HIRSCHMANN
A BELDEN BRAND

HOPF
PARTNER | SOLUTIONS | COMPONENTS

New Product Bulletin

NP 1012HG

Hirschmann™ EAGLE Tofino

Sicherheit für Ihr Steuerungsnetzwerk auf Zone Level

Schützen Sie Ihr Steuerungssystem vor Netzwerkproblemen und Cyber-Attacken

Vielleicht sind Sie noch nie von einem gefährlichen Hacker attackiert worden, doch typische Steuerungsnetzwerke sind äußerst anfällig für simple alltägliche Sicherheitsrisiken. Mangelhafte Netzwerkaufteilung, ungeschützte Zugangspunkte, „weiche" Ziele wie Rechner ohne Sicherheitspatch und angreifbare speicherbare Steuerungen sowie menschliche Fehler können signifikante Produktionsverluste und auch Sicherheitsprobleme verursachen.

Tofino Industrial Security ist eine verteilte Sicherheitslösung, mit der sich innerhalb Ihres Steuerungsnetzwerks schnell und kostengünstig ein wirksamer Schutz vor Cyber-Attacken einrichten lässt.

Die flexible Architektur von Tofino ermöglicht die Bildung von Sicherheitszonen – Zone Level Security™ – in Ihrem gesamten Steuerungsnetzwerk, um funktionskritische Systemkomponenten zu schützen. Tofino hilft Ihnen, die Anforderungen der Standards NERV CIP und ANSI/ISA-99 zu erfüllen. Und trägt dazu bei kostenintensive Stillstandzeiten zu vermeiden und die optimale Leistungsfähigkeit Ihres Betriebs sicherzustellen.

Vorteile von EAGLE Tofino™

- Kein IT-Knowhow erforderlich
- Erhöhte Daten- und Betriebssicherheit
- Erweiterung der Sicherheit gegen Cyber-Attacken auf die Ebene des Steuerungsnetzwerks
- Vereinfachte Einhaltung von Vorschriften und Normen
  - FERC / NERC CIP
  - ANSI/ISA-99
  - IEC 62443

HIRSCHMANN
A BELDEN BRAND

Zentrale Managementplattform und ladbare Sicherheitsmodule

Planen Sie Ihr Sicherheitssystem in vier einfachen Schritten

Schritt 1:

Legen Sie fest, wo Tofino-Sicherheit benötigt wird
Ermitteln Sie, an welchen Punkten Tofino-Sicherheitsgeräte installiert werden sollen, um Zone Level Security™ für die Teilnehmer in Ihrem Netzwerk einzurichten. Hinweis: ANSI/ISA-99 empfiehlt, die Kommunikation in unterlagerten Steuerungssystemen bzw. „Zonen" zu halten.

Schritt 2:

Bestimmen Sie, mit welchen ladbaren Tofino-Sicherheitsmodulen die einzelnen Hardwarepunkte geschützt werden sollen
Sie wollen Ihr Netzwerk wie mit einem Radar abtasten, um jede aktive oder angestoßene Gerätekommunikation mit einem spezifischen Tofino-Sicherheitsgerät nachzuverfolgen? Dann laden Sie das Tofino™ Secure Asset Management LSM.
Sie benötigen einen auf Netzwerkkommunikation spezialisierten „Verkehrspolizisten", der sämtliche Kommunikationsereignisse auf Regelkonformität prüft, den Zugang bei Verstößen blockiert und entsprechend Bericht erstattet? Dann laden Sie das Tofino™ Stateful Firewall Module.
Sie brauchen einen „Grenzposten", der jeden Modbus-Befehl und jede Rückmeldung kontrolliert sowie unzulässige Funktionscodes oder Speicheradressen blockiert und meldet? Dann laden Sie das Tofino™ Modbus TCP Deep Packet Instrumentation LSM.
Sie möchten sichere Kommunikationstunnel in Ihr Firmennetzwerk oder ins Internet einrichten? Dann laden Sie die Tofino™ VPN Client und VPN Server LSM.

Schritt 3:

Wählen Sie den bestgeeigneten Server oder Arbeitsplatzrechner für das zentrale Tofino-Management
Die Tofino™ Central Management Platform als Software gestattet die Konfiguration, Verwaltung und Überwachung sämtlicher Tofino-Sicherheitsgeräte von einer einzigen Workstation aus..

Schritt 4:

Informieren Sie sich über Produktdetails und Bestelldaten unter **www.hirschmann.com**

EAGLE Tofino™ Central Management Platform

Konfigurieren und managen Sie die Sicherheit Ihres gesamten Steuerungsnetzwerks von einem einzigen Standort aus

Traditionelle Sicherheitsgeräte müssen einzeln nach einander konfiguriert werden. Mit zunehmender Anzahl der Geräte ist schnell der Punkt erreicht, wo sich dies nicht mehr bewältigen lässt. Schlimmer noch: Die Geräte-orientierte Sicht bietet keine Möglichkeit, die Geschehnisse auf der Systemebene zu verfolgen, sodass sich die Diagnose und Behebung von Sicherheitsproblemen zeitaufwändig, fehlerträchtig und unrentabel gestaltet.
Mit der Software der Tofino Central Management Platform (CMP) können Sie sämtliche Ihrer Tofino-Sicherheitsgeräte von einem einzigen Arbeitsplatz aus konfigurieren, managen und überwachen. Die CPM-Software erstellt Ihnen im Handumdrehen ein Modell Ihres gesamten Steuerungsnetzwerks. Grafische Drag-and-Drop-Tools erleichtern Ihnen das Erstellen, Bearbeiten und Testen Ihrer Tofino-Konfiguration. Und wenn Sie Ihr Sicherheitssystem dann in Betrieb nehmen, zeigt Ihnen die CPM-Software auf einen Blick den Status des gesamten Systems und ermöglicht Ihnen eine koordinierte Reaktion auf potenzielle Cyber-Gefahren.

Kostenvorteile

- Erhöhte Netzwerkverfügbarkeit
- Zeit sparende Einrichtung
- Schnelle Fehlerlokalisierung
- Geringe Schulungs- und Personalkosten

Merkmale

- Konfiguration, Verwaltung und Überwachung aller Tofino-Sicherheitsgeräte von einem einzigen Arbeitsplatz aus
- Integrierter Netzwerkeditor zur schnellen Erstellung eines Modells Ihres Steuerungsnetzwerks
- Grafische Drag-and-Drop-Tools zur schnellen und einfachen Konfiguration von Sicherheitsregeln
- Vordefinierte Muster (Templates) für über 50 industrielle Busprotokolle und mehr als 25 Familien von Industriesteuerungen

Anwendungen

- Prozesssteuerung, SCADA-Systeme, Abtastregelung

EAGLE Tofino™ Firewall

Behalten Sie die Kontrolle über Ihren Netzwerkverkehr

In der überwiegenden Mehrheit aller Steuerungsnetzwerke sind die diversen unterlagerten Systeme kaum oder überhaupt nicht gegen einander abgeriegelt. Wenn dann ein fehlerhaft konfiguriertes Gerät, ein Hardwareausfall oder Virus Probleme in einem Teil des Netzwerks verursacht, können sich diese in wenigen Sekunden über das gesamte Netzwerk ausbreiten und Ihren Betrieb vollständig lahmlegen. Selbst redundante Backup-Systeme können gleichzeitig ausfallen, wenn ihre Netzanbindung nicht geschützt ist.
Das Tofino Firewall LSM ist ein „Verkehrspolizist" für industrielle Netzwerke, der die gesamte Kommunikation in Ihrem Steuerungsnetzwerk auf Einhaltung der von Ihren Steuerungstechnikern definierten „Verkehrsregeln" überwacht. Unzulässige Kommunikation wird von der Tofino-Firewall blockiert und gemeldet. Die Kommunikationsregeln werden mit Methoden erstellt, die Ihren Steuerungsexperten vertraut sind. Und der herausragende Testmodus von Tofino erlaubt Ihnen die Prüfung Ihrer Regeln ohne jedes Risiko für den laufenden Betrieb.

Kostenvorteile

- Vereinfachte Konformität mit Standards für Daten- und Betriebssicherheit
- Reduzierte Stillstandzeiten und Produktionsverluste
- Erhöhte Systemzuverlässigkeit und -stabilität

Merkmale

- Definition der Kommunikationsregeln – welche Geräte mit welchen Protokollen kommunizieren dürfen - durch Ihre Steuerungstechniker
- Einfache Regelerstellung mittels grafischem Drag-and-Drop-4-Editor
- Automatische Blockierung und Meldung von Regelverstößen
- Über 50 vordefinierte IT- und industrielle Busprotokolle
- Über 25 vordefinierte Controller-Templates
- Vordefinierte Sonderregeln für fortschrittliche Kommunikationsfilter und wirksamen Angriffsschutz

Anwendungen

- Abriegelung funktionskritischer Geräte gegen Gefahrquellen

EAGLE Tofino™ Secure Asset Management

Zuverlässige Lokalisierung von Geräten im Netzwerk und einfache Erstellung von Firewall-Regeln

Bevor Sie ein Steuerungssystem schützen können, müssen Sie genau wissen, welche Geräte sich im Netzwerk befinden und wie sie mit einander kommunizieren. Klingt logisch, doch bei der Komplexität heutiger Systeme kann die umfassende und genaue Beschaffung der Informationen über installierte Geräte und Protokolle ohne die richtigen Tools mit enormem Aufwand verbunden sein.
Wie ein Radar lokalisiert das Torino Secure Asset Management (SAM) Loadable Security Module (LSM) jedes Gerät, das über Ihre Tofino-Sicherheitsgeräte kommuniziert. Dabei verwendet es jedoch keine der traditionellen Abtastverfahren, die Prozessstörungen verursachen könnten.
Tofino SAM identifiziert die Geräte, sodass Sie auf einfache Weise mit Definitionen aus der Tofino CMP-Datenbank Kommunikationsregeln erstellen können. Falls eine dieser Regeln beim Test geändert werden muss, unterstützt Sie der SAM-Assistent beim Auswerten der von den Tofino-Sicherheitswarnungen erfassten Daten. Nach der Inbetriebnahme sorgt Tofino SAM für permanenten Schutz, indem es Sie warnt, wenn neue Geräte im Netz erkannt werden.

Kostenvorteile

- Vereinfachte Konformität mit Vorschriften und Sicherheitsstandards
- Reduzierter Zeit- und Arbeitsaufwand für die Aktualisierung von Bestandslisten
- Geringere Entwicklungs- und IT-Kosten dank leichterer Erstellung von Firewall-Regeln

Merkmale

- Identifikation von Steuerungsgeräten und Empfehlung von Firewall-Regeln mittels integrierter Gerätedatenbank
- Geführte Erstellung von Firewall-Regeln mittels Blockierberichten und Regelassistent
- Meldung neu entdeckter Betriebsmittel im Netzwerk in Form von Sicherheitswarnungen

Anwendungen

- Herstellen der Konformität mit ISA-99 und NERC anhand von Betriebsmittellisten und kontinuierlicher Überwachung
- Erkennung nicht-autorisierter Geräte im Netz, wie Laptops etc.

EAGLE Tofino™ Modbus TCP Enforcer

Fortschrittlicher Schutz von Modbus-Geräten vor Cyber-Attacken

Wussten Sie, dass jedes Gerät mit einer Netzwerkverbindung zu einem Modbus-Controller jeden der E/A-Kanäle oder Registerwerte des Controllers ändern kann? Viele Controller lassen sich sogar zurücksetzen, sperren oder mit neuer Steuerlogik und Firmware beschreiben.
Der Tofino Modbus TCP Enforcer ist ein „Inhaltskontrolleur" für die Modbus-Kommunikation. Er prüft jeden Modbus-Befehl und jede Rückmeldung auf Übereinstimmung mit einer von Ihren Steuerungstechnikern definierten Liste zulässiger Befehle (Content Inspection).

Kostenvorteile

- Vereinfachte Konformität mit Standards der Daten- und Betriebssicherheit
- Reduzierte Stillstandzeiten und Produktionsverluste
- Geringere Instandhaltungskosten
- Erhöhte Systemzuverlässigkeit und -stabilität

Merkmale

- Erste Content-Inspection-Applikation für industrielle Protokolle
- Definition zulässiger Modbus-Befehle, -Register und -Coils (Ausgänge) durch Ihre Steuerungsexperten
- Automatische Blockierung und Meldung von Datenverkehr, der nicht Ihren Regeln entspricht
- Plausibilitätsprüfung, blockiert jeden Datenverkehr, der nicht dem Modbus-Protokoll entspricht
- Unterstützung mehrerer Master- und Slave-Geräte
- Einfach Konfiguration und Überwachung mittels Tofino CMP
- Zertifizierung der Modbus-Konformität durch Modbus-IDA

Anwendungen

- Eichpflichtiger Datenverkehr in der Öl- und Gasindustrie
- Sicherheitsmesssysteme
- Management von SPS-Programmierarbeitsplätzen
- HMI-Anzeigeterminals

EAGLE Tofino™ VPN Server und Client

Leicht einzurichtendes VPN-System ohne Sicherheitsrisiken für industrielle Prozesse

Industriebetriebe möchten oft die hohen Geschwindigkeiten von Internet-Verbindungen nutzen, um Steuerungssysteme und/oder Menschen mehrerer Standorte zusammenzuführen. Doch wie lässt sich diese kostengünstige Technologie nutzen, ohne Ihre Steuerungs- und SCADA-Systeme den Risiken von Virenbefall und nicht-autorisierten Zugriffen auszusetzen?
Die Tofino™ VPN-Lösung überlagert unsichere Netzwerke, wie das Internet oder unternehmensweite Firmennetze, mit sicheren „Kommunikationstunneln". Im Gegensatz zu anderen VPN-Systemen lässt sich Tofino VPN relativ einfach einrichten, testen und managen. So wird gute Sicherheit nicht durch Konfigurationsfehler beeinträchtigt.
Tofino VPN unterstützt auch ältere Automatisierungsgeräte und Protokolle und ist industrietauglich. Mehr noch: Für umfassendere Sicherheitslösungen kann es mit anderen Tofino LSM kombiniert werden, wie dem Tofino Firewall LSM oder dem Tofino Modbus Enforcer LSM.

Kostenvorteile

- Reduzierte Telekommunikations- und Reisekosten
- Reduzierte Inbetriebnahme-, Entwicklungs- und IT-Kosten dank einfacher Einrichtung
- Investitionsfreundliche Möglichkeit der Einbindung von älteren Geräten ohne IP-Funktionalität

Merkmale

- Erstellung äußerst sicherer Tunnels mittel SSL-Technologie (Secure Socket Layer) zum Schutz der Integrität von Steuerungssystemen
- Einfache Einrichtung, Prüfung und Verwaltung über Drag-and-Drop-Konfigurationsschnittstelle
- Testen von VPN-Tunneln, ohne Steuerungsdatenverkehr darüber zuzulassen
- Unterstützung ältere Automatisierungsprotokolle
- Nahtlose Interoperabilität mit anderen Tofino LSM für feingranularen VPN-Zugang und SCADA-fähigen Firewall-Schutz

Anwendungen

- Verwaltung entlegener Werke von einem zentralen Standort aus
- Bereitstellung sicherer Zugänge zu Betriebseinrichtungen für Mitarbeiter an entfernten Standorten

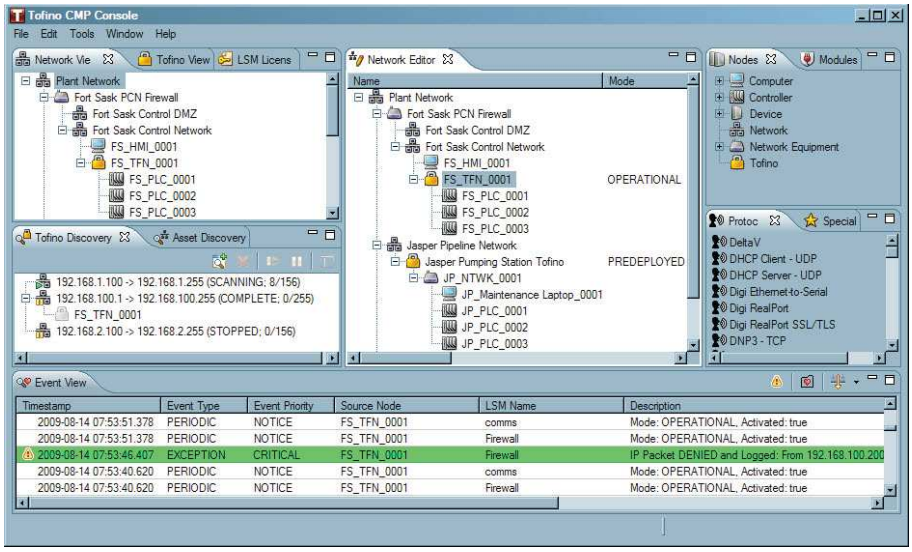
EAGLE20 Tofino™ Security Appliance

Schützen Sie Ihre Steuerungssystem vor Netzwerkproblemen und Cyber-Attacken

Aufgrund der elektrischen, Umwelt- und Betriebsanforderungen von SCADA- und Steuerungssystemen sind IT-orientierte Sicherheitslösungen für den Einsatz in industriellen Netzwerken ungeeignet. Daher wir die überwiegende Mehrzahl dieser Systeme ohne jeden nennenswerten Schutz vor zufälligen oder gezielten, böswilligen Cyber-Attacken betrieben. Schon ein einziger infizierter USB-Stick kann einen komplette Fabrik außer Betrieb setzen.

Der EAGLE 20 Tofino bietet richtungsweise Zone Level Security™, das heißt maßgeschneiderten Schutz für Gruppen von Speicherbaren Steuerungen, verteilten Steuerungssystemen, entlegenen Endgeräten und Bedienpanels gemäß ANSI/ISA-99. Das Gerät kann ohne spezielle Schulung, ohne Vorkonfiguration und bei laufendem Betrieb – also ohne Systemstillstand – in ein Netzwerk installiert und aktiviert werden. Es wurde von Grund auf gezielt für den Einsatz in rauer Umgebung, bei geringen Vorkenntnissen und unter Berücksichtigung industrieller Anforderungen ausgelegt. Der EAGLE 20 Tofino schütz besser und lässt sich einfacher Installieren als IT-Firewalls und andere Sicherheitsprodukte.

EAGLE20 Tofino Security Appliance



Central Management Plattform

Bestelldaten

Bezeichnung	Artikel-Nr.	Produktbeschreibung
EAGLE Tofino Central Management Platform	942 016-100	Central management platform for EAGLE Tofino
EAGLE Tofino Firewall LSM	942 016-110	Firewall Loadable Security Module for EAGLE Tofino
EAGLE Tofino Security Asset Management LSM	942 016-111	Security Asset Management Loadable Security Module for EAGLE Tofino
EAGLE Tofino Modbus TCP Enforcer LSM	942 016-112	Modbus TCP Enforcer Loadable Security Module for EAGLE Tofino
EAGLE Tofino VPN Server LSM	942 016-113	Virtual Private Network Server Loadable Security Module for EAGLE Tofino
EAGLE Tofino VPN Client LSM	942 016-114	Virtual Private Network Client Loadable Security Module for EAGLE Tofino
EAGLE Tofino VPN PC Client License	942 016-116	Virtual Private Network PC Client license for EAGLE Tofino
EAGLE Tofino Event Logger LSM	942 016-115	Event Logger Loadable Security Module for EAGLE Tofino
EAGLE20 Tofino TX/TX	943 987-501	EAGLE20 Tofino: Untrusted port - TX, trusted port - TX
EAGLE20 Tofino TX/MM	943 987-502	EAGLE20 Tofino: Untrusted port - TX, trusted port - MM
EAGLE20 Tofino MM/TX	943 987-504	EAGLE20 Tofino: Untrusted port - MM, trusted port - TX
EAGLE20 Tofino MM/MM	943 987-505	EAGLE20 Tofino: Untrusted port - MM, trusted port - MM

Immer die richtige Lösung

Belden ist ein weltweit führender Anbieter von Signalübertragungslösungen, einschließlich Kabeln, Vernetzungstechnik und aktiven Komponenten, für funktionskritische Anwendungen von der Industrieautomation über Datenzentren und Sendeanstalten bis hin zur Raum- und Luftfahrt. Das Portfolio umfasst eine Vielzahl hoch spezialisierter Produkte für die Leit- wie die Steuerungs- und die Feldebene, die das Unternehmen unter den Markennamen Belden®, Hirschmann™ und Lumberg Automation™ herstellt und vermarktet.

Gern stellen wir Ihnen unsere integrierte Produktpalette für Industrieanwendungen und den weltweiten Belden-Service näher vor. Weiterführende Informationen und technische Daten sind online auf www.beldensolutions.com verfügbar. Oder wenden Sie sich direkt an unser Vertriebsteam: Tel +49 7127 14 1809.

Tel.: +49 (0) 7127 / 14-1809
www.hirschmann.com