NAC dans l'automobile — Un niveau supérieur de sécurité et de contrôle du réseau OT

ÉTUDE DE CAS

La solution NAC de Belden, éprouvée sur le terrain et indépendante du fabricant, sécurise les réseaux opérationnels de l'un des plus grands constructeurs automobiles au monde.

Résumé 1
À propos du client 1
Défis du client 2
Définition de la solution 2
Parcours du projet 2
Résultats uniques 2
Fonctionnalités du module Advanced Security 3

Résumé

Les entreprises du monde entier sont la cible de cybercriminels qui veulent accéder aux réseaux de production, une perturbation contre laquelle les entreprises doivent se protéger pour rester compétitives.

Dans une entreprise opérant à l'échelle mondiale avec des sites de production répartis dans le monde, des normes de sécurité internationales et des infrastructures hybrides, Belden fournit une solution éprouvée sur le terrain et indépendante du fabricant avec macmon NAC (Network Access Control).

À propos du client

Le client est une entreprise mondiale du secteur automobile. La solution macmon NAC de Belden est déployée dans l'une des installations de production les plus modernes au monde.

Défis du client

Le client utilise PROFINET, un protocole de communication basé sur Ethernet largement utilisé dans le secteur de l'automatisation.

Il offre une grande largeur de bande et des capacités en temps réel, ce qui le rend intéressant pour de nombreuses applications.
Cependant, l'utilisation de PROFINET peut compliquer la sécurité, car il offre une surface d'attaque plus grande que les fieldbus conventionnels.

Définition de la solution

La solution macmon NAC de Belden est spécialement conçue pour protéger le réseau PROFINET contre les cyberattaques grâce aux fonctionnalités suivantes :

- Restriction de l'accès aux ressources du réseau aux dispositifs autorisés ou de confiance
- Intégration avec les solutions de sécurité existantes
- Isolement ou quarantaine des dispositifs problématiques ou compromis, sans perturber la production

Mise en oeuvre/parcours du projet

Les exigences spécifiques du client, identifiées dans une preuve de concept (POC), ont été mises en œuvre par les experts en cybersécurité de Belden dans un délai remarquablement court.

Des investissements supplémentaires en matériel et en conseil n'ont pas été nécessaires. Des fonctionnalités spéciales ont même été intégrées au produit en quelques jours seulement.

Le défi consistait à créer un moyen simple de déconnecter complètement une zone de production ou une « bulle de production » pour les terminaux inconnus.
Cela signifie que tous les terminaux à l'intérieur de la bulle peuvent continuer à produire, sauf en cas d'attaque immédiate contre un certain terminal.

Le défi consistait à créer un moyen simple de déconnecter complètement une zone de production ou une « bulle de production » pour les terminaux inconnus.

Cela permet d'éviter que des menaces potentielles ne se propagent à d'autres parties d'une installation en créant une séparation artificielle (air gap).
En outre, d'autres parties du système ne sont pas affectées dans ce cas d'utilisation jusqu'à ce que le problème soit résolu.
La solution macmon NAC ne repose pas sur l'utilisation obligatoire de RADIUS/802.1x dans certaines parties du système, mais il existe d'autres stratégies pour détecter un comportement indésirable dans les parties du système qui ne peuvent pas utiliser RADIUS/802.1x.

Résultats uniques

La solution macmon NAC de Belden utilise plusieurs technologies pour collecter des informations sur le système d'exploitation, le nom de domaine et les ports réseau d'un terminal. Cela améliore la visibilité du réseau et aide l'administrateur à mieux classer, identifier et localiser les terminaux.

La solution macmon NAC de Belden compare également les informations collectées avec les données existantes afin de prévenir les usurpations et les attaques ARP (Address Resolution Protocol).

Elle détecte et arrête les attaques de type « man-in-the-middle » et alerte et isole les dispositifs dont l'adresse IP est dupliquée.

Grâce à une fonctionnalité du module Advanced Security, macmon NAC de Belden peut inspecter chaque dispositif qui entre dans le réseau. La solution peut communiquer avec les dispositifs en utilisant leur adresse IP. Elle peut également vérifier que le terminal est identique ou similaire à celui qui a été autorisé précédemment. Dans le cas contraire, elle peut supprimer le dispositif du réseau ou le déplacer vers un réseau de quarantaine.

Elle peut alors examiner le niveau de menace et l'activité du dispositif dans un environnement sécurisé. Elle peut également se contenter de notifier ou de consigner l'événement.

Un autre moyen de vérifier le dispositif consiste à utiliser SSH, un protocole de prise d'empreintes digitales. L'empreinte SSH permet d'identifier chaque client de manière unique.

Le protocole TLS (Transport Layer Security) est utilisé pour des vérifications supplémentaires des certificats, et d'autres protocoles sont également disponibles pour la vérification.

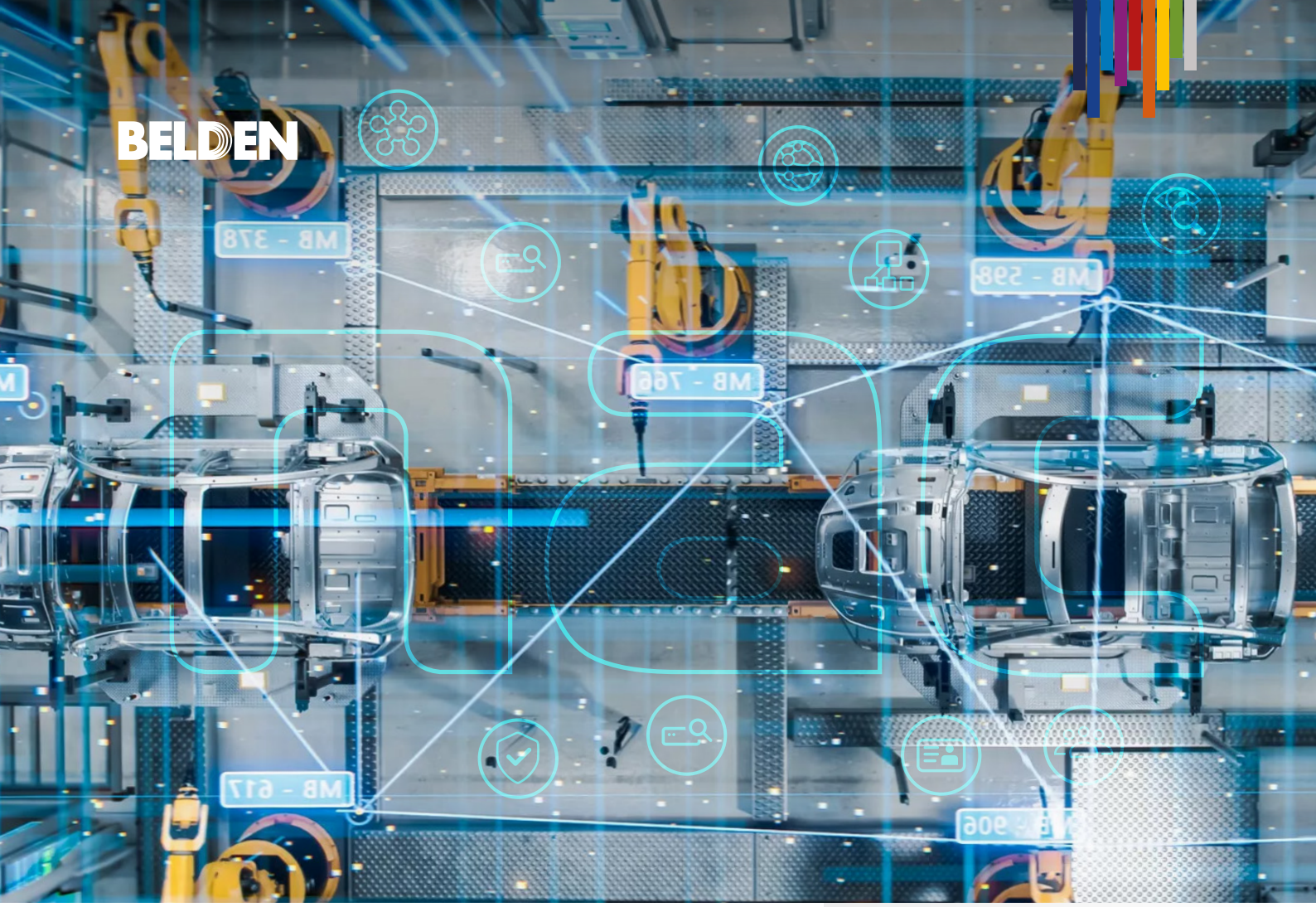
La solution macmon NAC de Belden peut vérifier périodiquement si les dispositifs sont toujours à jour en définissant une valeur temporelle dans l'interface Web, par exemple 60 minutes.

Fonctionnalités du module Advanced Security

La solution Advanced Security de macmon NAC de Belden offre aux clients les fonctionnalités suivantes:

- Identification des systèmes d'exploitation des dispositifs connectés au réseau
- Nom de l'emplacement du dispositif (emplacement physique)
- Identification des ports ouverts et fermés (TCP et UDP)
- Vérification de connexion réussie
- Nom du système
- Nom du domaine Active Directory
- Autorités de certification
- Empreintes
- Prévention des incidents de sécurité tels que l'usurpation d'adresse ARP, la non-concordance MAC IP, l'inondation d'adresses MAC et l'usurpation d'adresse MAC

En utilisant macmon NAC Advanced Security de Belden, l'entreprise automobile a atteint ce niveau supérieur de sécurité et de contrôle du réseau OT pour ses opérations de fabrication – sans aucun impact négatif sur la disponibilité de l'environnement de production.



À propos de Belden

Belden Inc. fournit l'infrastructure qui rend la transition numérique plus facile, plus intelligente et plus sûre. Nous ne nous concentrons pas seulement sur la connectique, mais aussi sur ce que nous rendons possible grâce à une gamme de produits axée sur la performance, un savoir-faire tourné vers l'avenir et des solutions sur mesure. Avec plus de 120 ans d'expérience en matière de qualité et de fiabilité, nous disposons d'une base solide sur laquelle nous pourrons continuer à bâtir à l'avenir. Notre siège social se trouve à St. Louis aux Etats-Unis et nous disposons de sites de production en Amérique du Nord, en Europe, en Asie et en Afrique.
Pour de plus amples informations, rendez-vous sur www.belden.com et suivez-nous sur Facebook, LinkedIn et X/Twitter.

En savoir plus

Pour plus d'informations, rendez-vous sur :
www.belden.com/networksecurity