ADDNET

novicom

Integriertes DDI/NAC. Ein Betriebs- und Sicherheitstool, das vollständige Netzwerktransparenz, hocheffiziente IP-Adressraumverwaltung und erweiterte Netzzugangskontrolle bietet.

ADDNET ist ein Instrument, das die Effizienz der Verwaltung des IP -Adressraums und des sicheren Netzzugangs in großen verteilten Netzwerken erheblich verbessert und vereinfacht. Dies wird durch die Integration von leistungsfähiger Netzwerküberwachung, IP address space management (IPAM), core network services (DHCP, DNS), network access control (NAC) und Kommunikation mit Netzwerkhardware erreicht. Durch die Integration dieser konventionell unabhängigen Dienste wird eine neue Ebene der Netzwerkverwaltung und Netzwerksicherheit erreicht.

ADDNET bietet Zuverlässigkeit, Sicherheit und flexible Implementierung dank innovativer Novicom-Technologien, wie der internen SGP-Grid-Plattform, dem SDP -Kommunikationsprotokoll oder dem internen Novicom -Appliance-System. Umfassende Netzwerktransparenz, einfache Integration mit anderen Sicherheitstools und die Möglichkeit, es mit dem Security Operation Center (SOC) zu kombinieren, bieten eine neue Alternative für eine schnelle Reaktion auf erkannte Sicherheitsvorfälle.

DIE WICHTIGSTEN VORTEILE VON ADDNET:

- **Leistungsstarke L2-Überwachung** mit der Möglichkeit, die physische Lokalisierung eines Geräts durch die Integration von Kabelaufzeichnungen zu bestimmen
- Die Einführung einer effizienten Verwaltung des **IP-Adressraums (DDI)** spart den Netzwerkadministratoren viel Zeit und Arbeitsaufwand
- **NAC-Einführung** - Netzwerkzugangskontrolle mit 802.1x oder MAC-Authentifizierung und -Autorisierung (VLAN-Zuweisung)
- Vollständig **automatisierte Verwaltung von BYOD-** und Mobilgeräten und ihrem eindeutigen Netzwerk
- Standardisierung der Aktivitäten von Netzwerkadministratoren und Möglichkeit zur Zentralisierung der Verwaltung großer verteilter Netzwerke
- Erheblich verbesserte Betriebszuverlässigkeit und Leistung von DNS, DHCP und NAC durch den Einsatz mehrerer Redundanzen und erstklassiger Skalierbarkeit
- Kostenreduzierung - Effizienz wird aufgrund von Arbeitsreduktion und Langzeitüberwachung erreicht
- **Volle Heterogenität** und einwandfreies Zusammenspiel mit Netzwerkhardware führender Technologiehersteller
- Einzigartige Unterstützung des verteilten Netzwerkmodells eine Garantie für **L2 Monitoring / DDI / NAC** Operationen auch von entfernten Standorten oder in Fällen, wenn eine Verbindung zum zentralen Standort verloren geht
- Datensammlung für den **Backup-Betrieb von entfernten Standorten - Syslogs, Datenflüsse**
- **Flexibler Einsatz** - geeignet sowohl für zentralisierte als auch für vollständig verteilte Organisationen
- **Einfache Implementierung** - kombiniert das ursprüngliche Netzwerk-Sniffing mit der Novicom-Implementierungsmethodik, die auf Best Practices“ basiert
- Bereit für die Implementierung in **technologische OT/ SCADA-Netzwerke**
- **Integration von ADDNET mit SOC** - gewährleistet eine schnelle Reaktion auf Vorfälle (Ereignissammlung / Bewertung / Reaktion)
- ADDNET ist in der Lage, **mit anderen Instrumenten integriert zu werden, wie z.B. MS Active Directory, SIEM, Log Management, NBA, DLP,** etc.
- **Alarmierung** - schnelles Benachrichtigungssystem bei potenziellen Problemen in einem Netzwerk

Umfang der ADDNET-Funktionalität:

Leistungsstarke L2-Überwachung

Die Echtzeitüberwachung bietet umfassende Informationen über den Standort eines Geräts (IP- und MAC-Adresse) im Netz (einschließlich Switch-Port und physischer Standort), sowie eine Visualisierung des physischen Standorts des Geräts auf einem Grundriss. Darüber hinaus bietet sie eine vollständige Historie der Netzwerkoperationen für Auditing-Zwecke.

Vollständige DDI (DHCP / DNS / IPAM)

Bereitstellung von zuverlässigen Kernnetzdiensten (DHCP und DNS). Einfache Verwaltung durch das integrierte IPAM-Tool. Durch die Integration mit der L2-Überwachung kann das System in Echtzeit Lösungen für Widersprüche zwischen den sich ständig ändernden Verbindungen im Betrieb und dem IP-Adressplan finden und so dazu beitragen, dass der Adressplan jederzeit mit der betrieblichen Realität übereinstimmt.

- **IPAM**

Das IP-Administrationssystem bietet ein vielseitiges und benutzerfreundliches Adressraum-Management-Tool mit einer integrierten Verwaltung aller notwendigen Komponenten (DHCP / DNS / NAC). Es ist einfach, ein neues Gerät hinzuzufügen oder die Netzwerkparameter bestehender Geräte im Rahmen des Adressplanungsprozesses zu ändern.

- **DHCP**

Die Standard-DHCP- Dienste sind für den Betrieb in großen verteilten Netzwerken und in Netzwerken, in denen ein Höchstmaß an Betriebssicherheit oder Leistung erforderlich ist, konzipiert. Die integrierte L2 -Überwachung bietet erweiterte Betriebsoptionen und Flexibilität, einschließlich der Zuweisung fester IP -Adressen durch DHCP entsprechend bekannten MAC-Adressen

- **DNS**

Integrierte DNS -Dienste sorgen für einen zuverlässigen Betrieb in verteilten Netzwerken. Aufgrund seiner Flexibilität ist ADDNET auch in der Lage, die bestehende DNS-Infrastruktur durch dynamische DNS -Updates zu steuern. Dies gewährleistet die vollständige Konsistenz der IPAM-, DHCP- und DNS-Umgebungen.

Integrierte NAC (Netzwerkzugangskontrolle)

Der Vorteil der AddNet NAC-Lösung ist, dass die Lösung Herstellerunabhängig ist und die Infrastruktur des Unternehmens keine Rolle spielt. Die Möglichkeit, 802.1x in Kombination mit MAC-Authentifizierung zu betreiben und die Fähigkeit, in großen verteilten Netzwerken zu implementieren. Folglich kann die NAC- Funktionalität von entfernten Standorten aus gewährleistet werden, auch wenn diese vorübergehend vom zentralen Standort getrennt sind.

- **Vollständige 802.1x-Authentifizierung**

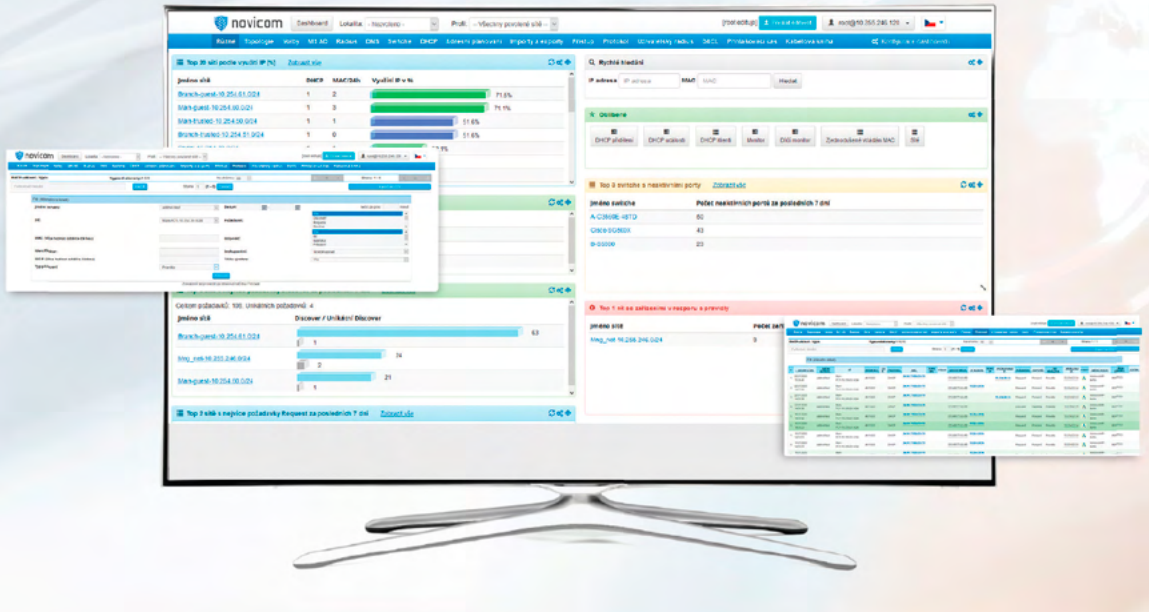
ADDNET gewährleistet eine sichere Geräteauthentifizierung überall im Netzwerk. Die Authentifizierungsdaten können vollständig in ADDNET verwaltet oder durch Integration mit Microsoft Active Directory oder anderen Quellen (OpenLDAP, Novell...) bezogen werden. Alle Standard- Authentifizierungsmodi werden unterstützt – jede Kombination von Client-Zertifikat/Benutzer-ID/ Passwort.

- **MAC-Authentifizierung mit Schutz**

Als Alternative für Geräte, die keine Authentifizierung durch Supplicants unterstützen, steht die MAC-Authentifizierung mit zusätzlichem Schutz zur Verfügung. Die integrierte L2 Überwachung kann mehrere Parameter auswerten, indem sie DHCP-Pakete und andere Kriterien analysiert. ADDNET benachrichtigt den Administrator über geänderte MAC - Adressen. Der Vorteil dieses Ansatzes ist die Zeiteffizienz, da die komplexe Implementierung und Verwaltung eines vollständigen 802.1x-Supplicant entfällt. Es müssen keine Ausnahmen verwaltet werden - alle Switch-Ports sind ständig unter Kontrolle.

- **Echtzeit-Informationen aus dem NAC-Betrieb**

ADDNET bietet eine übersichtliche Visualisierung von Informationen über Geräte, die sich im Rahmen des NAC anzumelden versuchen - wann, mit welcher ID (im Falle eines externen Berechtigungsbenutzers), in welchem Switch oder Port und in welches Netz das Gerät eingeteilt wurde.



Notfallplanung

ADDNET kann Krisenszenarien und kritische Elemente in der Infrastruktur einer Organisation definieren. Im Falle eines Sicherheitsvorfalls ist es möglich, einen Krisenplan mit einem einzigen Klick zu aktivieren und alle Geräte, die nicht in dem definierten Plan aufgeführt sind, sofort vom Netz zu trennen.

Netzwerkverwaltung und Zugangskontrolle für BYOD und mobile Geräte

ADDNET bietet ein vollständiges IP-Management für Wi -Fi- Netzwerke. Das DDI/NAC-Verwaltungsmodell wird durch eine einfache BYOD - und Mobilgeräteverwaltung ergänzt.
ADDNET bietet eine Self -Service-Zone, in der neue Geräte einfach zum Netzwerk hinzugefügt werden können. Der Vorteil von ADDNETs BYOD Modul ist die Fähigkeit, alle Arten von Benutzergeräten zu unterstützen, unabhängig vom Betriebssystem und der Umgebung des Geräts.

Erweiterte Kommunikation mit laufenden Komponenten

ADDNET liefert klare Informationen über aktive Netzwerkhardware im Speicher. Durch die kontinuierliche Überwachung des Up-/Down-Status von Ports kann ADDNET die Auslastung überwachen und die Anzahl der ungenutzten Netzwerkgeräte ermitteln. ADDNET bietet auch automatische Backups der Netzwerk-Hardware -Konfigurationen.

Dashboard

ADDNET liefert die wichtigsten Netz- und Nutzungsinformationen an einem Ort. Mit einem einzigen Klick kann der Benutzer schnell von den Dashboard-Daten zu detaillierten Informationen in ADDNET wechseln.

Leistungsstarke Berichterstattung

ADDNET bietet mehrere Möglichkeiten, den Betrieb von Geräten im Netzwerk einzusehen. Neben den Echtzeit -Informationen aus der L2-Überwachung und den detaillierten Daten aus dem DHCP liefert es auch Informationen von einzelnen Switches. Die Kombination verschiedener Quellen in einer einheitlichen Benutzeroberfläche bietet umfangreiche Möglichkeiten, um detaillierte Informationen über Geräte zu erhalten. Dies kann bei der Lösung von Sicherheitsvorfällen genutzt werden.

Erweiterte Netzwerkrichtlinien

Die miteinander verknüpften ADDNET -Funktionen ermöglichen eine einfache Implementierung fortschrittlicher Netzwerkrichtlinien, ohne dass der Einsatz separater Netzwerkadministrations -Tools erforderlich ist. Einige dieser Richtlinien umfassen:

- **Mikrosegmentierung**

ADDNET definiert und verwaltet effektiv DACL-Richtlinien für die meisten Access Switches. In der Praxis ist es daher einfach, die globalen Richtlinien des Geräts so anzupassen, dass es im Netz genau gemäß seiner korrekten Funktionalität kommuniziert. Durch die Angabe, dass es nur in bestimmten Bereichen des Netzwerks kommunizieren darf, werden andere Arten der Kommunikation nicht zugelassen, was den Schutz vor der potenziellen Verbreitung von Ransomware-Infektionen deutlich erhöht, ohne dass ein Agent auf den Stationen installiert werden muss.

- **Vertrauenswürdige Geräte**

ADDNET unterstützt vertrauenswürdige Geräte und Pools und ermöglicht automatisierte Netzwerkkonfigurationen und Zugriffsrichtlinien für große Unternehmen mit Niederlassungen. Neben ihrem Heimnetzwerk können vertrauenswürdige Geräte auch verschiedene Authentifizierungs-, Autorisierungs- und IP-Adresszuweisungsmethoden verwenden, ohne dass administrative Eingriffe erforderlich sind.

- **Anmeldezeit**

Organisationen mit festen Arbeitszeiten können ADDNET so einstellen, dass es nur in bestimmten Zeiträumen arbeitet (z.B. 7:00 -19:00). Diese Einstellung kann auch auf bestimmte Geräte abzielen oder andererseits ausgewählten Geräten eine Ausnahmeregelung gewähren.

Aktive SOC

Aufgrund seiner funktionalen Flexibilität und des verfügbaren verteilten Modells ist ADDNET eine sehr gefragte Ergänzung für die Security Operation Center (SOC). Zusammen mit den aus der Überwachung gewonnenen Informationen liefert es den SOC-Betreibern Informationen über Network Services (DHCP/DNS und NAC). Sie können durch die zuverlässige Erfassung von Syslog- und Flow-Daten von entfernten Standorten aus weiter verbessert werden. Das SOC erhält vollständige Informationen über den Netz- und Infrastrukturbetrieb aller Netzstandorte. Die Integration der SOC-Tools mit ADDNET gewährleistet eine sofortige Reaktion auf Störungen in Form einer Isolierung oder Abschaltung der fehlerhaften Geräte durch den SOC-Operator, ohne dass eine Zusammenarbeit mit dem lokalen Netzwerkadministrator erforderlich ist.

Integration

ADDNET ist bereit für mehrere Integrationen, die die Netzwerkverwaltung effizienter machen und eine schnelle Reaktion auf Störungen gewährleisten.

- **Bereitstellung und Erhebung von Betriebsdaten**

ADDNET ist eine wertvolle Quelle für die Bewertung von Informationen mit Hilfe der fortschrittlichsten Werkzeuge des Log- Management- oder SIEM-Typs. Über die Syslog-Schnittstelle werden Betriebsinformationen und Informationen über Nicht-Standardsituationen bereitgestellt. Darüber hinaus verfügt ADDNET in Form seiner erweiterten Anwendungen über die Fähigkeit, eine kontinuierliche Datenerfassung des Netzwerkbetriebs (Flow) oder des Zustands der Infrastruktur (Syslog) sicherzustellen. Diese Informationen werden sicher übertragen und können über spezialisierte Anwendungen (SIEM, NBA) an zentraler Stelle ausgewertet werden.

- **Integration von Anwendungen**

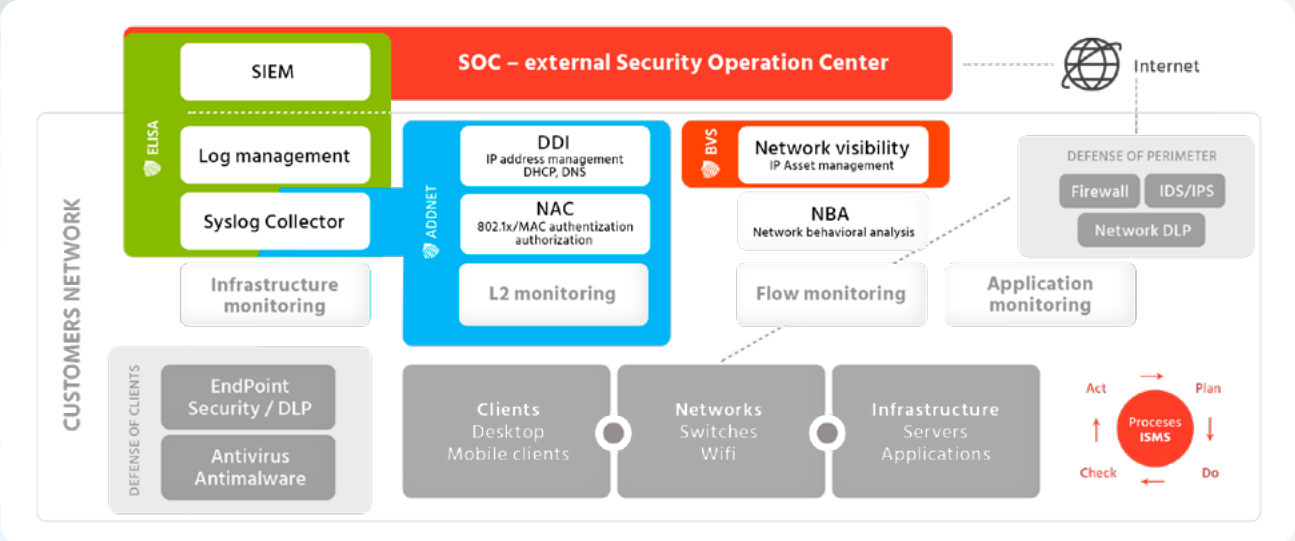
ADDNET bietet eine Schnittstelle für die Anwendungsintegration mit anderen Tools, wie z.B. Verhaltensanalyse (NBA), Log-Management oder SIEM. ADDNET ist auch bereit, eine Schnittstelle für automatisierte Interventionen zu implementieren. Glaubwürdige Erkennungssysteme wie DLP, NBA, Anti- Malware oder IDS/IPS können Informationen und Anweisungen übermitteln, die zur Durchführung von administrativen Eingriffen erforderlich sind.

Alert Center

ADDNET besteht aus einer Schnittstelle, über die der Administrator/Bediener Warnungen über mögliche Probleme verwalten kann. Der Zweck von Alert Center ist die Vereinfachung und Automatisierung des gesamten Verwaltungsprozesses, der mit der Prüfung von Alarmen verbunden ist. Das System integriert Warnungen aus der L2-Überwachung (z. B. doppelte MAC), dem Betrieb von NAC (z. B. erfolglose Authentifizierung 802.1x) und mehr.

ADDNET UND AKTIVE SOC

ADDNET ist ein wichtiger Bestandteil der Active SOC (Security Operation Center) -Strategie, die Novicom zusammen mit seinen SOC-Partnern auf dem Markt vorantreiben will. Novicom ADDNET wird zusammen mit der Novicom BVS -Lösung (zur Visualisierung von Netzwerken) und die Novicom ELISA (für das Abfangen und Auswerten von kybernetischen Sicherheitsereignissen) und die Novicom ELISA (für das Abfangen und Auswerten von Cyber- Sicherheitsereignissen) bilden ein einzigartiges Portfolio, das den Kunden eine schnelle und nahtlose Anbindung an den SOC-Service ermöglicht.



Kunden, die diese Produktplattform nutzen, können dann die Premium-Services von Active SOC in vollem Umfang in Anspruch nehmen. Damit sind ausgewählte SOC-Betreiber in der Lage, eine voll qualifizierte aktive Reaktion auf Cyber-Attacken im 24x7 -Modus zu gewährleisten, ohne dass eine Zusammenarbeit mit den Systemadministratoren beim Kunden erforderlich ist.
Dies entspricht vollkommen dem aktuellen Trend, die Top-Sicherheitsüberwachung (SOC) als Dienstleistung zu nutzen. Mit diesem Ansatz entfällt der wirtschaftliche Nachteil der Anschaffung einer kompletten Palette von Einzwecktechnologien und die Notwendigkeit, über ein eigenes hochspezialisiertes Team zu verfügen, das jederzeit in der Lage ist, professionellen Hackern entgegenzutreten.

NOVICOM – CYBER SECURITY & NETWORK MANAGEMENT HAS NEVER BEEN EASIER

novicom

Novicom, s.r.o.
Prag, Tschechische Republik
www.novicom.eu
sales@novicom.eu

ADDNET

NVC DE 2022-02