der digitalen Kompetenzen.

Struktur statt Firefighting.

Identität, Sicherheit und Governance schaffen das Fundament für einen Digital Workplace.

Ihr Digital Workplace brennt, und Ihre IT löscht. Die Wahrheit ist: Solange niemand das Fundament baut, wird es weiterbrennen. Mehr Tools lösen kein Strukturproblem – sie vergrössern es.

Die zentralen Erkenntnisse:

- **Firefighting ist ein Symptom, keine Strategie.** Wenn Ihre IT nur noch löscht, liegt das nicht an der IT, sondern an einer Arbeitsplatz-Landschaft ohne Fundament.

- **Identität ist der neue Perimeter.** 80 % der Datenpannen beginnen bei kompromittierten Zugangsdaten. Wer die Identitätsschicht nicht beherrscht, verliert die Kontrolle.

- **Der Wildwuchs hat seinen Preis.** Rund die Hälfte aller Lizenzen wird nicht genutzt, ein Viertel der Cloud-Ausgaben verpufft ohne Gegenwert. Das zu bereinigen ist kein Sparprogramm – es ist das Ende eines teuren Durcheinanders.

- **KI-Readiness beginnt beim Fundament.** Wer KI sinnvoll und sicher einsetzen will, braucht zuerst saubere Identitäten, klare Berechtigungsmodelle und Datensouveränität. Ohne dieses Fundament macht KI ein Unternehmen schneller angreifbar, nicht produktiver.

- **Regulierung wartet nicht.** revDSG, ISG, FINMA: Der Schweizer Regulierungsrahmen ist in Kraft. Bussen bis CHF 250‘000, Meldepflichten und persönliche Haftung sind die Konsequenzen für Unternehmen ohne saubere Architektur.

Nicht irgendwann. Jetzt.

Mit den richtigen Sofortmassnahmen, einem klaren 90-Tage-Plan und einer langfristigen Roadmap wird aus Firefighting Schritt für Schritt ein beherrschbarer Digital Workplace.

Gestaffelt nach drei Zeithorizonten – für IT-Leiter, CIO und CFO gleichermassen.

Sofortmassnahmen – diese Woche

1. Ticket-Realität anschauen: Lassen Sie sich die Support-Tickets der letzten drei Monate zeigen. Wie viel davon ist wiederkehrendes Firefighting? Diese Zahl ist Ihr Business Case gegenüber dem Management.

2. KI-Check durchführen: Welche KI-Tools nutzen Ihre Mitarbeitenden bereits – offiziell und inoffiziell? Welche Firmendaten landen dort? Das ist Ihr dringlichstes Schatten-IT-Risiko.

3. Tool-Inventar starten: Welche Anwendungen sind im Einsatz? Wer bezahlt sie, wer nutzt sie wirklich? Rechnen Sie mit Überraschungen.

4. Austritts-Test machen: Nehmen Sie einen fiktiven Mitarbeiteraustritt: Wie lange dauert es, bis sämtliche Zugänge entzogen sind? Wenn die Antwort in Tagen gemessen wird, kennen Sie Ihre grösste Compliance-Lücke.

Mittelfristig – in den nächsten 90 Tagen

1. Vollständige Bestandsaufnahme: Tools, Identitäten, Geräte und Zugriffe systematisch erfassen, inklusive Schatten-IT und Schatten-KI. Ungenutzte Lizenzen sofort kündigen.

2. Identitäts- und Zugriffsmodell definieren: Eine Identität pro Person, MFA flächendeckend, Roadmap zu Passkeys/Passwordless, Zugriff nach minimalen Rechten.

3. Endgeräte-Management aufsetzen: Jedes Gerät bekannt, konform und aus der Ferne verwaltbar. Sowohl Firmen- als auch private Geräte mit Firmenzugriff gehören ins Management.

4. Beratungsgespräch führen: Sprechen Sie mit einem Partner, der sich die Zeit nimmt, Ihre Situation zu verstehen – und Ihre Architektur ehrlich analysiert, bevor er etwas empfiehlt.

Strategisch: Ihre Workplace-Roadmap

1. Governance verankern: Klare Regeln für neue Tools, KI-Nutzung, Datenablage und Zugriffe. Leichtgewichtig, verbindlich, revDSG-konform.

2. Tools konsolidieren: Redundante Lösungen ablösen, verbleibende sauber integrieren. Ziel ist ein Workplace, nicht zehn.

3. Von reaktiv zu proaktiv: Monitoring und Automatisierung so aufbauen, dass Probleme gelöst werden, bevor Mitarbeitende sie bemerken.

4. KI-Readiness sicherstellen: Fundament aufbauen, das KI-Einsatz sicher macht: saubere Identitäten, Berechtigungsmodelle, Datensouveränität.

JETZT DEN ERSTEN SCHRITT MACHEN.

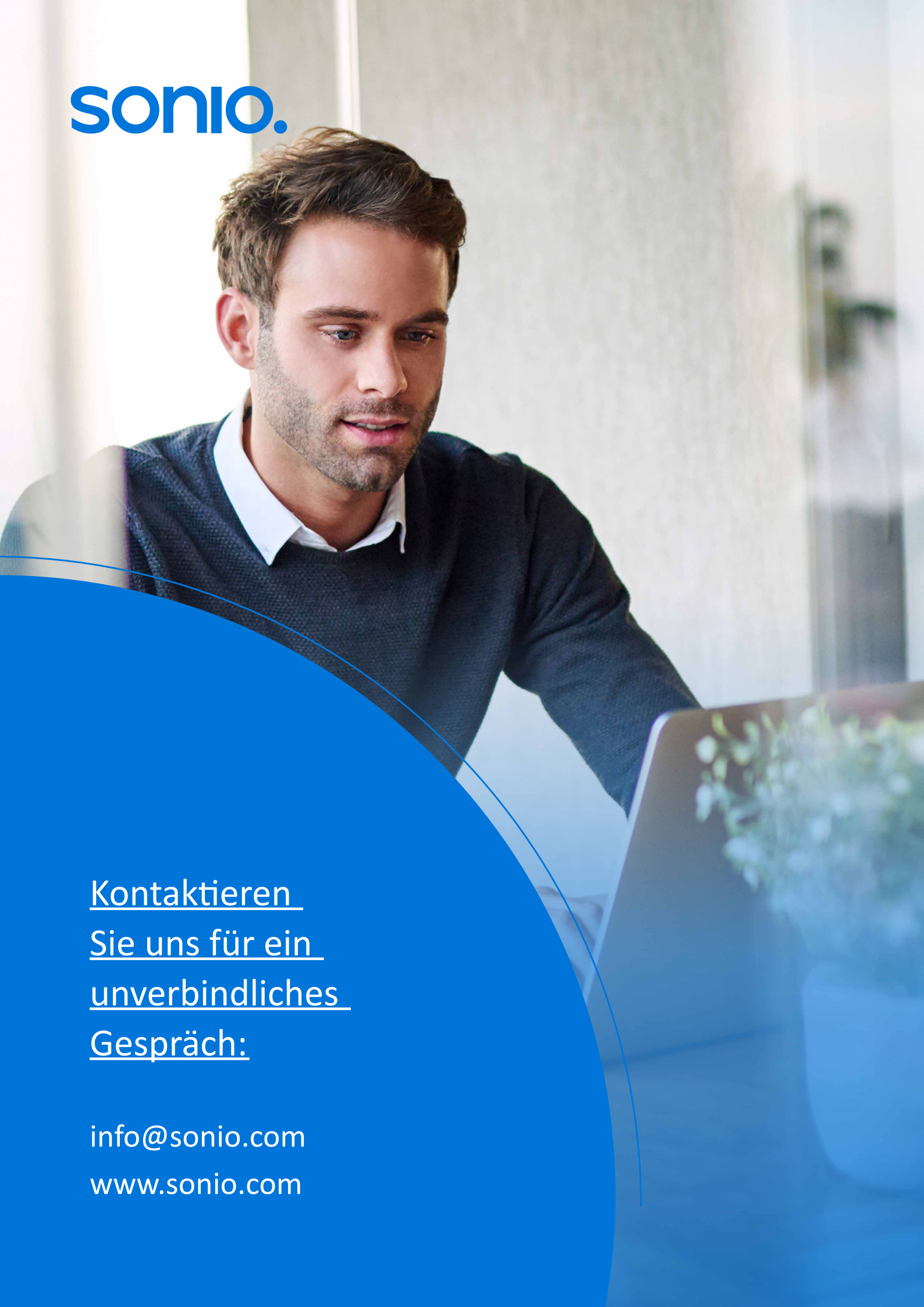
Lassen Sie uns Ihre aktuelle Arbeitsplatz-Architektur gemeinsam analysieren: wo Ihr Fundament steht, wo die grössten Brandherde liegen und welche Massnahmen sofort Wirkung zeigen.

Wir nehmen uns die Zeit, Ihre Situation zu verstehen – bevor wir etwas empfehlen.

Vereinbaren Sie jetzt ein unverbindliches Erstgespräch:
info@sonio.com
www.sonio.com/digital-workplace

Quellen: Primärquelle: Interview mit Michael Wilkens (Head of Digital Workplace, Sonio AG) und Jonny Neumann-Nitsche (Security & Modern Work Expert, Sonio AG), Juli 2026. Dieses Gespräch bildete die inhaltliche Ausgangsbasis des White Papers: Praxisbeobachtungen, Fundament-Modell, Firefighting-Metapher, KI-Readiness-Ansatz sowie die Positionierung von Sonio im Digital Workplace Umfeld entstammen direkt diesem Interview. Schweizer & EU-Quellen: NCSC Halbjahresbericht 2025/2 (Phishing und Ransomware als Hauptbedrohung Schweiz). SWICO ICT INDEX Q3 2026 (Kostendruck und Effizienz CH-Markt). ENISA Threat Landscape 2025 v1.2 (Identitäten als Einfallstor, EU). PwC Switzerland: «Welche wichtigen Veränderungen bringt das revidierte DSG mit sich?» (revDSG-Kostenfolgen CH). revDSG (Bundesgesetz über den Datenschutz, in Kraft seit September 2023). ISG (Informationssicherheitsgesetz, SR 128). Internationale Quellen: Zylo SaaS Management Index 2025 (Ø 275 SaaS-Apps, ein Drittel Schatten-IT, ~50 % Lizenzen ungenutzt). Flexera State of the Cloud 2025 (27 % Cloud-Spend verschwendet). Verizon Data Breach Investigations Report 2025 (80 % Datenpannen durch kompromittierte Anmeldedaten). Microsoft Security Berichte 2025 (7'000+ blockierte Passwort-Angriffe/Sek., +75 % YoY; BEC +34 %). Sonio AG: Blogartikel «Workplace Rollout Services: Ihr Wettbewerbsvorteil im digitalen Wandel», Juli 2025; «Der digitale Arbeitsplatz gelingt nur mit professionellen Pre- und Roll-Out Services»; Landing Pages sonio.com/digital-workplace, sonio.com/digital-workplace-firefighting.

sonio.



Kontaktieren Sie uns für ein unverbindliches Gespräch:

info@sonio.com
www.sonio.com