FORTINET / FIREMON

EXCLUSIVE NETWORKS

PARTNER-PLAYBOOK

Ihr Leitfaden, um den Markt zu erobern und das volle Potenzial Ihrer FireMon-Partnerschaft auszuschöpfen

SECURE SMARTER.

WILLKOMMEN BEI FIREMON

Secure Smarter
Verbesserte Sichtbarkeit, Verwaltung und Automatisierung von Sicherheitsrichtlinien vom Rechenzentrum bis zur Cloud.

Dieses Playbook ist Ihr Leitfaden, um die enormen Marktchancen von FireMon auszuschöpfen. Unser Ziel ist es, Sie bei „Secure Smarter" zu unterstützen, indem wir die Herausforderungen Ihrer Kunden lösen, neue Umsätze generieren und das Geschäftsvolumen steigern.

FireMon kennenlernen:

FireMon hat die Verwaltung von Firewall-Richtlinien im Jahr

2001

erfunden und ist mit über

1.800

Kunden in

70

Ländern ein innovativer Marktführer.

Firewall-Wildwuchs

Im Laufe der Zeit sammelt jedes Unternehmen Regelwerke an, ein verworrenes Geflecht aus redundanten, verdeckten und übermäßig permissiven Vorgaben. FireMon hilft Ihnen, diese Altlasten in den Fortinet- und Multi-Vendor-Umgebungen Ihrer Kunden zu beseitigen, die Angriffsfläche zu verringern und die Effizienz der Sicherheitsteams erheblich zu steigern.

Geben Sie Ihren Kunden ihre beste Waffe: Zeit

Sicherheitsteams stehen unter enormen Druck. FireMon automatisiert die mühsamen manuellen Aufgaben wie Compliance-Prüfungen und Regeländerungen und verschafft Ihrem Team die Freiheit, sich auf die Bekämpfung echter Bedrohungen zu konzentrieren. Der wahre Wert von FireMon liegt nicht nur in der Automatisierung, sondern auch in der Multiplikation der Effektivität, die es einem kleinen Team ermöglicht, eine große Umgebung sicher zu verwalten. Anstatt sich wochenlang auf ein Audit vorzubereiten oder tagelang für eine einzige Regeländerung zu benötigen, erledigen Teams diese Aufgaben nun in wenigen Minuten und können sich auf strategische Initiativen wie die Eindämmung von Angriffsflächen konzentrieren.

01

PRODUKTÜBERSICHT

FireMon Security Manager
Der Sicherheitsmanager von FireMon ist eine skalierbare Sicherheitsmanagement-Plattform in Echtzeit, die einheitliche Transparenz, Kontrolle und Compliance in hybriden Cloud- und On-Premises-Umgebungen bietet. Er ermöglicht Unternehmen, Risiken kontinuierlich zu bewerten, Richtlinien durchzusetzen und Änderungen auch in hochkomplexen Netzwerkinfrastrukturen effizient zu steuern.

ÜBERBLICK ÜBER DIE ZENTRALEN MODULE

01 Continuous Compliance

Kontinuierliche Compliance stellt sicher, dass die Konfigurationen von Firewalls und Netzwerkgeräten mit internen Richtlinien und externen regulatorischen Vorgaben übereinstimmen. Das Modul führt automatische Bewertungen durch und liefert Warnungen in Echtzeit, damit die Teams jederzeit auf Prüfungen vorbereitet sind und das Non-Compliance-Risiko verringern können.

ZENTRALE FUNKTIONEN:

- Führt automatische Compliance-Prüfungen nach gängigen Standards wie PCI-DSS, NIST und ISO durch.
- Erstellt anpassbare Prüfberichte und Dashboards für interne und externe Stakeholder.
- Warnt Teams in Echtzeit bei Verstößen und Konfigurationsabweichungen und ermöglicht so eine schnelle Korrekturmaßnahme.

Kundennutzen: Mit kontinuierlicher Compliance verkürzen Unternehmen die Vorbereitungszeit auf Audits, behalten regulatorische Vorgaben im Blick und erkennen Fehlkonfigurationen proaktiv, bevor sie zu Sicherheitsvorfällen führen.

02 Real-Time Change Monitoring

Die Änderungsüberwachung in Echtzeit verfolgt jede Konfigurationsänderung auf allen Netzwerksicherheitsgeräten und bietet vollständige Transparenz darüber, wer welche Änderungen wann vorgenommen hat. So schafft es die Grundlage zur Normalisierung von Geräteregeln und zur Vermeidung von unbefugten oder riskanten Änderungen.

ZENTRALE FUNKTIONEN:

- Erfasst und protokolliert alle Regel- und Konfigurationsänderungen an Firewalls, Routern und Cloud-Sicherheitskontrollen.
- Visualisiert Änderungsverläufe mit detaillierten Metadaten für forensische Analysen und operative Transparenz.
- Unterstützt Rollback- und Korrektur-Workflows, um Fehlkonfigurationen schnell zu beheben.

Kundennutzen: Mit der Änderungsüberwachung in Echtzeit behalten Sicherheitsteams jederzeit die Kontrolle über dynamische Umgebungen, minimieren operative Risiken und stellen Verantwortlichkeit in den Änderungsprozessen sicher.

01

PRODUKTÜBERSICHT

FireMon Security Manager
Der Sicherheitsmanager von FireMon ist eine skalierbare Sicherheitsmanagement-Plattform in Echtzeit, die einheitliche Transparenz, Kontrolle und Compliance in hybriden Cloud- und On-Premises-Umgebungen bietet. Er ermöglicht Unternehmen, Risiken kontinuierlich zu bewerten, Richtlinien durchzusetzen und Änderungen auch in hochkomplexen Netzwerkinfrastrukturen effizient zu steuern.

03 Rule Lifecycle Management

Regel-Lebenszyklus-Management unterstützt Unternehmen dabei, klare, effiziente und sichere Regelwerke aufrechtzuerhalten, indem unnötige Zugriffe erkannt und entfernt werden. Das Modul fördert die kontinuierliche Überprüfung der Regeln, Optimierung und das kontrollierte Abschalten veralteter Regeln.

ZENTRALE FUNKTIONEN:

- Analysiert die Regelnutzung, um nicht verwendete, zu weit gefasste oder redundante Regeln zu identifizieren.
- Automatisiert Regel-Prüfprozesse und unterstützt Richtlinien-Bereinigungsinitiativen.
- Integriert sich nahtlos in Change-Management-Systeme, um Governance während des gesamten Regel-Lebenszyklus sicherzustellen.

Kundennutzen: Mit Rule Lifecycle Management reduzieren Kunden die Komplexität von Richtlinien, verbessern die Geräteleistung und minimieren Risiken, die durch unnötige Zugriffsberechtigungen entstehen.

02

PRODUKTÜBERSICHT

FireMon Policy Manager
Der Policy Manager von FireMon ist eine Plattform für die Verwaltung von Netzwerksicherheitsrichtlinien (Network Security Policy Management, NSPM). Er bietet granulare Echtzeit-Transparenz für alle Sicherheitsrichtlinien und sorgt für kontinuierliche Compliance und automatisierte Änderungsprozesse in der gesamten hybriden IT-Landschaft eines Unternehmens.

ÜBERBLICK ÜBER DIE ZENTRALEN MODULE

01 Policy Optimizer

Der Richtlinien-Optimierer bietet eine tiefgehende Echtzeit-Sichtbarkeit des Zustands und der Komplexität bestehender Firewall-Richtlinien. Sein Hauptzweck besteht darin, Ineffizienzen im gesamten Regelwerk zu analysieren und aufzuzeigen, die das Risiko erhöhen und die Leistung beeinträchtigen. Das Modul ist für die Bereinigung und Hygiene von Richtlinien unerlässlich, insbesondere vor einer Migration oder im Rahmen der regelmäßigen Wartung.

ZENTRALE FUNKTIONEN:

- Erkennt technische Fehler in Richtlinien, darunter nicht verwendete, redundante, verdeckte und zu weit gefasste Regeln und Objekte.
- Bietet visuelle Dashboards, die die Richtlinienkomplexität, Regelverwendung und nicht referenzierte Netzwerk- oder Serviceobjekte darstellen.
- Unterstützt Kunden bei der Bereinigung veralteter Regelwerke mit Erkenntnissen, dass über 40 % der alten Richtlinien überflüssig sind und nicht migriert werden müssen.

Kundennutzen: Mit dem Richtlinien-Optimierer können Kunden ihre Angriffsfläche erheblich reduzieren, die Firewall-Leistung optimieren, Risiken verringern und Migrationen auf neue Plattformen wie Fortinet schneller, sauberer und kosteneffizienter durchführen.

02 Policy Planner

Der Richtlinienplaner konzentriert sich auf die Automatisierung und Validierung des Firewall-Änderungsmanagementprozesses. So können Sicherheitsteams neue Regeln und Richtlinienänderungen intelligent entwerfen, bewerten und umsetzen sowie sicherstellen, dass keine neuen Risiken oder Compliance-Verstöße eingeführt werden.

ZENTRALE FUNKTIONEN:

- Automatisiert den gesamten Workflow für Regeländerungen, von der ersten Anfrage bis zur Implementierung.
- Führt vor einer Änderung eine Auswirkungsanalyse durch, um eine vorgeschlagene Änderung auf Sicherheitsrisiken und Compliance-Verstöße zu prüfen, bevor sie eingeführt wird.
- Integriert sich nahtlos in IT-Service-Management-Systeme (ITSM), um den Änderungsprozesses innerhalb bestehender operativer Arbeitsabläufe zu beschleunigen.

Kundennutzen: Mit dem Richtlinienplaner werden Änderungsprozesse beschleunigt, die Bearbeitungszeit für Regeländerungen um bis zu 90 % reduziert und riskante Fehlkonfigurationen verhindert. So ist gewährleistet, dass jede Änderung den standardisierten Sicherheitsrichtlinien und Compliance-Vorgaben entspricht.

DIE GEMEINSAME LÖSUNG MIT FORTINET

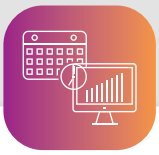
Wo FortiManager aufhört, fängt FireMon an.
FireMon verleiht dem FortiManager echte Superkräfte. Mit FireMon erhalten Kunden zusätzliche Informationen, Transparenz und Verwaltungskompetenz, die sie benötigen, um Firewall- und L2-L3-Sicherheitsrichtlinien über ihr gesamtes hybrides Unternehmensnetzwerk hinweg effektiv zu managen. Während FortiManager sich hervorragend für die Verwaltung von FortiGate-Geräten eignet, erweitert FireMon die Möglichkeiten deutlich: Es bietet eine zentrale Plattform für eine einheitliche Firewall-/Sicherheitsrichtlinien- und Regeltransparenz, Echtzeit-Compliance und intelligente Automatisierung über alle Hersteller hinweg, einschließlich Fortinet, Cisco, Palo Alto und führender Cloud-Anbieter.

HAUPTVORTEILE

Vereinheitlichte Multi-Vendor-Transparenz: Ein zentrales Dashboard für alle Richtlinien und Regeln, einschließlich Fortinet- und Nicht-Fortinet-Geräte.

Automatisierte Compliance und Governance: Erstellen Sie Audit-Berichte 9-mal schneller mit sofortiger Unterstützung für PCI, NIST, HIPAA und mehr.

Intelligente Änderungsautomatisierung: Reduzieren Sie die Bearbeitungszeit für Regeländerungen um bis zu 90 % und verhindern Sie riskante Fehlkonfigurationen, bevor sie eingeführt werden.



Einfachere, sorgenfreie Migrationen: Beschleunigen Sie Firewall-Migrationen-Regeln zu Fortinet um das Neunfache durch Bereinigung und Optimierung veralteter Regelwerke vor der Migration. So wird der Umfang unnötiger Firewall-Regeln um ca. 40 % reduziert, während der ROI der Migration steigt.

DER WETTBEWERBSVORTEIL VON FIREMON: ECHTZEIT-TRANSPARENZ UND LEISTUNGSSTARKE ANALYSEN

Die FireMon-Plattform ist so konzipiert, dass sie sofort verfügbare, detaillierte und umsetzbare Informationen liefert, die die Mitbewerber nicht bieten können. Dies ist keine zusätzliche Funktion, sondern ein grundlegender Designunterschied, der einen erheblichen Wettbewerbsvorsprung schafft.

Echtzeitdaten und -warnungen: FireMon erkennt und meldet Richtlinienverstöße und Konfigurationsänderungen sofort. Dieser proaktive Ansatz steht in scharfem Kontrast zu Mitbewerbern wie Tufin, das ein reaktives Modell verwendet und Verstöße erst nach der Implementierung kennzeichnet, oder AlgoSec, das auf eine Polling-basierte Datenerfassung setzt, deren Informationen Stunden bis Tage alt sein kann.

Leistungsstarke Suche mit SIQL: Mit der Security Intelligence Query Language (SIQL) bietet FireMon flexible Echtzeit-Suchfunktionen für die gesamte Plattform. So können Anwender benutzerdefinierte Abfragen, Berichte und Dashboards erstellen und erhalten sofort tiefgehende Einblicke.

Vollständig anpassbare Berichte: FireMon bietet über 500 integrierte Kontrollprüfungen und ermöglicht vollständig anpassbare Berichte, Analysen und Dashboards.

FIREMON ICP GTM: FOKUS AUF UNTERNEHMEN

Der ideale Kunde ist das Ziel: „ICP – Ideales Kundenprofil"

Das ideale Kundenprofil hat einen Umsatz von über 1 Mrd. £, mehr als 1.000 Mitarbeitende, mehr als zwei Firewall-Anbieter und eine hybride Umgebung. Die Kunden können aus allen Branche stammen. Die wichtigsten Branchen wie Finanzdienstleistungen, Gesundheitswesen, Einzelhandel und Produktion haben in der Regel Compliance- und gesetzliche Anforderungen.

01 Zielgruppen und Buyer Personas:

Unternehmen
- Umsatz von über 1 Mrd. £ ist ideal
- Mehr als 1.000 Mitarbeitende
- Mehr als 2 Firewall-Anbieter im Einsatz
- Betreibt eine hybride Unternehmensumgebung (vor Ort, Edge, SD-Wan, SASE) und Cloud-Umgebungen
- Unterliegt externen oder internen regulatorischen Anforderungen

Top-Branchen
- Finanzdienstleistungen
- Gesundheitswesen
- Einzelhandel
- Fertigung
- Versicherungen
- Telco
- Versorgungsunternehmen
- Unternehmen im Bereich M&A

Buyer Personas
- **Wirtschaftliche Entscheider:** VP - Netzwerk, Sicherheit, Infrastruktur; CISO/CIO
- **Technische Entscheider:** Netzwerk-/Cloud-Architekten, Netzwerkadministratoren, Sicherheitsarchitekten, Sicherheitsanalysten, SOC-Teams
- **Audit-/Compliance-Verantwortliche:** Risiko-/Compliance-Manager

Auf einen Blick:

Wen ansprechen: Unternehmen mit über 1 Mrd. £ Umsatz, mehr als 1.000 Mitarbeitenden und einer unübersichtlichen Mischung verschiedener Firewalls. Je mehr Mitarbeitende, desto mehr Firewalls.

Wo gewinnen: In Finanzwesen, Gesundheitswesen, Einzelhandel, Produktion – überall dort, wo Compliance entscheidend ist und Komplexität zur Schwachstelle wird.

Mit wem sprechen: Mit dem VP für Infrastruktur, der nachts kein Auge zubekommt, dem Sicherheitsarchitekten, der in Support-Tickets untergeht, und dem CISO/CIO, der dem Vorstand Bericht erstatten muss.

IM EINKLANG MIT MARKTTRENDS

01 Der Aufstieg der Zero-Trust-Architektur

Fortinet liefert die Zero-Trust-Durchsetzungspunkte über FortiGate. FireMon stellt die zentrale Transparenz und das Sicherheitsrichtlinienmanagement bereit, um zu gewährleisten, dass die Zero-Trust-Strategie Ihrer Kunden wirklich greift. Das Netzwerksicherheitsrichtlinienmanagement (Network Security Policy Management, NSPM) bildet dabei das Rückgrat einer Zero-Trust-Strategie, da es die erreichbare Angriffsfläche reduziert. Sicherheitskontrollen sind nur so stark wie ihre Richtlinien. Schlechte Richtlinien = Technologieversagen. Eine granulare Sichtbarkeit und Verwaltung der Sicherheitsrichtlinien ist unerlässlich, um die Richtlinienhygiene zu gewährleisten, unbekannte Fehlkonfigurationen oder Schwachstellen zu beheben, die Gefährdung zu kontrollieren, Ihre Vermögenswerte zu schützen und Sicherheitskontrollen und Compliance im gesamten Netzwerk durchzusetzen, nicht nur in der Fortinet-Infrastruktur.

02 FireMon als „Fabric Extender" für Multi-Vendor-Umgebungen:

Was passiert, wenn ein Kunde zusätzlich zu seiner Fortinet-Lösung auch Cisco, Palo Alto und AWS einsetzt? FireMon validiert und erweitert die Leistungsfähigkeit der Fortinet Security Fabric auf Ihr gesamtes Multi-Vendor-Unternehmensnetzwerk. FireMon ist das entscheidende Bindeglied, das sicherstellt, dass die Prinzipien der Transparenz und Automatisierung der Fabric für jede Firewall, Netzwerksicherheitsrichtlinie und Cloud-Richtlinie gelten, unabhängig vom Anbieter. Dadurch wird die allgemeine Sicherheitslage Ihrer Kunden gestärkt und der tägliche Betrieb vereinfacht.

03 KI-gesteuerte Sicherheitsoperationen (AI-Ops)

„Secure Smarter" ist nicht nur ein Slogan. Mit der neuen KI-gestützten FireMon Insights Analytics Platform können Sie Ihre Fortinet-Sicherheitslage im Branchenvergleich messen, Risiken proaktiv erkennen und komplexe Firewall- und Sicherheitsrichtlinienaufgaben per natürlicher Sprache steuern. So wird Ihr Sicherheitsteam zu einem effizienteren, datengesteuerten Betrieb, während es den Geschäftsinhabern ermöglicht, die KPIs Ihres Sicherheitsteams mit tatsächlichen Ergebnissen nachzuvollziehen.

Mit der Verschmelzung von IT- und OT-Netzwerken wird es immer wichtiger, getrennte, aber konforme Sicherheitsrichtlinien aufrechtzuerhalten. FireMon bietet dafür eine zentrale Management-Oberfläche für beide Welten und erweitert den Schutz der Fortinet Security Fabric tief hinein in Ihre industriellen Steuerungssysteme.

04 Risikofreie Einführung von SD-WAN- und SASE:

Plant Ihr Kunde einen Umstieg auf Fortinet Secure SD-WAN? FireMon stellt sicher, dass die neuen Sicherheitsrichtlinien Ihrer Kunden vom ersten Tag an sauber, konform und optimiert sind. FireMon hilft Ihrem Kunden, alte Regelwerke zu analysieren und zu bereinigen, die Migration relevanter Richtlinien zu automatisieren und eine kontinuierliche Compliance in seiner neuen, agilen Netzwerkarchitektur sicherzustellen.

WARUM EINE PARTNERSCHAFT MIT FIREMON?

Eine Partnerschaft, die auf Ihr Wachstum ausgelegt ist.
Bei FireMon sind die Partner nicht ein Teil des Geschäfts, sondern sind das Geschäft. Die Zusammenarbeit mit FireMon verschafft Partnern eine leistungsstarke, differenzierte Lösung, mit der sie die komplexesten Sicherheitsprobleme ihrer Kunden lösen können. Dies schafft erhebliche finanzielle Möglichkeiten und stärkt Ihre Position als vertrauenswürdiger Berater.

Das haben Sie davon:

Ein direkter Weg zu Rentabilität und planbaren Einnahmen
FireMon hat ein Geschäftsmodell entwickelt, das Partner vom ersten Tag an profitabel und erfolgreich macht.

100% Channel-orientiertes Unternehmen:

FireMon engagiert sich voll für seine Partner. FireMon verkauft nicht direkt, das bedeutet keine Channel-Konflikte und das gesamte Geschäft wird über unsere geschätzten Partner abgewickelt.

Hohe Margen und wiederkehrende Umsätze:

Die Partnerschaften basieren auf mehrjährigen Lizenz- und ARR-Modellen (Annual Recurring Revenue) mit hohen Margen. So entsteht eine vorhersehbare, langfristige und profitable Einnahmequelle für Ihr Unternehmen.

Attraktive SPIFFs und Anreize:

FireMon investiert in Vertriebs- und Technikteams. Mit den FireMon Prämienprogrammen Sales Performance Incentive Funds (SPIFFs) werden Vertriebsmitarbeiter und Ingenieure in jeder Phase des Vertriebszyklus belohnt.

Für Vertriebsmitarbeiter:

- 100 $ für die erste Terminvereinbarung mit einem Zielkunden.
- 250 $ für die Einreichung einer qualifizierten Geschäftsregistrierung.
- Bis zu 750 $ zusätzlicher Bonus bei Geschäftsabschluss.

Für Vertriebsingenieure (SEs):

- Bis zu 500 $ für den Abschluss von Basis- und Techniktrainings.
- Bis zu 350 $ zusätzlicher Bonus, wenn ein von Ihnen unterstütztes Geschäft abgeschlossen wird.

EIN STARKER STRATEGISCHER UND WETTBEWERBSENTSCHEIDENDER VORTEIL

Eine Partnerschaft mit FireMon eröffnet Ihnen die Möglichkeit, strategische Gespräche mit Ihren Kunden über deren wichtigste geschäftliche Herausforderungen zu führen, Mehrwert zu liefern, Ihr Geschäftsvolumen zu erhöhen und höhere Abschlussquoten zu erzielen.

Steigern Sie Ihren Status zum Trusted Advisor:
Sie lösen kritische Geschäftsprobleme, von der Komplexität der Richtlinien über Compliance-Verstöße bis hin zur Multi-Vendor-Transparenz, und festigen damit Ihre Rolle als strategischer Sicherheitsberater.

Erhöhen Sie die Kundenbindung:
FireMon wird tief in die Sicherheitsprozesse Ihres Kunden integriert. Durch die Bereitstellung von Transparenz, Analysen und Automatisierung wird FireMon unverzichtbar, reduziert die Abwanderung und schafft eine solide Grundlage für zukünftige Verkäufe.

Mit mehr Fortinet-Deals schneller zum Abschluss:
FireMon ist ein leistungsstarker Beschleuniger für Ihr Fortinet-Geschäft. Verwenden Sie FireMon, um das Risiko komplexer Migrationen zu verringern, Multi-Vendor-Umgebungen einfach zu verwalten und die granulare Transparenz zu liefern, die Unternehmenskunden benötigen. Gleichzeitig helfen Sie Ihren Kunden, ihre Fortinet-Investitionen zu maximieren, kombinierte ROI-Effekte zu realisieren und Sie zu unterstützen, Fortinet-Geschäfte schneller abzuschließen.

Hochwertige Unternehmenskunden ansprechen:
Die Lösungen von Firemon sind auf die komplexen Anforderungen von Großunternehmen zugeschnitten und ermöglichen es Ihnen, sich auf strategischere und lukrativere Geschäftsmöglichkeiten zu konzentrieren und den durchschnittlichen Geschäftswert zu erhöhen.

UNÜBERTROFFENER SUPPORT UND GEZIELTE UNTERSTÜTZUNG FÜR IHREN ERFOLG

Wir stellen Ihnen die Tools, Schulungen und den Go-to-Market-Support bereit, den Sie für einen erfolgreichen Start benötigen.

01 Spezielles Vertriebsteam und Partnerportal:

Das weltweite FireMon-Vertriebsteam steht Ihnen zur Seite. Über das Ignite-Partnerportal haben Sie zentralen Zugriff auf Geschäftsregistrierungen, das Pipeline-Management und Ressourcen.

02 Fertige „Kampagnenpakete“:

FireMon stellt Ihnen eine vollständige Suite von Co-Branded Marketing- und Vertriebsunterlagen bereit, darunter Battlecards, Lösungsübersichten und E-Mail-Kampagnen. So reduzieren Sie Ihren Marketingaufwand und können sofort mit der Leadgenerierung starten.

03 Umfassendes, kostenloses Training:

Die FireMon University bietet kostenlose, modulbasierte Online-Schulungen für Vertrieb und Technik. Damit stellen Sie sicher, dass Ihre Teams zertifiziert, kompetent und bestens vorbereitet sind, um die FireMon-Lösung zu präsentieren und zu demonstrieren.

04 Das Partner-Portal (Ignite):

Ihr zentraler Zugangspunkt für Trainings (FireMon University), Werbematerial, Kampagnenpakete und Geschäftsregistrierung.

05 Gemeinsames Go-To-Market (GTM) Engagement:

Dies ist eine echte Partnerschaft. Wie diese Kampagne beweist, arbeitet Exclusive Networks mit Ihnen und FireMon zusammen, um den Bekanntheitsgrad zu steigern und durch gemeinsame Roadshows, Kundentreffen, Webinare und digitale Marketingmaßnahmen neue Möglichkeiten zu schaffen.

Der Mehrwert von Exclusive Networks:

Als Ihr Value-Added-Distributor bietet Exclusive Networks lokalen Pre-Sales-Support, technische Schulungen, Marketingressourcen und flexible Finanzierungsmöglichkeiten, um Ihren Erfolg zu beschleunigen.

So starten Sie:

01 Absolvieren Sie das Sales 101 Training an der FireMon University.

02 Vereinbaren Sie einen Termin für eine Demo mit Ihrem Exclusive Networks-Team.


EXCLUSIVE
NETWORKS