DAS UNTERNEHMEN – ÜBERSICHT

Warum sich Kunden für Thycotic entscheiden

Geben Sie Angreifern keine Chance. Seien Sie stets bereit für Audits. Schützen Sie Ihr wichtigstes Kapital.

Thycotic unterstützt mehr als 10.000 Unternehmen – von kleinen Firmen bis hin zu Fortune 500-Unternehmen – mit seinen Lösungen für Privileged Access Management. Wir machen Privilege Management auf Unternehmensebene für alle zugänglich: komplexe Sicherheitstools gehören der Vergangenheit an und Produktivität, Flexibilität und Kontrolle rücken in den Vordergrund. Mit Thycotic erreichen Sie mehr als mit jedem anderen PAM-Sicherheitstool.

> 10.000
KUNDEN WELTWEIT

95%
KUNDEN-ZUFRIEDENHEIT

97%
KUNDEN-BINDUNG

Sparen Sie wertvolle Zeit und Energie

Thycotic bietet Ihnen die Agilität, immer einen Schritt voraus zu sein. Verabschieden Sie sich von einer manuellen Bereitstellung oder mühsamem Passwortmanagement und erstellen Sie Berichte ohne mühsames Durchsuchen von Auditprotokollen. So können Sie Fragen von der Geschäftsleitung oder von Auditoren beantworten, noch bevor sie gestellt werden.

Mit Thycotic haben Sie Ihre Mitarbeiter auf Ihrer Seite

Unsere Lösungen erfreuen sich großer Beliebtheit bei Sicherheitsteams, IT-Betreibern, Systemadministratoren, Helpdesk-/Support-Teams, Entwicklern und allen Mitarbeitern, die privilegierte Konten für ihre Arbeit brauchen.

Warum sollte Privileged Access Management im Hinblick auf Cybersicherheit oberste Priorität haben?

Die Zugangsdaten der privilegierten Konten von Domänenadmins, Service- , Anwendungs- und Root-Accounts zählen zu den beliebtesten Angriffszielen von Hackern.
Wenn es Angreifern gelingt, diese Zugangsdaten zu kapern, stehen ihnen Tür und Tor zu den sensibelsten Unternehmensdaten und kritischsten Systemen offen.
Mit den Zugriffsrechten können sie Daten manipulieren, Konfigurationen ändern oder sogar Ihren ganzen Betrieb lahmlegen. Getarnt als privilegierte Nutzer können sie ihre Spuren verwischen und monatelang oder noch länger unentdeckt ihr Unwesen treiben.

GARTNER INSIGHTS

PAM sollte bei IT-Sicherheitsteams oberste Priorität haben

FORRESTER

PAM kann das Risiko von Angriffen um 80 % senken

GARTNER BEST PRACTICES FÜR PAM

PAM senkt das Risiko ausgeklügelter Angriffe um 50 %

thycotic

SECRET SERVER

Sicherheit für privilegierten Konten und Passwortschutz.

Secure Vault einrichten – Legen Sie granulare Zugriffsrechte, Benutzer und Strukturen entsprechend Ihrer Organisation fest.

Privilegien ermitteln – Identifizieren Sie alle Service-, Anwendungs-, Administrator- und Root-Accounts, um eine Vergabe von zu hohen Berechtigungen zu vermeiden.

Secrets verwalten – Sie können Zugriffsrechte zuweisen und entziehen, eine hohe Passwortsicherheit gewährleisten und Zugangsdaten regelmäßig ändern.

Zugriff delegieren – Richten Sie eine rollenbasierte Zugriffskontrolle, Workflows für Zugriffsanforderungen und Genehmigungen für Dritte ein.

Sitzungsüberwachung – Nutzen Sie die Möglichkeit, Sitzungen zu starten, verwenden Sie Proxies und zeichnen Sie Sitzungen zu Überwachungszwecken auf.

Unix schützen – Erstellen Sie Whitelists für UNIX-Befehle und die Verwaltung von SSH-Keys.

PRIVILEGE MANAGER

Erhöhung der Berechtigungsstufe von Endgeräten und Anwendungskontrolle

Einsatz von Agenten – Finden Sie Endgeräte, Anwendungen und Prozesse auf Konten in und außerhalb der Domäne.

Restriktive Rechtevergabe – Entfernen Sie überflüssige Berechtigungen, Mitgliedschaften in Kontrollgruppen und Zugangsdaten.

Festlegung von Richtlinien – Erstellen Sie granulare Richtlinien für das Whitelisting, Blacklistung und Graylisting von Anwendungen.

Anwendungen hochstufen – Vergeben Sie mithilfe richtlinienbasierter Kontrollen Berechtigungen für Anwendungen, die Administratorrechte für die Ausführung erfordern.

Produktivität steigern – Ermöglichen Sie Mitarbeitern, Anwendungen und Kontrollen auch ohne Adminrechte zu nutzen.

CONNECTION MANAGER

Einheitliches Management von mehreren Remote-Sitzungen.

Remote Access – Starten und konfigurieren Sie Sitzungen in unterschiedlichen Umgebungen.

Sitzungsmanagement – Die Zugangsdaten werden bei Bedarf automatisch in den Sitzungen eingegeben.

Zentrale Steuerung – Das Management der Sitzungen erfolgt über eine zentrale Benutzeroberfläche.

Aufzeichnung von Sitzungen – Erstellen Sie eine lückenlose Aufzeichnung der Aktivitäten von privilegierten Nutzern.

Tracking und Auditing – Erstellen Sie einen Auditbericht zur Einhaltung von Compliance-Anforderungen.

ACCOUNT LIFECYCLE MANAGER

Vermeiden Sie eine unkontrollierte Ausbreitung von Servicekonten.

Workflow erstellen – Einfacher Einstieg mit wenigen Schritten und individueller Anpassung mithilfe von Workflow-Vorlagen.

Verantwortlichkeiten delegieren – Erstellen Sie nach Bedarf Benutzer, Gruppen und Rollen mit rollenbasierten Berechtigungen.

Servicekonten bereitstellen – Definieren Sie Workflow(s) für die automatische Bereitstellung von Konten und legen Sie die erforderlichen Genehmigungen für jede Anforderungsart fest.

Konsequente Governance – Legen Sie die Zuständigkeiten und Verantwortlichkeiten für Ihre Servicekonten fest.

Servicekonten deaktivieren – Versenden Sie automatische Benachrichtigungen, wenn Konten erneuert, neu genehmigt oder gelöscht werden sollen.

PRIVILEGED BEHAVIOR ANALYTICS

Vorausschauende Vermeidung von Sicherheitslücken und Vorbeugung vor Datendiebstahl.

Grundmuster feststellen – Analysieren Sie typische Verhaltensmuster bei privilegierten Konten, um Warnzeichen zu erkennen.

Überwachen und erkennen – Überwachen Sie privilegierte Konten und stellen Sie Aktivitäten in individuellen Dashboards priorisiert dar.

Erkennen und Warnen – Erkennen und verifizieren Sie verdächtige Aktivitäten und geben Sie eine Warnmeldung an das Notfallteam aus.

Handeln – Ändern Sie Zugangsdaten in regelmäßigen Abständen, setzen Sie eine MFA durch oder verwenden Sie Genehmigungen, um die Auswirkungen eines Angriffs einzugrenzen.

DEVOPS SECRETS VAULT

Schutz Ihrer Passwörter in der Cloud mit höchster Geschwindigkeit und Skalierbarkeit.

Einrichten eines Secure Vaults – Speichern Sie privilegierte Zugangsdaten in einem verschlüsselten, zentralen Vault.

Zentralisieren der Secrets – Minimieren Sie das Risiko von mehreren separaten Vaults.

Zugriffe verwalten – Stellen Sie eine revisionssichere Verwaltung und Durchsetzung aller privilegierten Zugriffe sicher.

Verknüpfen aller Tools – Profitieren Sie von höchster Flexibilität dank einer plattformunabhängigen Lösung mit Integration von DevOps und Tools für die robotergestützte Prozessautomatisierung (RPA).

Automatische Skalierung – Verwalten Sie Secrets mit der Geschwindigkeit und Skalierung von DevOps- und RPA-Lösungen.

Der Schwerpunkt bei Thycotic liegt auf dem größten Angriffspunkt – den Berechtigungen. Thycotic verfolgt einen mehrschichtigen Sicherheitsansatz, mit dem Sie Ihre privilegierten Konten durchgängig vor Angreifern schützen können – vom Endgerät bis hin zu den Berechtigungen.

thycotic.com | sales@thycotic.com