

Extreme Platform ONE™

Die KI-gestützte Netzwerk- und Sicherheitsplattform für den Mittelstand

Ideal für den Mittelstand: Eine Plattform für Ihr Netzwerk

Extreme Platform ONE™ ist die neue, KI-gestützte Netzwerk- und Sicherheitsplattform von Extreme Networks, die Netzwerkbetrieb, Zugriffssicherheit und Lizenz-/Lifecycle-Management in einer einzigen Oberfläche bündelt und damit klassische Insellösungen ablöst. Dieser Solution Guide ordnet die Plattform strategisch ein, geht auf Architektur und Use Cases ein und zeigt, wie enthus Ihre IT-Organisation bei Konzeption, Migration und Betrieb unterstützt.

Viele IT-Leiter mittelständischer Unternehmen stehen vor identischen strukturellen Problemen, unabhängig von Branche und Größe:

- **Heterogene, historisch gewachsene Netzwerke**
Verschiedene Hersteller, unterschiedliche Management-Tools, Legacy-Switches/Access Points
- **Zunehmende Sicherheitsanforderungen**
NIS2, ISO 27001, KRITIS-nahe Anforderungen bei gleichzeitigem Fachkräftemangel im Netzwerk- und Security-Bereich
- **Verteilte Arbeitswelten**
Remote Work, Außenstellen, Produktionsstandorte, IoT/OT mit sehr unterschiedlichen Anforderungen an Konnektivität und Zugriffsschutz
- **Komplexe Lizenz- und Wartungsverträge**
Erschwerte Budgetplanung, Compliance und Transparenz

Die Folge: Die IT verbringt zu viel Zeit mit „Feuerwehr“ und manueller Administration und zu wenig Zeit mit Vorwärtsstrategie – also Projekten, die wirklich einen Wertbeitrag fürs Business liefern.



Dieser Solution Guide kurz zusammengefasst:

Mittelständische IT-Teams jonglieren heute mit gewachsenen Netzwerken, knappen Ressourcen und steigenden Compliance-Anforderungen wie NIS2 oder ISO 27001. Extreme Platform ONE™ bündelt Netzwerkbetrieb, Zugriffssicherheit und Lizenzmanagement auf einer KI-gestützten Plattform. Cloud NAC und Universal ZTNA regeln Zugriffe für Onsite, Remote und IoT über eine gemeinsame, identitätsbasierte Policy-Engine. Der AI Core übernimmt Diagnosen und Workflows, die sonst wertvolle Stunden kosten. So wird Zero Trust vom Buzzword zur gelebten Architektur. enthus bringt als Diamond-Partner von Extreme Networks die Erfahrung mit, die aus Technik echten Mehrwert macht.

Dieses Dokument ist sowohl in digitaler Form als auch als Printmedium urheberrechtlich geschützt. Das Dokument darf, ohne vorherige ausdrückliche, in schriftlicher Form erfolgte, Genehmigung von enthus weder gedruckt noch anderweitig vervielfältigt und weder in Form noch Inhalt verändert werden.

Copyright enthus, 2026

Zugleich entsteht durch Fragmentierung eine versteckte technische Schuld: Je mehr Einzellösungen, desto höher das Risiko von Fehlkonfigurationen, Sicherheitslücken und Wissensinseln.

Extreme Platform ONE™ zielt genau auf diesen Schmerzpunkt: weg von Produkt-Silos, hin zu einem einheitlichen, KI-gestützten Betriebsmodell für Netzwerk und Zugriffssicherheit.

Was ist Extreme Platform ONE™?

Extreme Platform ONE™ ist eine **Enterprise Connectivity Plattform**, die Netzwerkbetrieb, Zugriffssicherheit, Inventar- und Lizenzmanagement sowie KI-gestützte Automatisierung in einer integrierten Umgebung zusammenführt. Sie adressiert sowohl **NetOps** als auch **SecOps** und unterstützt den gesamten Lifecycle von „Learn – Plan – Deliver – Fix“.

- Ein **einheitlicher Echtzeit-Workspace** für Netzwerk, Sicherheit und Inventar (Switches, Access Points, Services).
- **Integrierte KI**, die weit über klassisches AI-Ops hinausgeht und Use Cases für Planung, Betrieb, Troubleshooting, Compliance und Beschaffung automatisiert.

- **Integrierte Zugriffssicherheit** über Extreme Platform ONE™ Security mit Cloud NAC und Universal ZTNA in einer gemeinsamen, identitätsbasierten Policy-Engine.
- **Vereinfachtes Lizenzmodell:** Netzwerkmanagement, Sicherheit, KI-Funktionen und Support werden über ein vereinheitlichtes Subscription-Modell abgebildet.

Damit positioniert sich Extreme Platform ONE™ als strategische Plattform, auf der Sie über Jahre Ihre **Netz- und Sicherheitsarchitektur** konsolidieren und weiterentwickeln können.

Die Architekturbausteine im Überblick

Echtzeit-Workspace und Multi-Domain-Sicht

Der zentrale Arbeitsbereich von Extreme Platform ONE™ bietet eine modulare und anpassbare Oberfläche, in der NetOps, SecOps und ggf. Business-Teams (z. B. Compliance, Einkauf) auf den gleichen Datenbestand zugreifen – jeweils mit eigenen Rollen, Dashboards und Sichten.



Wichtige Eigenschaften:



Multi-Domain-Ansicht über LAN, WLAN, Fabric und WAN in einer Oberfläche.



Netzwerk- und Fabric-Visualisierung von Topologie, Services und Abhängigkeiten.



Einheitliches Monitoring für Geräte, Benutzer, Applikationen und Policies.



Multimodale KI-Interaktion: Conversational AI und automatisierte Workflows.

Für Ihr IT-Management bedeutet das: Ein zentrales „Cockpit“, in dem sowohl der Netzwerkverantwortliche als auch der CISO bzw. Informationssicherheitsbeauftragte dieselbe Wahrheit sehen – aber jeweils auf die für sie relevanten Sichten und Kennzahlen heruntergebrochen.

Der neue Exteme AI Expert: AI Core mit AI Expert-System und AI Agenten

Der AI Core ist das übergreifende KI-Framework, das in Extreme Platform ONE™ eingebettet ist. Es nutzt konversationelle, multimodale und agentische KI, um typische Aufgaben entlang des Netzwerk- und Sicherheitsbetriebs zu beschleunigen:



Automatisierte Diagnosen und Fehleranalyse, um von Symptomen schneller zur Root Cause zu gelangen.



Proaktive Empfehlungen zu Kapazitätsplanung, Firmware-Compliance und Konfigurationsoptimierung.

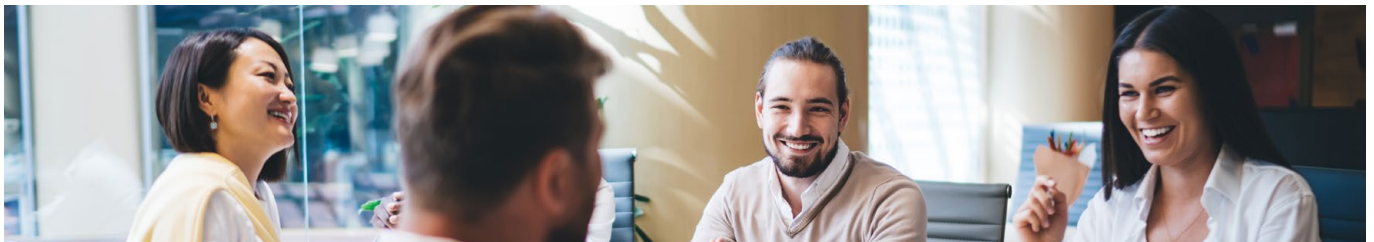


Agentische Workflows für komplette Prozessketten wie Policy-Anlage und Subscription-Management.



Service Agent verkürzt Lösungszeiten im Support durch Standardanalysen und Handlungsempfehlungen.

Damit verschiebt sich die Rolle der IT vom manuellen „Ticket-Abarbeiten“ hin zur Steuerung und Freigabe von automatisierten Aktionen.



Extreme Platform ONE™ Security: Cloud NAC & Universal ZTNA

Ein zentrales Element für Ihr zukünftiges IT-Management ist Extreme Platform ONE™ Security: Sie vereint Cloudbasiertes Network Access Control (NAC) und Universal ZTNA* in einer gemeinsamen, identitätsbasierten Policy-Engine.

Kernfunktionen:

- **Einheitliche Policies** für Benutzer, Geräte (inkl. IoT), Standorte, Netzwerke und Applikationen.
- **Cloud NAC für Campus- und Edge-Szenarien**, inklusive Integration in Identity Provider wie Microsoft Entra ID, OKTA oder Google Workspace.

- **ZTNA für Remote-Zugriffe**, mit granularen, applikationsbasierten Zugriffskontrollen und durchgängiger Zero-Trust-Architektur.
- **KI-gestützte** Policy-Empfehlungen und Validierung, um Fehler und Inkonsistenzen in der Policy-Landschaft zu reduzieren.

Universal ZTNA **kombiniert Cloud NAC und ZTNA** und ermöglicht damit eine einheitliche Zugriffslogik für Onsite- und Remote-User sowie IoT-Devices. Für **NIS2-** oder **ISO-27001-**getriebene Projekte ist das ein entscheidender Hebel, da Zugriffskontrolle, Authentisierung und Segmentierung zentral gesteuert und lückenlos dokumentiert werden können.

*Universal ZTNA (Extreme Platform ONE™ Security) ist als optionale, zusätzlich lizenzierbare kostenpflichtige Ergänzung zur Extreme Platform ONE™ Basis-Subscription verfügbar.

Universal Hardware und Fabric-Integration

Extreme Platform ONE™ nutzt die Universal-Hardware-Plattform von Extreme Networks, also Switches und Access Points, die über gleiche Lizenzen flexibel in unterschiedliche Feature-Sets gebracht werden können. Diese Universal-Geräte sind eng in Extreme Fabric integriert und lassen sich zentral konfigurieren, überwachen und in die Zero-Trust-Architektur einbinden.

Besonders relevant für mittelständische IT-Teams:

- „Instant Secure Port“-Konzepte für schnelle NAC-Aktivierung auf Switch-Ports.
- Automatisierte Sicherheitskonfiguration und Policy-Durchsetzung direkt über die Cloud-Plattform.
- Ein durchgängiges Inventory- und Lifecycle-Management für Hardware, Subscriptions und Support-Verträge.



Wann empfehlen wir Extreme Platform ONE™?

Moderne Campus-Netzwerke mit Zero Trust

Viele mittelständische Organisationen – vom produzierenden Betrieb bis zum Dienstleister – betreiben Campus-Netzwerke mit wachsender Zahl an IoT/OT-Geräten. Extreme Platform ONE™ ermöglicht hier:

- **Rollenbasierte Zugriffskontrolle** über Cloud NAC und Fabric-basierte Segmentierung von Datenströmen.
- **Automatisches Zuweisen** von Policies abhängig von Rolle, Gerätetyp, Standort und Sicherheitsstatus (z. B. Compliance-Status aus MDM/Intune).
- **Vollständige Transparenz** über Nutzer, Devices und Applikationen im Echtzeit-Workspace.

Sichere Remote-Arbeit mit Universal ZTNA

Homeoffice und mobile Arbeit sind im Mittelstand längst Standard – allerdings oft abgesichert mit historisch gewachsenen VPN-Lösungen. Universal ZTNA erlaubt, diese Strukturen zu modernisieren:

- **Zugriff** wird applikationsbasiert und identitätszentriert gesteuert, nicht mehr ausschließlich über Netzwerkeinwahl.

Ein praxisnahes Beispiel:

Ein neues IoT-Gerät wird angeschlossen, wird über Universal Hardware und Cloud NAC identifiziert, einem dedizierten VLAN/Fabric-Service zugeordnet und erhält nur den minimal notwendigen Zugriff auf Produktionssysteme, nicht aber auf interne Office-Netze. Was früher mehrere manuelle Schritte erforderlich machte oder sogar unentdeckt blieb, wird nun automatisiert mit maximaler Sicherheit gelöst.

- **Zentrales Policy-Management** für Office und Remote mit einheitlicher Zero-Trust-Logik.
- **Integration mit Entra ID und MDM-Lösungen** ermöglicht, nur konforme, registrierte Geräte zuzulassen.

Für den IT-Leiter bedeutet das: Eine konsistente Zugriffssicherheitsstrategie über alle Standorte und Arbeitsmodelle hinweg, mit klaren Audits und weniger operativem Aufwand.

NIS2-, ISO- und Compliance-getriebene Security-Projekte

Mit der zunehmenden Relevanz von NIS2 auch für viele mittelständische Unternehmen rücken Nachweispflichten, Risikomanagement und technische Maßnahmen stärker in den Fokus. Extreme Platform ONE™ unterstützt hier in mehreren Bereichen:

- **Durchgängige Sicht** auf Assets (Netzwerk-Devices, User, Applikationszugriffe) als Grundlage für Risikobewertungen.
- **Zero-Trust-Zugriffskontrolle** als technische Maßnahme zur Reduktion von Angriffswegen.
- **KI-gestützte Analyse** für Schwachstellen, Firmware-Compliance und Policy-Lücken.
- **Lückenlose Protokollierung** von Änderungen und Zugriffen für Audits.

Gerade in Branchen wie **Healthcare**, **Fertigung** mit kritischen Lieferketten, Defense oder **öffentlichen Einrichtungen** hilft die Plattform, regulatorische Anforderungen nicht nur formal, sondern operativ sauber umzusetzen.

Zusammenfassung im Überblick: viele Vorteile für mittelständische IT-Organisationen

Technische Vorteile

- **Vereinheitlichte Netzwerk- und Sicherheitsarchitektur:** Statt isolierter Tools entsteht ein konsistentes Betriebsmodell.
- **Schnellere Fehleranalyse und -behebung** dank KI-gestützter Diagnosen und automatisierter Workflows.
- **Durchgängige Zero-Trust-Zugriffskontrolle** über NAC und ZTNA hinweg, mit identitätsbasierter Policy-Engine.
- **Bessere Skalierbarkeit** – vom einzelnen Standort bis zu verteilten Campus- und Edge-Szenarien.

Organisatorische Vorteile

- **Reduktion manueller Tätigkeiten** und Standard-Tasks durch Automatisierung; die knappen Fachkräfte konzentrieren sich stärker auf anspruchsvolle Aufgaben.
- **Gemeinsame Datenbasis** und Sichten für NetOps, SecOps und Business-Teams, was Entscheidungsprozesse beschleunigt.

Effizientere Betriebsprozesse und Kostenkontrolle

Ein oft unterschätzter, aber für mittelständische IT-Budgets entscheidender Aspekt ist die Vereinfachung von Beschaffung, Subscription-Management und Support. Extreme Platform ONE™ unterstützt dies durch:

- **Zentral** verwaltete Subscriptions inkl. Verlängerungen und Upgrades in wenigen Klicks.
- **KI-Assistenz** für Lizenz- und Vertragsmanagement, um technische und finanzielle Risiken (z. B. auslaufende Subscriptions, Über- oder Unterlizenzierung) frühzeitig sichtbar zu machen.
- Plattform-integrierten **globalen Support**

Für Sie bedeutet das konkret: Mehr Transparenz in Kosten und Laufzeiten, weniger „Lizenzwildwuchs“ und ein klarer Rahmen für Budgetplanung und Investitionsentscheidungen.

- **Klarere Verantwortlichkeiten** und standardisierte Prozesse entlang des „Learn – Plan – Deliver – Fix“-Lifecycles.

Wirtschaftliche Vorteile

- **Senkung von Betriebsaufwänden** durch Automatisierung und Konsolidierung von Tools.
- **Besser planbare Kosten** durch ein vereinfachtes, integriertes Lizenzmodell statt vielfältiger Einzelverträge.
- **Reduziertes Risiko** von Sicherheitsvorfällen und damit verbundenen Folgekosten, da Zero-Trust-Prinzipien zentral umgesetzt werden.



Mit enthus: Vom Konzept zur produktiven Plattform

Extreme Platform ONE™ entfaltet seine Wirkung nicht durch das Produkt allein, sondern durch ein durchdachtes Design und eine saubere Implementierung. Genau dafür sind wir da – als einer der langjährigsten Partner von Extreme Networks mit Diamond-Status.

Strategische Netzwerk- und Security-Architektur

enthus unterstützt Sie dabei, aus einer gewachsenen Netzwerk- und Sicherheitslandschaft eine zukunftsfähige Architektur mit Extreme Platform ONE™ zu modellieren. Typische Schritte umfassen dabei meist:

- **Analyse** der bestehenden Netz- und Sicherheitsarchitektur (Hersteller, Topologien, Policies, „Schatten-IT“).
- **Definition** einer Roadmap zur Konsolidierung von Tools und Herstellern auf der Plattform.
- **Abgleich** mit Compliance-Anforderungen (z. B. NIS2, ISO 27001, branchenspezifische Vorgaben) und Ableitung von Zielzuständen für Zero Trust, Segmentierung und Monitoring.

Wir erarbeiten ein klares, mehrstufiges Zielbild, das Ihnen realistische Etappen und Budgets aufzeigt – statt „Big Bang“-Ansätzen, die im Alltag scheitern.

Entscheidungsleitfaden für Entscheider

Wenn Sie als IT-Leitung im Mittelstand die Einführung oder Modernisierung Ihrer Netzwerk- und Sicherheitsplattform planen, sollten Sie insbesondere folgende Fragen adressieren:

- **Welche Hersteller- und Tool-Landschaft** betreiben wir heute – und wie viele davon wollen wir in drei bis fünf Jahren wirklich noch haben?
- **Welche regulatorischen Anforderungen** (NIS2, ISO, branchenspezifische Vorgaben) werden in den nächsten Jahren für uns relevant – und bietet unsere aktuelle IT-Architektur dafür eine belastbare Basis?
- **Wie stark sind wir als IT heute von „Heldentaten Einzelner“ abhängig** – und wie viel können wir durch Standardisierung und Automatisierung abfangen?
- Haben wir ein **durchgängiges** Zero-Trust-Konzept über Onsite und Remote, Nutzer und IoT, Applikationen und Infrastruktur hinweg?

Technische Umsetzung und Migration

Die Einführung von Extreme Platform ONE™ erfolgt typischerweise iterativ, um Risiken zu minimieren und Mehrwerte früh sichtbar zu machen. enthus begleitet mit höchster Kompetenz und dem Blick für das pragmatisch Machbare u. a. in folgenden Bereichen:

- **Design und Implementierung** von Extreme Fabric, LAN/WLAN-Infrastruktur und Universal Hardware.
- **Aufbau** von Cloud NAC und Universal ZTNA inklusive Integration in Entra ID, MDM/Intune und bestehende IAM-Landschaften.
- **Migration** bestehender Policies und Access-Mechanismen in die gemeinsame Policy-Engine, inklusive Bereinigung und Vereinfachung.
- Schrittweise **Aktivierung von KI-Funktionen**, um Betriebsteams nicht mit „zu viel Neuerung auf einmal“ zu überfordern.

Wichtig ist dabei ein enges Zusammenspiel mit Ihren internen Teams – wir verstehen uns niemals als Ersetzer, sondern als technische Enabler und **#Erfolgreichmacher**.

- **Wie transparent** und beherrschbar sind unsere Lizenzen, Wartungsverträge und Subscriptions?

Extreme Platform ONE™ bietet eine konsistente Antwort auf diese Fragen – technisch wie organisatorisch. Die Plattform schafft die Grundlage, mit einem eher kleinen, aber leistungsfähigen IT-Team ein modernes, sicheres und skalierbares Netzwerk zu betreiben.



Nächste Schritte

Gemeinsam erfolgreich

Wenn Sie Ihre Netzwerk- und Sicherheitsarchitektur auf ein zukunftsfähiges, KI-gestütztes Fundament stellen wollen, ist jetzt der richtige Zeitpunkt, eine Plattformstrategie zu definieren und nicht das nächste Einzelfeature anzuschaffen. Lassen Sie uns gemeinsam prüfen, wie Extreme Platform ONE™ in Ihre bestehende Umgebung passt und welche konkreten Schritte – von der Standortanalyse über ein Pilotprojekt bis hin zur stufenweisen Migration – sinnvoll sind. enthus bringt die technische Tiefe in Extreme Networks-Lösungen, die Erfahrung aus anspruchsvollen Projekten im deutschen Mittelstand und die Sprache der Entscheider zusammen.



Unsere Standorte



Kostenfreies Erstgespräch

Sie wollen aus einer komplexen Tool-Landschaft eine sichere, skalierbare Plattform machen? Vereinbaren Sie ein unverbindliches Strategiegelgespräch mit unseren Expert:innen und holen Sie sich Handlungsfreiheit zurück. Wir gehen Ihr Setup, Ihre Compliance-Anforderungen und Ihre Roadmap zusammen durch.

enthus

Über 500 Enthusiast:innen an mehreren Standorten in Deutschland, Österreich und der Schweiz sind bei über 200 Millionen Euro Jahresumsatz leidenschaftliche **#erfolgreichmacher** für IT und Digitalisierung. Mit innovativen IT-Lösungen, Managed Services & XaaS sowie unseren smarten Lösungen für digitale Geschäftsprozesse wollen wir **#yourfirstchoice** auf dem Weg ins digitale Zeitalter sein.

Denn Herausforderungen löst man am besten im Schulter-schluss – partnerschaftlich und auf Augenhöhe.

Weitere Informationen finden Sie unter: **www.enthus.de**



Interessiert?

Robert Weiler

Head of Technical Sales Network Infrastructure

E-Mail: hallo@enthus.de