CASE STUDY

mondoo

# Campminder reduziert mit Mondoo Fehlkonfigurationen und Schwachstellen um 50%

## Über Campminder

Campminder ist eine webbasierte Softwareplattform, die speziell für Ferienlager entwickelt wurde. Sie ermöglicht die Verwaltung aller Aspekte des Betriebs, einschließlich Online-Anmeldung, Personalverwaltung, Gesundheitsdaten, Kommunikation mit den Eltern, Transportlogistik, Fotos und vieles mehr. Sie bietet im Wesentlichen eine zentrale Anlaufstelle, um die Verwaltung von Ferienlagern zu rationalisieren und effizienter zu gestalten.

**#Standort:** Boulder, USA

**# Mitarbeiter:** 100

**Cloud:** Azure, AWS, Kubernetes

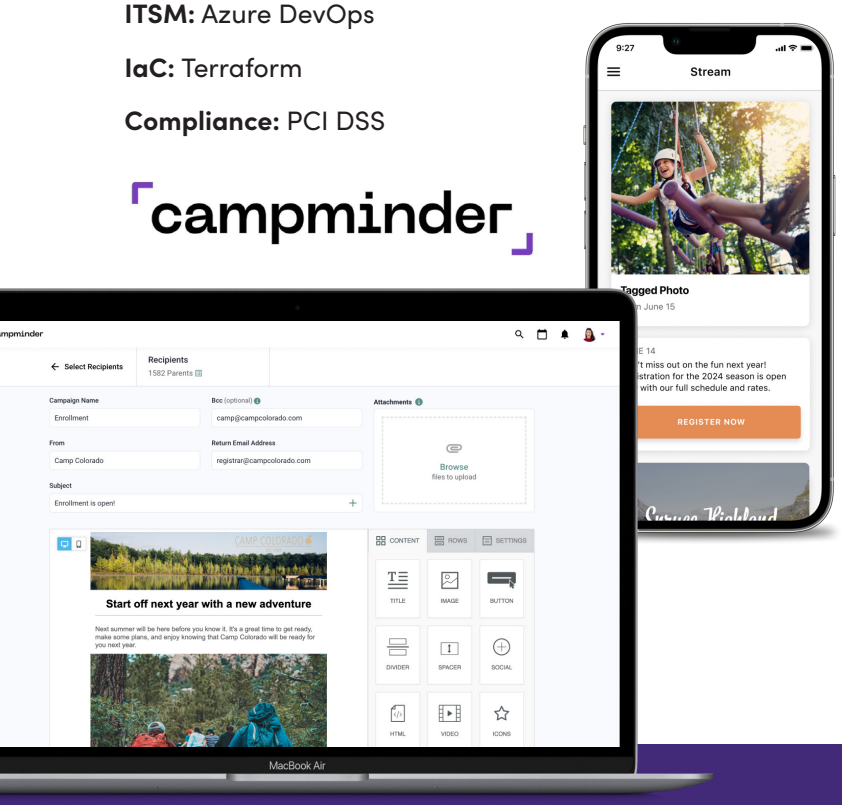
**SaaS:** Okta, Slack, Google Workspace

**ITSM:** Azure DevOps

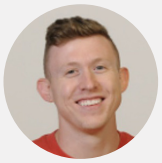
**IaC:** Terraform

**Compliance:** PCI DSS

campminder




> **Wir haben uns verschiedene Anbieter angesehen, und Mondoo hat der Himmel geschickt"**



**Austin Palmer**
Head of Cybersecurity and Compliance

## Mit Mondoos Hilfe erzielte Campminder:

**50%**
weniger Fehlkonfigurationen und Schwachstellen

**< 16 Tage**
Durchschnittszeit bis zur Problemlösung (MTTR)

**4x-5x**
weniger manuelle Arbeit

**$$$$ => $**
Vier Tools weniger und kein Bedarf mehr an Professional Services

## Cloud-first IT Infrastruktur

Campminder nutzt die Cloud für alle Workstations und Server. Es gibt keine lokalen Instanzen und kein internes Netzwerk. Dies erhöht die Flexibilität, Skalierbarkeit und Kosteneffizienz von Campminder und ermöglicht es dem Unternehmen, proaktiver auf Sicherheit zu achten. Campminder nutzt hauptsächlich Azure und teilweise AWS und verwendet zahlreiche SaaS-Tools, darunter Okta, Slack und Google Workspaces.

## Security Herausforderungen

Austin Palmer, Head of Cybersecurity and Compliance, stand vor mehreren Herausforderungen und Lücken in der IT-Security von Campminder:

- **IMPRAKTIKABLES SCHWACHSTELLEN-SCANNING:** Sie benutzten einen teuren Vulnerability-Scanner, der ihnen nur Hunderte von Seiten mit Schwachstellen und wenig nützlichen Informationen lieferte. „Wir brauchten Stunden, um die Berichte durchzugehen, und erhielten nur wenige verwertbare Ergebnisse“, sagt Palmer.

- **KEIN ASSET MANAGEMENT:** Sie hatten keinen Überblick über ihr IT-Inventar, was besonders problematisch war, wenn sie sicherstellen wollten, dass alle Systeme gepatcht waren, und wenn sie auf Zero-Day-Bedrohungen reagieren mussten.

- **KEINE ÜBERPRÜFUNG DER PCI DSS-KONFORMITÄT:** Die Liste der PCI DSS-Anforderungen, die Campminder erfüllen musste, war um das Zehnfache angewachsen. Austin Palmer: “Da es sich um eine viel strengere und umfassendere Bewertung handelte, war uns klar, dass wir ein Tool benötigen würden, um dies zu bewerkstelligen.”

> **Wir haben Unsummen an einen Drittanbieter bezahlt, um unsere Schwachstellen zu scannen und zu überwachen, ohne dass wir einen Nutzen davon hatten.”**
>
> Austin Palmer, Head of Cybersecurity and Compliance

## Tenable und Rapid7 überzeugten nicht

Austin Palmer schaute sich zunächst Tenable und Rapid7 an, um diese Probleme zu lösen. Tenable erzeugte jedoch viele unbrauchbare Warnmeldungen und bot keine Inventar- oder Asset-Verwaltung. Rapid7 schnitt zwar besser ab, aber das Hauptproblem war, dass sowohl Tenable als auch Rapid7 stark von der Installation von Agenten abhängig sind, was steigende Kosten für die Rechenleistung bedeutet und die Leistung verringert. Dann lernte Austin Palmer Mondoo kennen.

> **Einer der Hauptgründe, warum wir uns gegen Tenable, Rapid7 und andere Tools dieser Art entschieden haben, ist, dass sie stark von Agenten abhängig sind. Doch je weniger Agenten ich auf meinen Boxen habe, desto besser.”**
>
> Austin Palmer, Head of Cybersecurity and Compliance

## Die Lösung: Mondoo

“Mondoo hat der Himmel geschickt,” sagt Palmer. “Wir waren sofort beeindruckt von der Demo und der Tatsache, dass wir die Scanergebnisse in einer leicht verständlichen und umsetzbaren Form sehen konnten. Mondoo hat uns auch dabei geholfen, unser altes ASV-Scantool zu ersetzen, was eine weitere Funktion war, die wir gesucht haben”.

**Mit Mondoo erhält Campminder jetzt:**

- **Umsetzbare Erkenntnisse:** Klare und nach Prioritäten geordnete Einblicke in ihre Schwachstellen und Fehlkonfigurationen.
- **Asset Management:** Ein vollständiges Inventar aller IT-Assets und eine einfache Suchmöglichkeit.
- **Compliance:** Kontinuierliches und vollautomatisches Scannen zur Einhaltung des PCI DSS.
- **Geführte Korrekturmaßnahmen:** Die Möglichkeit, Probleme mit allen relevanten Informationen und Behebungsschritten zuzuordnen, wodurch sich die Behebungszeiten erheblich verkürzen.

- **ASV Scanning:** Externes Vulnerability Scanning durch einen Drittanbieter, der Mondoo verwendet.
- **Optimierte Security:** Verstehen, wie man mit Hilfe von Impact Scoring und Blast Radius die größten Verbesserungen in der Security Posture mit dem geringsten Aufwand erreichen kann.

> **Mondoo hat uns bei der Erfüllung unserer PCI DSS-Anforderungen wahnsinnig geholfen”**
>
> Austin Palmer, Head of Cybersecurity and Compliance

## Umsetzung

Der Einsatz von Mondoo war überraschend einfach. Austin Palmer sagt: “Es ist großartig, dass Mondoo nicht für jedes einzelne Asset einen Agenten benötigt. So konnten wir Mondoo umgehend mit unserer Umgebung verbinden und mit dem Scannen loszulegen.”

Als Campminder kürzlich eine andere Applikation für Camp-Management akquirierte, war es ein Leichtes, Mondoo auch mit der neuen Umgebung zu verbinden und mit dem Scannen nach Schwachstellen und Fehlkonfigurationen zu beginnen. Das bedeutete, dass sie die App sehr schnell und sicher in Betrieb nehmen konnten und die Zeit bis zur Wertschöpfung ihrer Akquirierung erheblich verkürzt wurde.

Die Möglichkeit, Assets in Arbeitsbereichen innerhalb von Mondoo zu organisieren, war für Campminder ebenfalls sehr nützlich. Austin Palmer: “Wir konnten einen separaten Arbeitsbereich für die neue App einrichten. Da es sich um eine völlig andere IT-Infrastruktur mit ausschließlich On-Prem-Servern und Workstations handelte, war es äußerst hilfreich, die Assets getrennt von unseren Cloud-Assets sehen zu können.

## Ergebnisse

Mit Hilfe der Mondoo-Plattform hat Campminder die folgenden Ergebnisse erzielt:

- **Reduzierung der Fehlkonfigurationen und Schwachstellen um 50 %**
- **Die mit Abstand meisten Risiken werden nun in weniger als 16 Tagen behoben.**
- **Reduzierung des manuellen Aufwands um das Vier- bis Fünffache (da keine langen Schwachstellenberichte mehr gesichtet werden müssen, optimierte Zuweisung von Korrekturmaßnahmen, automatische Konformitätsprüfungen).**
- **Die Anschaffung separater Tools für Asset Management, Schwachstellenmanagement, PCI-Compliance und ASV-Scans wurde vermieden.**

## Fazit

„Ein Tool wie Mondoo ist unglaublich hilfreich, vor allem für kleine IT-Teams, die mehrere Aufgaben zu erledigen haben“, sagt Austin Palmer. “Ich habe in früheren Unternehmen Tools wie Rapid7 verwendet, aber sie waren nicht benutzerfreundlich und es war mühsam, Schwachstellen im gesamten Unternehmen aufzuspüren, da es keine einfache Möglichkeit gab, nach Assets und Maschinen zu suchen.

Das Tolle an Mondoo ist auch, dass wir mit ihnen gemeinsam an neuen Funktionen arbeiten können, die wir uns wünschen. Sie sind immer sehr hilfsbereit und nehmen sich unser Feedback zu Herzen. Ich würde Mondoo auf jeden Fall Unternehmen empfehlen, die manuelle Arbeit einsparen und ihre Security optimieren wollen”.

**Erfahren Sie mehr über die Vorteile von Mondoo.**

mondoo.com