

DIGITAL WORKPLACE
DAS GANZE SEHEN. WEITER KOMMEN.



MANAGED WORKPLACE

Ganzheitlicher Betrieb Ihrer Microsoft 365 Arbeitsplätze.

Über ADLON

 **1988**
GRÜNDUNG

IT-Beratungsunternehmen
mit Umsetzungs- und
Betriebskompetenz

52


Nutzen regelmäßig
HOMEOFFICE



ALTER

27001
 **ISO**



ECO-Netzwerk
gemanagt seit 2014



work like a
digital leader 

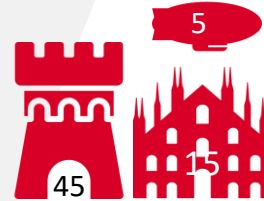
49  **65** **MITARBEITER**  **16**

Great Place To Work.



2009

Management Buyout

5


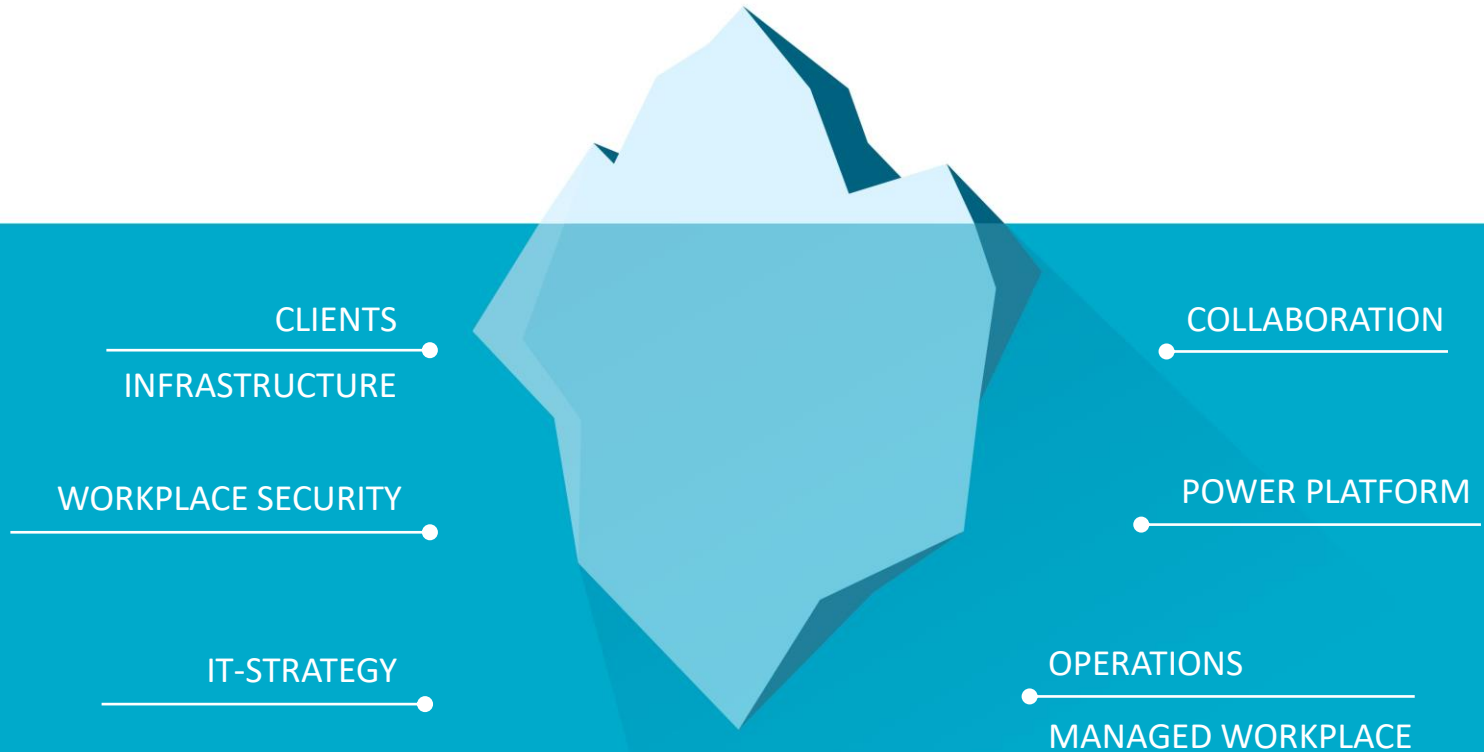
STANDORTE



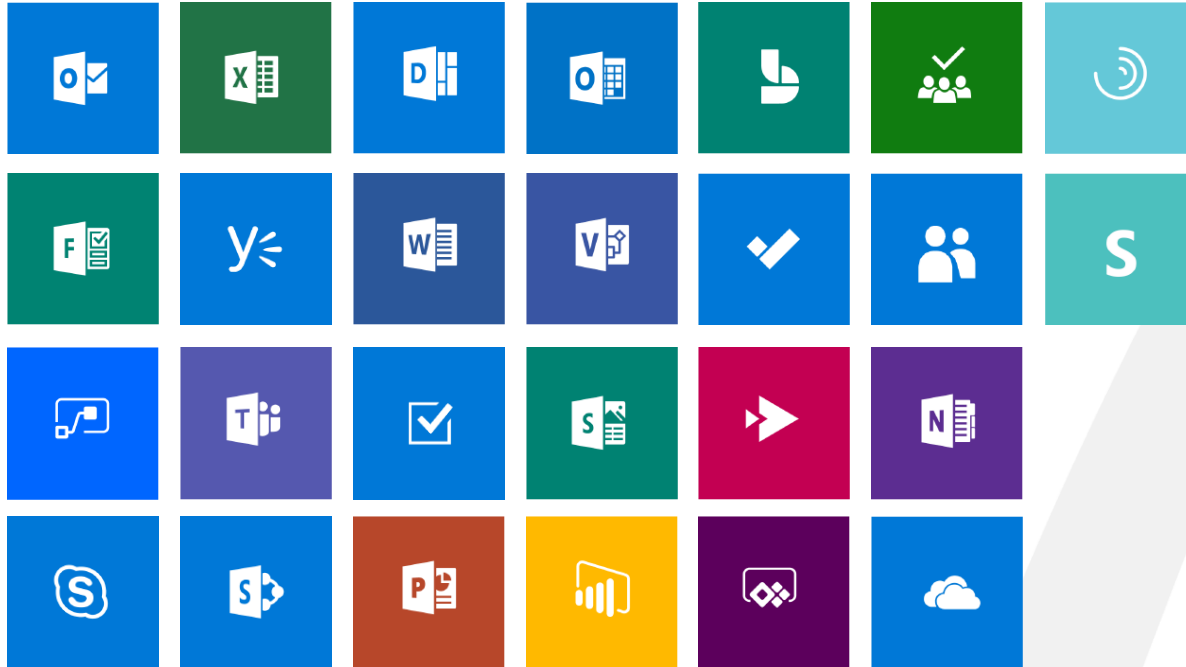
D21
Netzwerk
Digitale Gesellschaft

DIGITAL WORKPLACE

DAS GANZE SEHEN. WEITER KOMMEN.



Microsoft 365: alle Apps für pragmatische Ansätze im Überblick



- Teamarbeit
- Office
- Intranet
- Online Besprechung
- Soziales Netzwerk
- Datenspeicherung & Freigabe
- Aufgabenverwaltung
- Geschäftsprozessautomatisierung
- Suchen & Entdecken
- Analyse & Auswertung
- Mail & Kalender
- Personalplanung

<https://adlon.de/office-365-uebersicht>

The image displays a collage of Microsoft security and management dashboards:

- Microsoft Endpoint Manager admin center:** Shows device enrollment (OK), compliance (11 devices not in compliance), and configuration (OK) status. It also lists client apps and app protection policy user status.
- Microsoft Defender Security Center:** Features a Threat & Vulnerability Management dashboard with an exposure score of 44% (401/902). It includes a bar chart for application exposure scores (e.g., 36%, 46%, 57%, 58%, 43%) and a donut chart for machine exposure distribution (880k total).
- Microsoft Azure Active Directory:** Provides an overview of user risk, showing 8 new risky users detected and 17 unprotected risky sign-ins. It also displays 111 total sign-ins, with 85 unprotected and 26 protected.
- Top security recommendations:** Lists critical alerts such as "Block executable files from running unless they meet...", "Block untrusted and unsigned processes that run from...", "Block [redacted] from creating child processes", "Block Office communication application from creating...", and "Block process creations originating from [redacted] and...".

Wer kümmert sich um ... ?



Bedürfnis aus dem Markt: Sicherer Betrieb digitaler Arbeitsplätze = managed

Microsoft
Partner

Gold Cloud Productivity
Gold Datacenter
Silver Collaboration and Content
Silver Cloud Platform
Silver Small and Midmarket Cloud Solutions
Silver Application Development
Silver Windows and Devices

Betrieb für den Arbeitsplatz auf dem Punkt gebracht

Der Fokus liegt auf Services, die einen produktiven und sicheren Betrieb von Microsoft 365-Arbeitsplätzen gewährleisten.

So können sich Ihre Mitarbeiter auf Ihre Arbeit konzentrieren.

Mehr Zeit für Innovation durch Auslagerung

Wir übernehmen den Betrieb und Support Ihrer Arbeitsplätze ganzheitlich.

So geben Sie Ihrer IT Spielraum für Ihr Kernbusiness und für Innovation.

Rundum-Service pro Device

Neben dem Betrieb übernehmen wir auch die Beschaffung, Bereitstellung und Verwaltung Ihrer Devices.

So reduzieren Sie die Komplexität der IT-Prozesse über ausgelagerte Standards.

Zertifizierter Microsoft-Partner

Profitieren Sie von unserer Erfahrung in der Einführung von digitalen Arbeitsplätzen sowie von 30 Jahren Betriebs- und Support-Expertise.

Durch einen zuverlässigen Ansprechpartner.

Managed Workplace \neq Managed Service



Was verstehen wir unter dem Begriff **Managed** konkret?

MONITORING

REAKTION

BETREUUNG

MANAGED

TECHNOLOGISCHE
WEITERENTWICKLUNG

PATCHMANAGEMENT

GOVERNANCE

Managed Cloud

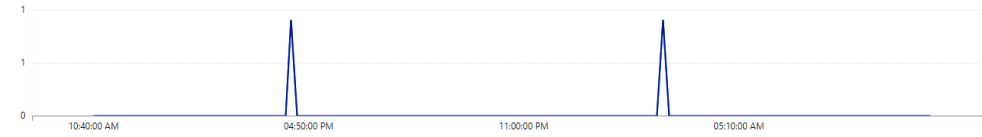
- **Monitoring:**
Kontinuierliche Überwachung des digitalen Arbeitsplatzes und eine frühzeitige Warnung kritischer Ausfälle durch die Nutzung von Microsoft Alerting Funktionen und Security Dashboards.
Z. B. Monitoring automatisierter Prozesse mit PowerAutomate.
- **Backup & Recovery:**
Schnelle Datenwiederherstellung und Gewährleistung der Ausfallsicherheit durch automatisierte und dokumentierte (ISO) Sicherungen und Wiederherstellungsprozesse.
Z. B. um ein gelöscht Verzeichnis wieder herzustellen.
- **Reaktion:**
Effizientes Beheben von Störfällen aus dem Monitoring und Identifikation kritischer Mustern durch ein standardisiertes oder individuelles Vorgehen. Z. B. Aktivierung eines gestoppten Flows.
- **Betreuung:**
Unkomplizierte Sicherstellung der Lauffähigkeit und Produktivität am digitalen Arbeitsplatz mittels kleinerer Anpassungen und Serviceleistungen.
Z. B. Anlage eines externen Users als Mitglied in Teams.
- **Technologische Weiterentwicklung:**
Bewertung der Hersteller- und Produkt-Releases auf Relevanz für das eigene Business und Integration dieser Entwicklungsschritte durch erfahrene und zertifizierte Experten.
Z. B. Neues Apple IOS, für das in Intune der Switch vorbereitet werden muss.
- **Governance:**
Sicherstellung eines strukturierten Ökosystems und einer skalierfähigen Struktur durch durchdachte Berechtigungen und Rollenkonzepte sowie fertige Templates und Apps.
Z. B. Die Teamsrequester App für Microsoft Teams
- **Patchmanagement:**
Reduktion von Sicherheitslücken und hohe Aktualität der Arbeitsplätze durch regelmäßige Updates und Patches. Z. B. Update von Windows Betriebssystemen und Prüfung der Auswirkungen.

Monitoring & Alerting

Vorfälle

[Benachrichtigungsregel erstellen](#)

Neueste Vorfälle und Benachrichtigungen



Vorfälle Benachrichtigungen

1-1 < > 6 Monate Spalten auswählen 30 Elemente pro Seite Filter

✓	Vorfallname	Tags	Schweregr...	Untersuchungsstatus	Kategorien	Betroffene Entitäten	Aktive Warnu
>	Multiple failed user logon attempts to a service		■ ■ ■ Hoch	N/V	Verdächtige Aktivität		1/1

Microsoft 365 Defender - New incident

Customer	ADLON Intelligent Solutions GmbH
ID	9518
Incident name	Multiple failed user logon attempts to a service
Severity	High
Categories	SuspiciousActivity
Time	7/15/2021 9:04:11 AM UTC
Incident page	https://sip.security.microsoft.com/incidents/byalert?alertId=ca60effa06cdbeaf0b8767746e&source=incidentemail&tid=c5474d26-aacb-4625-b8fa-fbd51ff0427d

Reaktion & Betreuung

Vorfälle > Multiple failed user logon attempts to a service

Multiple failed user logon attempts to a se...

Vorfall verwalten ? Bedrohungsexperten konsultieren Kommentare und Verlauf

Zusammenfassung Warnings (1) Geräte (0) Benutzer (0) Postfächer (0) Untersuchungen (0) Beweis und Antwort (0) Diagramm

Warnungen und Kategorien

1/1 aktive Benachrichtigungen
Kein MITRE ATT&CK-Taktiken
1 sonstige Warnungskategorien

Bereich: Keine betroffenen Entitäten

Nachweis: **Keine Entitäten gefunden**

© 2018 The MITRE Corporation. Diese Arbeit wird reproduziert und mit der Erlaubnis von The MITRE Corporation verteilt.

8. Sep. 2021, 02:59:49 | Neu
Multiple failed user logon attempts to a service

Warnungen > **Multiple failed user logon attempts to a service** 8.9.21 02:59

Multiple failed user logon attempts to a service Active Directory instance 0

Warnung schließen ^

- False Positive...
- Unschädlich...
- True Positive...

Beschreibung
Aktivitätsrichtlinie "Multiple failed user logon attempts to a service" wurde ausgelöst.

Aktivitätsprotokoll

In Aktivitätsprotokoll untersuchen 1 - 10 von 10 Aktivitäten Details anzeigen Tabelleneinstellungen

Aktivität	Benutzer	App	IP-Adresse	Standort	Gerät	Datum
Failed log on (Failure message: WrongPassword)	N/V	Active Director...	[REDACTED]	-	[REDACTED]	7. Sept. 2021, 12:51

Vorfall verwalten

Vorfallsname
Multiple failed user logon attempts to a service

Vorfallstags

Mir zuweisen
Nicht zugewiesen

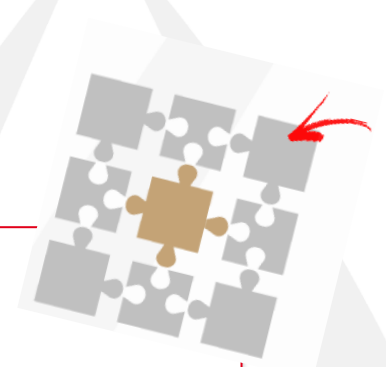
Vorfall auflösen

Das Lösen eines Vorfalls löst ebenfalls alle verknüpften aktiven Warnungen.

Klassifizierung
Nicht festgelegt

- Nicht festgelegt
- Falsche Warnung
- Echte Warnung

Service-Bausteine **Managed Workplace**



Managed M365 Base



**Managed
Clients**



**Managed
Security**



**Managed
Collaboration**



**Managed
Power Platform**



IT-Service Desk

Service-Bausteine **Managed Workplace**



Managed M365 Base

Zur Abdeckung der Mindestanforderungen an Transparenz, Kontinuität, Sicherheit und Entwicklung.

- Kontinuierliche Transparenz zur Arbeitsplatzproduktivität mit regelmäßigen Checks und schneller Reaktion.
- Grundlegende Sicherheitsmaßnahmen durch die in Microsoft 365 enthaltenen Funktionen.
- Hohe Entwicklungskraft durch Microsoft als treibendes Innovationsunternehmen. Erfahrene und zertifizierte Experten von Adlon prüfen die Relevanz und adaptieren die Funktionen auf Ihre Arbeitsplatz-Umgebung.
- Basiert auf der Business Premium Lizenzierung
 - [Overview of Microsoft 365 Business Premium Security - Office Support](#)

M365
Projekt

Workshop

Konfiguration

Managed Workplace mit „Managed M365 Base“

Service-Bausteine **Managed Workplace**



Zur zentralen, maximal automatisierten Bereitstellung und Verwaltung aller Devices im Unternehmen.

- Durchgängige Aktualität der Devices (Windows/Mobil) insb. bei Änderung von Umgebungsparametern.
- Minimaler Aufwand beim Device Management durch das UEM von Microsoft 365 für alle Devices.
- Adäquate Steigerung digitaler, automatisierter Prozesse in der Administration.
- Unkomplizierte Anbindung an ein Geräte-Verwaltungsportal zur Reduktion der Komplexität von Prozessen.



Service-Bausteine **Managed Workplace**



Zum Schutz der Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Informationen sowie zur aktiven Vorbeugung vor akuter Bedrohung.

- Schutz der Endpunkte – Clients und/oder Server
- Prävention & Reaktion bei Risiken und Gefahren
- Aktualität & Konformität von Datenschutz und Technik
- Security- & Risikomanagement

Risiko
Analyse

Einrichtung der Dashboards/Bausteine

Sicherer Betrieb mit: Identity Protection | Endpoint Protection |
Vulnerability Management | Cloud Backup

Managed Security - Leistungsscheine

Absicherung von Clients und Servern mit "Endpoint Protection,,

Sicherheit von Daten und Informationen – insbesondere im Homeoffice

Initial wird die Konfigurationen des Endpoint Managements vorgenommen:

- Konfiguration der Umgebung
- Einrichtung der Dashboards
- Bereitstellung der Dokumentationsform

Anschließend wird fortlaufend gemanaged:

- Monitoring und Alarmierung von aktiven Bedrohungen, Schwachstellen und Konfigurationsfehlern in der Endgerätestruktur durch IT-Sicherheitsspezialisten
- Einstufung der Risiken nach Schweregrad
- Behandeln von Risiken durch z. B. Anpassung an der Konfiguration der Endgeräte oder Kommunikation
- Betreuung durch Nachuntersuchung, Anpassungen z. B. auch der Risikorichtlinien
- Umstellungen in Backendsystem bei technologischen Sprüngen von Microsoft bzw. der Endgerätehersteller
- Basiert auf Defender for Endpoint
 - [Microsoft Defender für Endpunkt, Microsoft 365](#)
 - [Reduce organizational risk with Threat and Vulnerability Management \(cloudguides.com\)](#)



Typische Risiken, die durch Endpoint Protection behoben werden können:

- Erkennen von Rootkits
-
- Erkennen von Schadsoftware oder Spyware
-
- Erkennen von Konfigurationsfehlern
-
- Angriffsflächen durch fehlende Anpassungen in der Konfig & Security

Quelle: ADLON 2021

Monitoring

- Startseite
- Vorfälle & Warnungen
 - Vorfälle
 - Benachrichtigungen
- Suche
- Aktionscenter
- Bedrohungsanalysen
- Sicherheitsbewertung
- Lern-Zentrum

Endpunkte

- Suchen
- Geräteinventar
- Sicherheitsrisikomanagement
 - Dashboard
 - Empfehlungen
 - Wartung
 - Softwarebestand
 - Schwächen
 - Ereigniszeitachse
- Partner und APIs

Threat & Vulnerability Management dashboard

Gefährdungsscore der Organisation

Gefährdungsscore

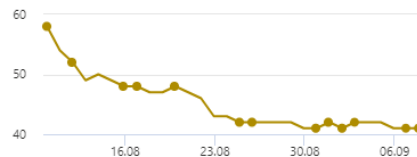
Diese Bewertung spiegelt die aktuelle Gefährdung wider, die mit Geräten in Ihrer Organisation verbunden ist. Die Bewertung wird möglicherweise durch aktive Ausnahmen beeinflusst.



41/100

■ Niedrig 0-29 ■ Mittel 30-69 ■ Hoch 70-100

Gefährdungsscore im Zeitverlauf



[Bewertung verbessern](#)

Die wichtigsten Sicherheitsempfehlungen

Empfehlung	Ge...
Block process creations originating from PSEXEC and WMI ...	83
Google Chrome aktualisieren	35
Adobe Acrobat Reader Dc aktualisieren	27

[Mehr anzeigen](#)

[Ausnahmen anzeigen](#)

Microsoft-Sicherheitsbewertung für Geräte

Ihre Bewertung für Geräte: 78 %

Diese Bewertung widerspiegelt den gemeinsamen Status der Sicherheitskonfiguration Ihrer Geräte über Betriebssystem, Anwendung, Netzwerk, Konten und Sicherheitskontrollen hinweg. Die Bewertung wird möglicherweise durch aktive Ausnahmen beeinflusst.

707/902 Punkte erreicht

Application	59/75
OS	149/197
Network	87/98

Reaktion

- Startseite
- Vorfälle & Warnungen
 - Vorfälle
 - Benachrichtigungen
- Suche
- Aktionscenter
- Bedrohungsanalysen
- Sicherheitsbewertung
- Lern-Zentrum
- Endpunkte
 - Suchen
 - Geräteinventar
 - Sicherheitsrisikomanagement
 - Dashboard
 - Empfehlungen

Security recommendations

Exportieren

Filter: Korrekturart: Softwareupgrade +2

Sicherheitsempfehlung	Betriebssystem-Plattf...	Schwachstellen	Zugehörige Kom
Google Chrome aktualisieren	Windows	285	Google Chrome
Adobe Acrobat Reader Dc aktualisieren	Windows	517	Adobe Acrobat Ri
Icinga aktualisieren	Windows	13	Icinga
Microsoft Windows Server 2012 R2 aktualisieren (Betriebssystem und integriert...	Windows	100	Microsoft Window
Teamviewer aktualisieren	Windows	4	Teamviewer
Microsoft Windows Server 2019 aktualisieren (Betriebssystem und integrierte A...	Windows	426	Microsoft Window
Microsoft Windows Server 2016 aktualisieren (Betriebssystem und integrierte A...	Windows	103	Microsoft Window
Oracle Jre aktualisieren	Windows	202	Oracle Jre

Google Chrome aktualisieren

Wartung erforderlich

Softwareseite öffnen Ungenauigkeit melden

Allgemein Gefährdete Geräte Installierte Geräte Verbundene CVEs Korrekturmaßnahmen

Beschreibung

Chrome aktualisieren auf eine neuere Version zur Minderung von 285 bekannten Sicherheitsrisiken Ihre Geräte beeinträchtigen.

Verbundene CVEs

Kritisch | Hoch | Mittel | Niedrig
3 | **161** | **121** | **0**

- Ein Verifiziert codeausführung per fernzugriff-Exploit ist für eine oder mehrere Schwachstellen im Zusammenhang mit dieser Empfehlung öffentlich verfügbar

Details

Anzahl von Sicherheitsrisiken
285

Exploit verfügbar
Ja

Gefährdete Geräte
35 / 57

Auswirkungen
▼ 7.99

Gefährdete Betriebssysteme
Windows 10, Windows Server 2019

Wartung anfordern

Ausnahmooptionen

Betreuung

Google Chrome aktualisieren > Wartung anfordern

● **Wartungsanforderung**

○ Überprüfen und fertigstellen

Wartungsanforderung

Füllen Sie die Wartungsanfrage aus, damit das zuständige Team diese Sicherheitsempfehlung umsetzen kann. Änderungen

- Startseite
- Vorfälle & Warnungen
- Vorfälle
- Benachrichtigungen
- Suche
- Aktionscenter
- Bedrohungsanalysen
- Sicherheitsbewertung**
- Lern-Zentrum
- Endpunkte
 - Suchen
 - Geräteinventar
 - Sicherheitsrisikomanagement
- Dashboard
- Empfehlungen
- Wartung
- Softwarebestand
- Schwächen
- Ereigniszeitachse

Korrektur

Korrekturmaßnahmen Ausnahmen

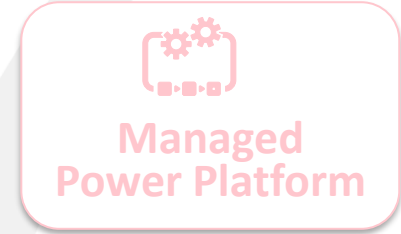
7 Laufende Aktivitäten 7 Überfällige Aktivitäten

Exportieren

15 Elemente Filter Spalten anpassen

Korrekturmaßnahme	Zugehörige Komponente	Korrekturart	Priorität	Gerätewartungsstatus	Status der Gerätewartung
Google Chrome aktualisieren	Google Chrome	Softwareupdate	Hoch	In Bearbeitung	7/21
Adobe Acrobat Reader Dc aktualisieren	Adobe Acrobat Reader Dc	Softwareupdate	Hoch	In Bearbeitung	5/30
Teamviewer aktualisieren	Teamviewer	Softwareupdate	Hoch	In Bearbeitung	5/29
Microsoft .net Framework aktualisieren	Microsoft .net Framework	Softwareupdate	Hoch	In Bearbeitung	1/3
Icinga aktualisieren	Icinga	Softwareupdate	Hoch	In Bearbeitung	0/26
Zoom aktualisieren	Zoom	Softwareupdate	Hoch	In Bearbeitung	8/18
Mozilla Firefox aktualisieren	Mozilla Firefox	Softwareupdate	Hoch	In Bearbeitung	7/12
Update Adobe Acrobat Reader Dc	Adobe Acrobat Reader Dc	Softwareupdate	Hoch	Abgeschlossen	59/59
Fix unquoted service path for Windows services	Operating system (Services)	Konfigurationsänderung	Hoch	Abgeschlossen	64/64

Service-Bausteine **Managed Workplace**



Für einen produktiven Betrieb von Microsoft Teams, Sharepoint und Exchange Online u.a. mit Backup, Monitoring, Lifecycle- & Feature-Management.

- Produktivität der Collaboration Lösungen Teams, Sharepoint und Exchange wird sicher gestellt.
- Kontinuierliche Transparenz zur Produktivität von Teams, Sharepoint und Exchange.
- Regelmäßigen Checks und schneller Reaktion auf Auffälligkeiten - so dass Sie es nicht tun müssen.
- Einrichten dedizierter Sicherheitsmaßnahmen durch die in den Lösungen enthaltenen Funktionen
- Erfahrene und zertifizierte Experten von Adlon prüfen die Relevanz von neuen Entwicklungen und adaptieren die Funktionen auf Ihre Anforderung.

Collabor.
Projekt

Konfiguration

Managed Workplace mit „Managed Collaboration“ für Teams, Sharepoint, Exchange

Service-Bausteine **Managed Workplace**



Für einen reibungslosen Betrieb von Microsoft Power Platform (PowerAutomate, PowerBI, PowerApps, ...) u.a. mit Monitoring, Backup & Feature-Management.

- Produktivität der Lösungen die mit PowerPlatform gebaut wurden, wird sichergestellt.
- Kontinuierliche Transparenz zur Produktivität von PowerApps, PowerBI und PowerAutomate.
- Regelmäßigen Checks und schneller Reaktion auf Auffälligkeiten - so dass Sie es nicht tun müssen.
- Kontinuierliche Digitalisierung bzw. Weiterentwicklung als fixes Bestandteil des Managed Workplace.
- Erfahrene und zertifizierte Experten von Adlon prüfen die Relevanz von neuen Entwicklungen und adaptieren die Funktionen auf Ihre Anforderung.

PowerP.
Projekt

Konfiguration

Managed Workplace mit „Managed PowerPlatform“ für PowerAutomate, PowerBI, PowerApps, ...

Bedenken gegen das Outsourcing des Managed Workplaces



Wird schon gut gehen



Dass können wir uns sparen



Angst vor Abhängigkeit

Gründe für das Outsourcing des Managed Workplaces



Unterstützung der internen IT



Neuester Stand an Technik & Sicherheit



Kontrolle / Investitionsschutz

DIGITAL WORKPLACE

DAS GANZE SEHEN. WEITER KOMMEN.



MANAGED WORKPLACE

Ganzheitlicher Betrieb Ihrer Microsoft 365 Arbeitsplätze.

Online Impuls: Managed Workplace
am 14. September
Kostenlos anmelden!



#MANAGED WORKPLACE

Worauf es bei der Verwaltung, Sicherheit und
Weiterentwicklung des digitalen Arbeitsplatzes ankommt.

