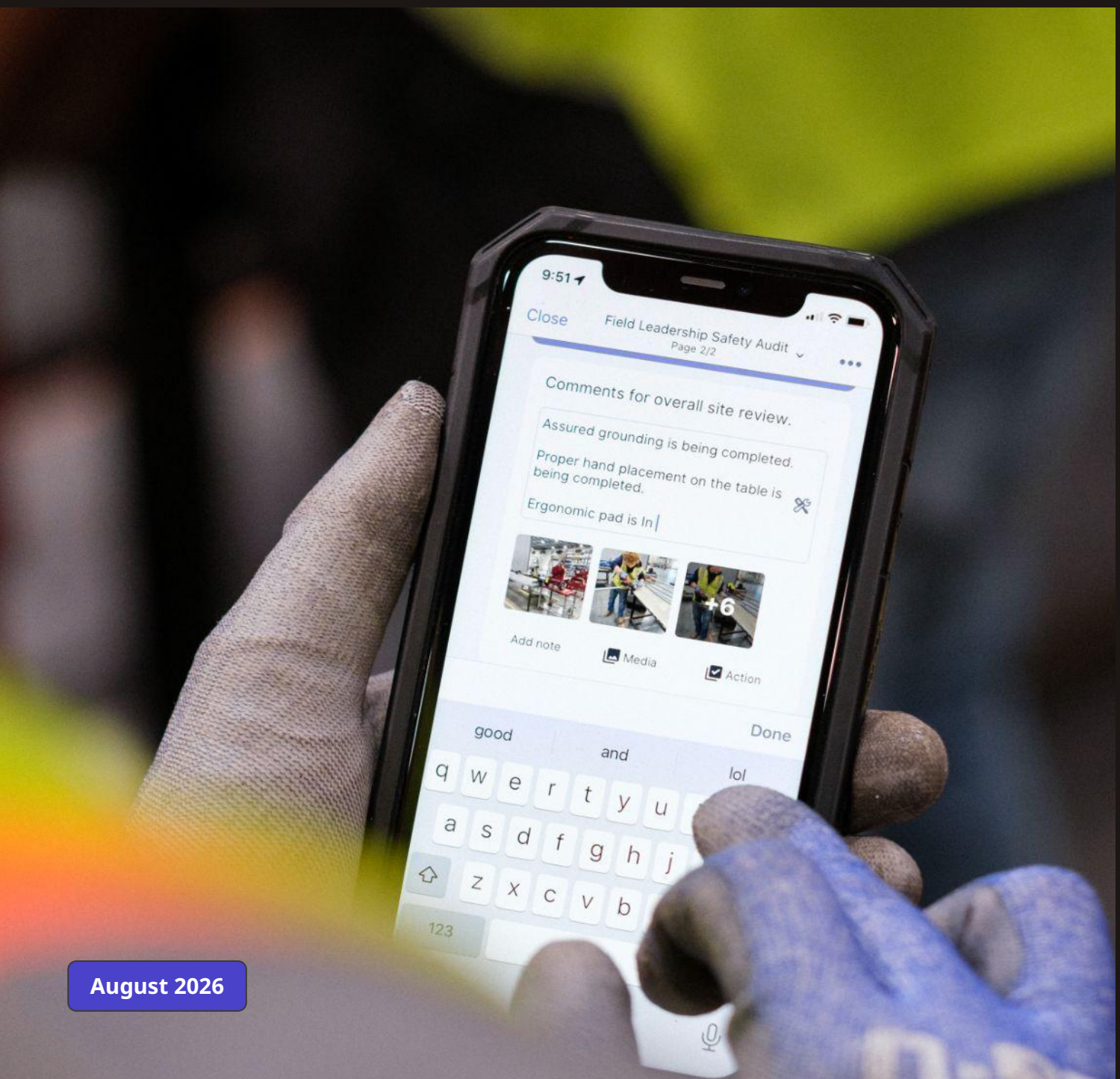
Mitti
by SafetyCulture

Überblick: Sicherheit

Mittis Cybersicherheit verstehen



August 2026

Inhaltsverzeichnis

Handhabung 4

Übersicht über die Cybersicherheit 5

Sicherheitspraktiken auf Unternehmensebene 6

Sicherheits-Governance
Zugriff auf interne Systeme und Cloud-Plattformen
Protokollierung und Überwachung
Drittanbietersicherheit
Schulungen zum Sicherheitsbewusstsein
Patch- und Schwachstellenmanagement

Schutz von Kundendaten 9

Einschränkung des Datenzugriffs
Physischer Zugriff auf Kundendaten
Datenverschlüsselung
Datensicherungen
Löschung und Entsorgung von Daten

Sicherheit unserer Produkte 11

Sichere Softwareentwicklungspraktiken
Änderungskontrolle
Identifizierung von Schwachstellen und Patch-Entwicklung

Umgang mit Sicherheitsvorfällen 12

Mitti und KI 14

Wie Mitti KI verwendet
KI-Funktionen in Mitti
KI-Anbieter und Sicherheit
Zugriff und Kontrollen
Kundendaten und Trainingsmodelle

Schlussbemerkung 15

Literaturhinweise

Mitti

“

Vor der Einführung von Mitti mussten wir die Daten von Checklisten im Büro manuell abtippen und sie dann in Excel analysieren, bis wir sie endlich mit dem Team teilen konnten. Die Analysen liefern uns umfassendere Daten in einem Gebiet, die wir teilen können.

”

Deaky Wong
Wartungsingenieur bei Cathay Pacific

Unser Fokus

Die Mission von Mitti ist es, Unternehmen dabei zu unterstützen, durch innovative, kostengünstige Mobile-First-Produkte sicherere und hochwertigere Arbeitsplätze auf der ganzen Welt zu schaffen.

Wir erfüllen unsere Mission durch unsere Software-as-Service (SaaS)-Produkte.

Unsere Produkte werden täglich von mehr als 27.000 Unternehmen weltweit in zahlreichen Branchen und für eine Vielzahl von Anwendungsfällen eingesetzt.

Wir sind stolz darauf, dass Mitti als ein weltweit führender Anbieter von Produkten zur Förderung von Sicherheit und Qualität geschätzt wird, und wir wissen, wie wichtig unsere Rolle ist, wenn es darum geht, unseren Kunden zu helfen, ihren täglichen Betrieb zu optimieren.

Wir sehen unsere Vorgehensweise bei der Cybersicherheit als eine wichtige tragende Säule, um unseren Status als führendes Unternehmen in diesem Bereich aufrechtzuerhalten, und dieser Inhalt gibt einen Überblick darüber, wie wir Cybersicherheit als Unternehmen angehen

Mitti ist nach ISO 27001:2024 zertifiziert und wir befolgen die AICPA Vertrauensdienste Kriterien, die unser Engagement für die Sicherheit unserer Kunden bekräftigen.

Überblick

Cybersicherheitsprogramm

Mitti verfügt über ein aktives, robustes und sich kontinuierlich verbesserndes Cybersicherheitsprogramm, um sicherzustellen, dass unser Unternehmen und die von uns bereitgestellten Produkte sicher sind. Das Cybersicherheitsprogramm von Mitti setzt eine Reihe von Kontrollen auf technischer und operativer Ebene ein, um sicherzustellen, dass wir über einen effektiven, umfassenden Verteidigungsansatz verfügen, um uns vor Cyberangriffen zu schützen und die von unseren Software-as-a-Services (SaaS)-Produkten verarbeiteten Daten zu sichern.

Zu den wichtigsten Funktionen gehören:

Ein Sicherheitsprogramm, das an Best-Practice-Standards der Branche ausgerichtet ist, einschließlich der Verwendung von Cloud-Plattformen, die vertrauenswürdigen Sicherheits-Benchmarks wie ISO 27001 und SOC 2 entsprechen.

Der Fokus darauf, die richtigen Grundlagen zu schaffen und zu erkennen, dass die Grundlagen der Sicherheit nach wie vor die kritischsten sind.

Dazu gehören:

- Schulung unserer Mitarbeiter über die Bedeutung der Sicherheit.
- Ein engagiertes Sicherheitsteam zu haben, das dafür verantwortlich ist, unser Unternehmen vor tatsächlichen und möglichen Bedrohungen für unser Geschäft und die Daten zu schützen, die Kunden uns anvertrauen.
- Einsatz robuster Mechanismen, um sicherzustellen, dass der Zugriff auf die Systeme und Kundendaten von Mitti sorgfältig kontrolliert wird.
- Verschlüsseln der von uns gespeicherten Kundendaten (sowohl während der Übertragung als auch im Speicher) mit robusten Verschlüsselungsmechanismen.
- Sicherstellen, dass wir Patches in unserer IT-Umgebung und auf unseren Produkten so schnell wie möglich anwenden, um die Möglichkeit zu minimieren, dass Schwachstellen von Cyberangreifern ausgenutzt werden.
- Aktive Überwachung und Prüfung unserer IT-Umgebung und unserer Produkte auf Schwachstellen und deren schnellstmögliche Behebung.
- Ein klar definierter Prozess zur Bereitstellung effektiver Unterstützung und Reaktion im Falle eines Sicherheitsvorfalls.

Wir wenden die gebotene Sorgfalt an, um sicherzustellen, dass unsere Dienstanbieter die Industriestandards in Bezug auf Sicherheit erfüllen – wir wissen, dass die Sicherheit unserer Partner uns und unsere Kunden direkt betrifft, daher wählen wir sehr sorgfältig aus, mit wem wir zusammenarbeiten.

Die übrigen Teile dieses Dokuments bieten einen Überblick über die verschiedenen Teile unseres Sicherheitsprogramms.

Sicherheitspraktiken auf Unternehmensebene

Die Sicherheitsverfahren unseres Unternehmens orientieren sich an den empfohlenen Best Practices anerkannter Normen wie NIST, ISO 27001 und SOC.

Sicherheitsmanagement

Mitti verfolgt eine Reihe dokumentierter Richtlinien, Standards und Verfahren, die das Sicherheitskonzept unserer Organisation definieren. Diese Richtlinien und Verfahren werden mit allen Mitarbeitern geteilt und mindestens jährlich überprüft und aktualisiert (und häufiger, wenn wesentliche Änderungen erforderlich sind), um sicherzustellen, dass unser Sicherheitsansatz aktuell bleibt
.
Wir achten darauf, dass die Verantwortlichkeit für die Sicherheit im gesamten Unternehmen gewährleistet ist. Zu diesem Zweck haben wir ein Forum für Informationssicherheitsmanagement mit wichtigen Stakeholdern aus dem gesamten Unternehmen Mitti eingerichtet, das regelmäßig zusammenkommt, um sicherheitsrelevante Themen zu überprüfen und zu besprechen sowie Entscheidungen zu treffen, die Einfluss auf unseren Ansatz zur Cybersicherheit haben.

Mitti ist nach ISO 27001:2024 zertifiziert und wir befolgen die AICPA Vertrauensdienste Kriterien, die unser Engagement für die Sicherheit unserer Kunden bekräftigen.

Zugriffskontrollen

Wir stellen sicher, dass der Zugriff auf Systeme in unserer IT-Umgebung, einschließlich der von uns genutzten Cloud-Plattformen, auf Mitarbeiter beschränkt ist, die diesen Zugriff für ihre Arbeit ausdrücklich benötigen.

Alle Zugriffe von Administratoren erfordern eine Multi-Faktor-Authentifizierung, und Mitarbeiter, die auf unsere Umgebung zugreifen, müssen eine genehmigte VPN-Lösung verwenden.

Die Berechtigungen für den Zugriff auf unsere Systeme werden regelmäßig für jeden einzelnen Mitarbeiter überprüft und nach Bedarf geändert. Im Rahmen unseres Off-Boarding-Verfahrens wird ausscheidenden Mitarbeitern jeglicher Zugriff auf Systeme und Dienste entzogen.

Drittanbietersicherheit

Wir überprüfen von Anfang an und fortlaufend die Sicherheitspraktiken der von uns beauftragten Dienstleistern, um sicherzustellen, dass deren Praktiken den Branchenstandards entsprechen und mit unseren eigenen Datenschutz- und Sicherheitsrichtlinien und -verfahren übereinstimmen. Wenn solch ein Drittanbieter Zugriff auf unsere Systeme benötigt, stellen wir sicher, dass der Zugriff speziell auf den Zweck beschränkt ist, für den er beauftragt wurde.

Da Amazon Web Services (AWS) einer unserer wichtigsten Anbieter ist, arbeiten wir mit AWS nach dem Modell der geteilten Verantwortung für Sicherheit und Compliance zusammen, um sicherzustellen, dass klar definiert ist, wer welche Verantwortung für die Sicherheit übernimmt. AWS verfügt über Akkreditierungen vieler der neuesten Branchenstandards akkreditiert und erfüllt diese. Weitere Informationen finden Sie hier: https://aws.amazon.com/de/artifact.

Für die Verarbeitung von Finanz- und Kreditkartendaten nutzt Mitti mehrere Partner (Chargify, eWay und Stripe), deren Sicherheitspraktiken den Payment Card Industry Data Security Standard (PCI-DSS) erfüllen.

Netzwerksicherheit

Die Unternehmensnetzwerke von Mitti sind durch Firewalls sowie ein Eindringerkennungssystem (Intrusion Detection System, IDS) und ein Eindringver- hinderungssystem (Intrusion Prevention System, IPS) an der Peripherie geschützt, die spezielle Netzwerksicher- heitsgeräte bereitstellen, damit wir jeglichen bösartigen Datenverkehr erkennen und verhindern können.

Für unsere Cloud-basierten Plattformen nutzen wir mit einer mehrschichtigen Strategie zum Schutz vor externen Angriffen hauptsächlich Amazon Web Services (AWS). Auf der Infrastrukturebene setzt AWS Strategien wie Kontrolle des Zugriffs auf Netzwerkgeräte, Trennung von Daten durch Firewalls und virtuelle private Clouds ein, um bösartigen Datenverkehr herauszufiltern, und nutzt umfangreiche Protokollierungs- und Überwachungsfunktionen, um netzwerkbasierte Angriffe zu verhindern. Auf Anwendungsebene nutzen wir Cloudflares Web Application Firewall (WAF) und den Schutz vor Distributed Denial of Service (DDoS), um webbasierte Angriffe und Denial-of-Service-Angriffe auf unsere Produkte zu verhindern.

Unsere Entwicklungs-, Test- und Produktionsumgebungen sind voneinander getrennt.

Sicherheitspraktiken auf Unternehmensebene

Protokollierung und Überwachung

Mitti verwendet ein zentralisiertes Protokollsystem, das Audit-Ereignisse für den Zugriff auf die Anwendung enthält. Diese Protokolle werden 90 Tage lang aufbewahrt. Außerdem nutzen wir die Protokolle von Amazon Elastic Load Balancing (ELB), um Zugriffsanfragen auf den Dienst zu verfolgen. Die in AWS gespeicherten Protokolle können nicht geändert werden, und der Zugriff ist auf die Personen beschränkt, für deren Aufgaben dies erforderlich ist.

Wir sind uns bewusst, wie wichtig es ist, Protokolle regelmäßig zu überprüfen, um böswillige Nutzeraktivitäten aufzudecken und potenzielle Schwachstellen in unseren Produkten zu identifizieren; wir verfügen über ein automatisiertes Überwachungssystem, das uns auf bestimmte Arten potenziell böswilliger Ereignisse innerhalb unserer globalen Infrastruktur hinweist.

Schulungen zum Thema Sicherheit

Alle Mitarbeiter in Technischen und Nicht-Technischen Bereichen von Mitti nehmen regelmäßig an Schulungen zum Thema Sicherheit teil. Zusätzliches Schulungsmaterial zum Thema Sicherheit wird den einzelnen Mitarbeitern bei Bedarf zur Verfügung gestellt, um sicherzustellen, dass sie für die spezifischen sicherheitsrelevanten Herausforderungen ihrer Rolle gerüstet sind.

Patch- und Schwachstellenmanagement

Das Patchen unserer IT-Umgebung ist eine der wichtigsten Maßnahmen, die wir ergreifen, um uns gegen potenzielle Sicherheitsverletzungen zu schützen. Um dies zu erreichen, gehen wir wie folgt vor:

- Wir verwenden AWS System Manager, um regelmäßig Patches für unsere Cloud-basierte Infrastruktur bereitzustellen.
- Wir nutzen Lösungen zur Verwaltung mobiler Geräte (MDM), um sicherzustellen, dass wichtige Patches schnell und effizient installiert werden.
- Unsere Geräte sind mit Endpoint Security-Technologien gesichert, um Sicherheitsbedrohungen wie Viren und Malware-Angriffe zu erkennen und zu verhindern, und überwachen sie auf bösartige Aktivitäten.
- Werden zuerst Patches für die kritischsten Schwachstellen installiert, und zunächst in unserer nicht produktiven Umgebung getestet, bevor sie schnell in der gesamten IT-Umgebung eingesetzt werden.

Schutz von Kundendaten

Mitti nimmt die Sicherheit der Daten unserer Kunden sehr ernst. Wir ergreifen eine Reihe von Maßnahmen, um sicherzustellen, dass Kundendaten sorgfältig geschützt sind.

Schutz der Kundendaten

Einschränkung des Datenzugriffs

Mitti implementiert technische und organisatorische Kontrollen, um Kundendaten vor unbefugtem Zugriff oder Missbrauch durch nicht autorisierte Personen (extern oder intern) zu schützen. Kundendaten werden nur in unserer Produktionsumgebung gespeichert, und der Zugriff auf diese Daten durch Mitti-Mitarbeiter ist auf Mitarbeiter mit der erforderlichen Zugriffsberechtigung zur Erfüllung ihrer Standardaufgaben beschränkt. Der Zugriff auf Kundendaten wird über Zugriffskontroll- und Authentifizierungstools (einschließlich der Verwendung der Zwei-Faktor-Authentifizierung) verwaltet, die von Amazon Web Services und unseren anderen Cloud-Partnern bereitgestellt werden.

Kundendaten werden nur für Zwecke der Erbringung der vertraglich vereinbarten Dienstleistungen, z. B. zur Behebung von Problemen bei technischen Support-Anfragen verwendet. Ausführliche Informationen finden Sie in der Mitti-Datenschutzerklärung hier: https://mitti.com/legal/privacy-policy/

Wenn die Support-Mitarbeiter von Mitti auf bestimmte Kundendaten zugreifen müssen (zur Fehlerbehebung oder zu Support-Zwecken), dann verlangt Mitti immer die Zustimmung des Kunden, bevor er auf diese Daten zugreift.

Wir speichern oder zwischenspeichern keine Finanzdaten von Kunden, die zur Abrechnung über die Mitti-Plattform verwendet werden, und unsere Mitarbeiter haben keinen direkten Zugriff auf Abrechnungsdaten.

Physischer Zugriff auf Daten

Kundendaten werden auf einer Infrastruktur gehostet, die von Amazon Web Services bereitgestellt wird und die Sicherheit ihrer Standorte mithilfe von branchenüblichen Best-Practice-Kontrollen gewährleistet, wie auf ihrer Sicherheits- und Compliance-Website beschrieben: https://aws.amazon.com/architecture/security-identity-compliance/.

In unseren Geschäftsräumen werden keine Kundendaten gespeichert.

Datenverschlüsselung

Mitti verfügt über Mechanismen, die sicherstellen, dass die Daten unserer Kunden jederzeit geschützt sind.

Im Ruhezustand werden alle in den Systemen gespeicherten Kundendaten mit AES-256 verschlüsselt und die Schlüssel über den Key Management Service von Amazon Web Services verwaltet. Alle Daten werden gemäß den Sicherheitsrichtlinien und -verfahren von AWS gespeichert.

Zum Schutz der Daten bei der Übertragung verwendet Mitti Transport Layer Security (TLS) und setzt einen Mindeststandard von TLS v1.2 mit 128-Bit-Chiffrierschlüsseln durch. Wir unterstützen Verbindungen mit bis zu 256-Bit-Chiffre-Schlüsseln für die Verwendung einer AES-Chiffre.

Datensicherungen

Mitti-Daten werden täglich in separaten, verschlüsselten Datenspeicherlösungen von Amazon Web Services gesichert. Die Sicherungen werden auf mehrere AWS-Standorte in der Region des Kunden (APAC, USA oder EU) repliziert.

Der Zugriff auf die Datensicherungen ist nur denjenigen Mitarbeitern von Mitti vorbehalten, für die dieser Zugriff im Rahmen ihrer Rollenanforderungen erforderlich ist. Backups werden verschlüsselt und schreibgeschützt gespeichert.

Löschung und Entsorgung von Daten

Unsere Kundendaten werden gemäß den Lösch- und Entsorgungsverfahren von Amazon Web Services gespeichert und unterliegen diesen. Diese Verfahren umfassen einen Prozess zur Löschung von sicheren alten Medien. Gelöschte Medien werden inspiziert, um die erfolgreiche Vernichtung der Daten sicherzustellen.

Mitti-Hardware, die vertrauliche Daten enthält (einschließlich Mitti-Backups) unterliegt vor dem Recycling einer logischen Datenvernichtung nach branchenüblichen Standards.

Sicherung unserer Produkte

Wir wissen, dass für den Großteil der Kunden ihre Haupterfahrung mit Mitti durch unsere Produkte sein wird. Sicherheit ist ein wichtiger Bestandteil der Entwicklung und des Funktionierens unserer Produkte.

Sichere Software-Entwicklungspraktiken

Als Teil unseres Produktentwicklungsprozesses wird jede Code- und Infrastrukturänderung in einem Versionskontrollsystem gespeichert, versioniert, geprüft und auf ihre Auswirkungen hin untersucht, bevor die Änderung für die Produktion freigegeben wird. Diese Überprüfung umfasst die Einhaltung bewährter Sicherheitsverfahren. Wir trennen auch unsere Entwicklungs-, Test- und Produktionsumgebungen und verwenden auch keine Kundendaten in unseren Nicht-Produktionsumgebungen.

Änderungskontrolle

Alle Änderungen an Mitti-Produkten werden während ihrer Entwicklung aktiv getestet, um sicherzustellen, dass die Auswirkungen auf die Endbenutzer vor dem Einsatz bewertet werden, und alle wesentlichen Änderungen werden in die Produktions-Release-Notes aufgenommen.

Mitti setzt Systeme zur Änderungsverfolgung und Versionskontrolle ein, um Änderungen an der Codebasis oder Konfiguration unserer Produkte aktiv zu überwachen und zu verwalten. Wir verwenden automatisierte Prozesse, um Änderungen in unseren Umgebungen bereitzustellen, und können Änderungen bei Bedarf rückgängig machen. Wir verwenden auch Amazon CloudTrail, um alle zugrunde liegenden Konfigurationsänderungen an der Cloud-Plattform zu verfolgen, auf der unsere Produkte betrieben werden.

Schwachstellenidentifizierung und Patch-Entwicklung

Wir arbeiten intensiv daran, die Anzahl der in unseren Produkten auftretenden Schwachstellen zu minimieren, und wir wissen, dass es wichtig ist, proaktive Schritte zu unternehmen, um sicherzustellen, dass wir alle Schwachstellen so schnell wie möglich beheben. Zu diesem Zweck führt Mitti jährliche Penetrationstests durch und testet und überwacht unsere Anwendungen aktiv auf Schwachstellen. Wir führen ein privates Bug-Bounty-Programm durch, da wir wissen, dass eine Gemeinschaft unabhängiger Sicherheitsforscher, die dazu angeregt werden, unsere Produkte laufend zu testen, um potenzielle Probleme zu identifizieren, dazu beiträgt, die Sicherheit unserer Produkte zu erhöhen.

Wenn eine Schwachstelle identifiziert wird (intern oder extern), wird das Problem nachverfolgt und entsprechend der potenziellen Schwere der Auswirkung auf unsere Kunden priorisiert. Bei Problemen mit kritischem Schweregrad kann dies bedeuten, dass unsere Entwickler rund um die Uhr arbeiten, bis das Problem behoben ist.

Patches für Probleme werden entwickelt und durch einen kontinuierlichen Integrationsprozess (CI/CD) in die Produktionsumgebung freigegeben und so schnell wie möglich angewendet.

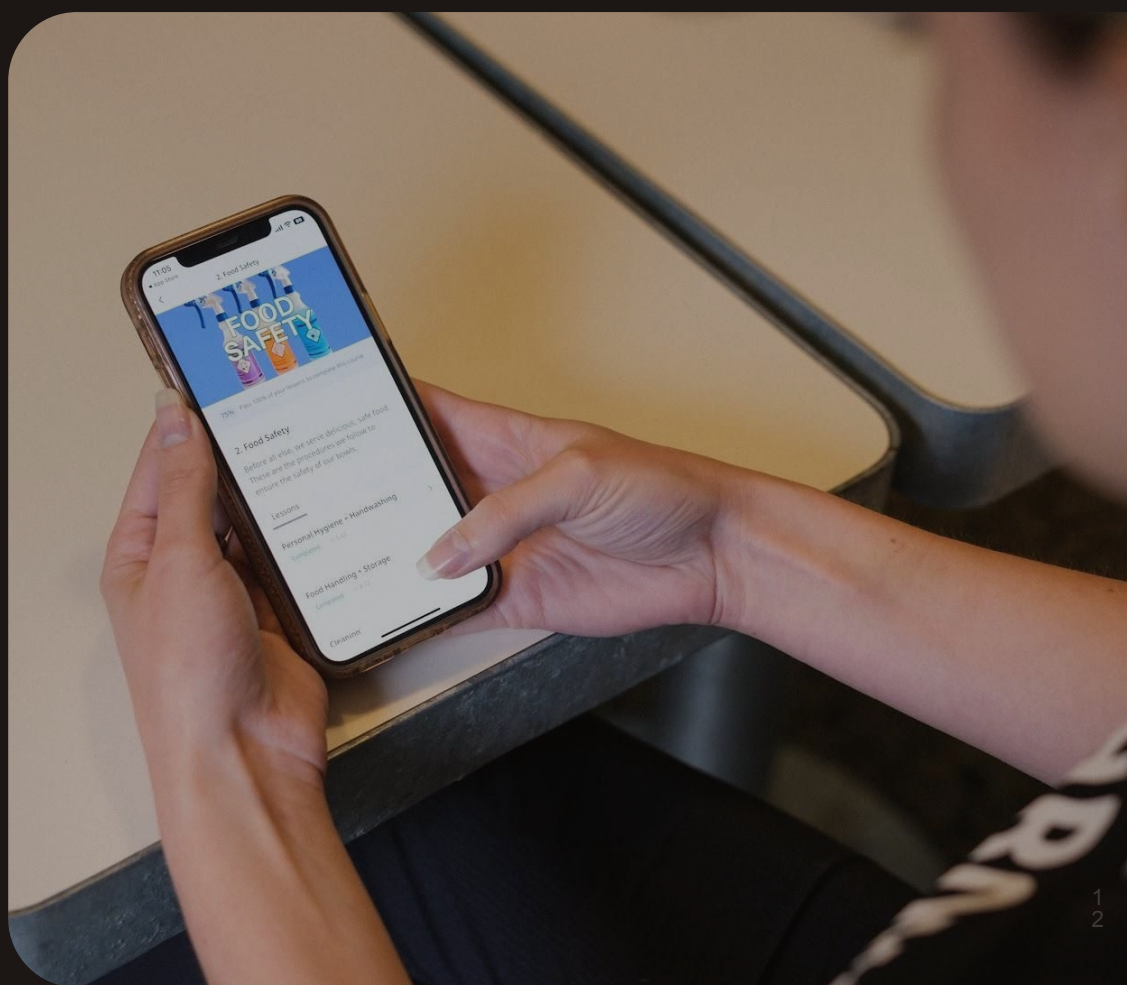
Handhabung von Sicherheitsvorfällen

Während wir unser Möglichstes tun, um Sicherheitsvorfälle zu verhindern, sind wir uns bewusst, dass wir auch darauf vorbereitet sein müssen, mit diesen Vorfällen umzugehen, sollten sie auftreten, um die möglichen Auswirkungen auf unsere Kunden und Mitti zu minimieren.

Wir haben eine Reihe von Maßnahmen ergriffen, darunter:

- Ein dokumentiertes Incident-Management-Verfahren, das unseren Prozess zum Umgang mit der Vertraulichkeit, Integrität und Verfügbarkeit unserer IT-Umgebung und unserer Produkte definiert.
- Die garantierte Unterstützung eines globalen Unternehmens im Falle eines Vorfalls.
- Etablierte Disaster-Recovery-Pläne und Notfallstrategien, die uns dabei helfen können, die Betriebskontinuität während eines Vorfalls aufrechtzuerhalten. Dies umfasst die Verwendung mehrerer geografischer Verfügbarkeitszonen, die von Amazon Web Services bereitgestellt werden, und die Replikation von Daten über mehrere Systeme in jeder Zone. Dies gewährleistet einen kontinuierlichen Datenzugriff bei Vorfällen, die die Systemverfügbarkeit beeinträchtigen, und bietet Datenredundanz im Falle von System- oder Datenspeicherausfällen.

Mitti informiert betroffene Kunden umgehend über schwerwiegende Vorfälle, die die Verfügbarkeit von Mitti-Services oder -Daten beeinträchtigen, sowie über Vorfälle, die die Vertraulichkeit und Integrität ihrer Daten gefährden.



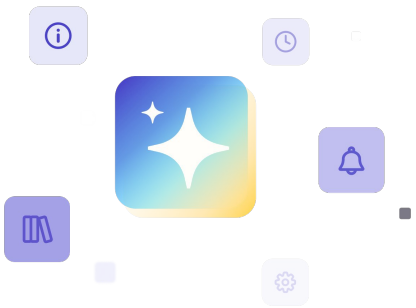
„Wir haben Sichtbarkeit in alles, was wir tun, aufgrund der Daten, die wir mit Mitti erfassen. Wenn es eine Schwellenwertausnahme oder einen Prozess gibt, der verbessert werden muss, müssen wir uns nur die Daten genau anschauen, und wir finden die Ursachen.”

Sofia Dias
Managerin für Lebensmittelsicherheit und Qualitätssicherung

Marley Spoon

Mitti und KI

Mitti innoviert kontinuierlich und bringt unseren Kunden auf sichere Weise neue Funktionen und Technologien. Dazu gehören Funktionen der Künstlichen Intelligenz (KI). Bei Mitti möchten wir gegenüber unseren Kunden transparent sein, wie wir KI zum Aufbau unserer Produkte einsetzen und wie wir KI nutzen, um die Erfahrung unserer Nutzer zu verbessern.



Wie Mitti KI verwendet

KI ermöglicht es Mitti, unsere Funktionsentwicklung zu beschleunigen, manuelle Arbeit zu automatisieren, Werkzeuge zu verbessern und bessere Ergebnisse für Kunden zu erzielen.

Wir nutzen selbst gehostete KI-Infrastruktur und KI-Drittanbieter.

KI-Funktionen in Mitti

Innerhalb von Mitti haben wir KI, die Nutzern helfen kann, Fragen zu ihren Daten zu stellen, Zusammenfassungen zu generieren, Inhalte zu erstellen, zu übersetzen, Erkenntnisse zu gewinnen und Empfehlungen zu erhalten.

KI-Anbieter und Sicherheit

Mitti nutzt Large Language Models (LLMs), die von Mitti und Drittorganisationen wie Anthropic, Google und AWS gehostet werden.

Wir evaluieren kontinuierlich LLM-Anbieter und ihre Modelle, um unseren Nutzern die bestmögliche Erfahrung zu bieten. Drittparteien, die Kundendaten verarbeiten, einschließlich KI-Drittanbieter-Services, sind auf unserer Unterauftragsverarbeiterseite veröffentlicht: https://mitti.com/legal/privacy-sub-processors

Zugang und Steuerung

KI-Funktionen sind berechtigungsbewusst und respektieren bestehende Berechtigungsstrukturen, sodass Nutzer nur auf Inhalte zugreifen, die sie einsehen dürfen. Nur autorisierte Nutzer, wie Administratoren, können Berechtigungen aktualisieren, den Zugriff eines Nutzers auf KI-Funktionen gewähren oder entfernen.

Kundendaten und Trainingsmodelle

Kunden bestimmen, welche Daten an KI-Anbieter weitergegeben werden und wie die Ergebnisse der KI-Verarbeitung genutzt werden.

Mitti erlaubt es Drittanbieter-Services nicht, Kundendaten zum Training der von uns verwendeten Modelle zu nutzen.

Zusätzliche Ressourcen

Mitti ist bestrebt, gegenüber unseren Kunden transparent zu sein, was unsere Produkte betrifft und wie wir KI einsetzen, um die Erfahrung unserer Nutzer zu verbessern. Falls gewünscht, finden Sie hier weitere Ressourcen:

- KI in Mitti
- Datenschutz in Mitti
- Unterauftragsverarbeiter Ihrer D

Abschließende Gedanken

Mitti betrachtet Cybersicherheit als grundlegenden Bestandteil unseres Geschäfts und der Dienstleistungen, die wir Unternehmen auf der ganzen Welt anbieten. Während die von uns eingerichteten Kontrollen und Maßnahmen erheblich über das hinausgehen, was hier behandelt wird, dient der vorliegende Inhalt dazu, ein allgemeines Verständnis für den vielschichtigen Ansatz, den wir verfolgen und unser Engagement für die Sicherheit zu vermitteln.

Wenn Sie Fragen zu diesen Inhalten haben oder weitere Informationen zu unserem Ansatz in Bezug auf Support, Sicherheit oder Datenschutz benötigen, kontaktieren Sie uns bitte unter den nachstehenden Kontaktdaten.

- **Support:** support@mitti.com
- **Datenschutz:** privacy@mitti.com

Um Sicherheitsprobleme zu melden, kontaktieren Sie uns unter security@mitti.com

Weiterführende Informationen

Unsere Sicherheitsseite: https://www.mitti.com/de/sicherheit

Unser Datenschutzportal:
https://www.mitti.com/de/rechtliches/datenschutz-portal

Unsere Service-Statusseite: https://status.mitti.com