HIRSCHMANN
A BELDEN BRAND

New Product Bulletin

NP 1012HE

Hirschmann™ EAGLE Tofino

Zone Level Security™
for your control network

Protect your control system against network problems and cyber threats

You may not be attacked by a serious hacker, but conventional control networks are extremely vulnerable to simple day to day security issues. Poor network segmentation, unprotected points of entry into the network, "soft" targets such as unpatched PCs and vulnerable PLCs, and human error can result in significant production losses and even safety issues.

The Tofino Industrial Security Solution is a distributed security solution that quickly and cost-effectively implements cyber security protection within your control network. Tofino's flexible architecture allows you to create security zones - Zone Level Security - throughout your control network to protect critical system components. Tofino helps you meet and exceed NERC CIP requirements and ANSI/ISA-99 Standards. And best of all, it helps you avoid expensive down time and achieve optimal performance in your plant.

EAGLE Tofino™ Key Benefits

- No IT knowledge required
- Enhanced security and safety
  - Extend Cyber Security down into the control network
- Simplified regulatory and standards compliance
  - FERC / NERC CIP
  - ANSI/ISA-99
  - IEC 62443

HIRSCHMANN
A BELDEN BRAND

Central Management Platform and Loadable Security Modules

Design your security system in four easy steps

Step One:

Determine where to place Tofino Security

Determine where Tofino Security Appliances need to be placed to create Zone Level Security™ for the devices in your network. Note: the ANSI/ISA-99 Standards recommend containing communication in control sub-systems known as "zones".

Step Two:

Determine which Tofino LSMs are required to secure each hardware location

Do you require "radar" sweeping your network to track every existing and incoming device communicating through a specific Tofino Security Appliance? Then load the Tofino Secure Asset Management LSM.
Do you require a "traffic control cop" for industrial networks checking all communications against a list of traffic rules and blocking and reporting traffic that does not match the rules? Then load the Tofino Stateful Firewall Module.
Do you require a "border guard" inspecting every Modbus command and response, blocking and reporting function codes or register addresses not on the "allowed" list? Then load the Tofino Modbus TCP Deep Packet Inspection LSM.
Do you require secure communications "tunnels" over your corporate network or the Internet? Then load the Tofino VPN Client and Server LSMs.

Step Three:

Choose the best server or workstation for the Tofino Central Management Platform

The Tofino Central Management Platform software enables configuration, management and monitoring of all your Tofino Security Appliances from one workstation.

Step Four:

For product and ordering details, go to www.hirschmann.com

EAGLE Tofino™ Central Management Platform

Configure and manage security for your entire control network from one location

Traditional security devices force you to configure them one at a time. This quickly becomes unmanageable as the number of devices increases. What's worse, this device-centric view provides no way to see what is happening at the system level, so diagnosing and correcting security issues is time-consuming, error-prone, and expensive.

The Tofino Central Management Platform (CMP) software enables configuration, management and monitoring of all your Tofino Security Appliances from one workstation.

Using the Tofino CMP you can quickly create a model of your entire control network. Visual drag-and-drop editing tools help you create, edit, and test your Tofino configuration. And, after you commission your security system, the Tofino CMP lets you see the status of the entire system at a glance and respond to cyber threats in a coordinated manner.

Saves you money through:

- Increased network availability
- Rapid network security deployment
- Fast fault finding
- Lower training and staffing costs

Features

- Configure, manage and monitor all Tofino Security Appliances from one workstation
- Built-in Network Editor to quickly model your control network
- Visual drag-and-drop editors for quick and easy configuration of security rules
- Pre-defined templates for more than 50 industrial communication protocols and over 25 families of industrial controllers

Applications

- Process control
- SCADA systems
- Discrete control

EAGLE Tofino™ Firewall

Take control of your network traffic

The vast majority of control networks have little or no isolation between different subsystems. If a device misconfiguration, hardware failure, or virus causes a problem in one part of the network, it can spread throughout the entire network in seconds and bring your whole plant down. Even redundant backup systems can fail simultaneously if their network connections are not protected.
The Tofino Firewall LSM is a traffic control cop for industrial networks, checking all communications on your control network against a list of traffic "rules" defined by your control engineers. Any communication that is not on the "allowed" list will be blocked and reported by the Tofino Firewall.
Traffic rules are created using terms and concepts that are already familiar to control specialists. And, the unique "test" mode of Tofino lets you test your rules without any risk to plant operation.

Saves you money through:

- Simplifying compliance to safety and security standards
- Reduced down time and production losses
- Improved system reliability and stability

Features

- Traffic rules are defined by your control engineer, specifying which devices may communicate using what protocols
- Rule definition is simple using a graphical drag-and-drop editor
- Traffic that does not match the rules is automatically blocked and reported
- Over 50 pre-defined IT and industrial communication protocols
- Over 25 pre-defined controller templates
- Pre-defined "special rules" for advanced traffic filtering and vulnerability protection

Applications

- Isolate critical devices from threat sources
- Separate control network into security "zones", restricting communications between zones
- Protect controllers with known vulnerabilities

EAGLE Tofino™ Secure Asset Management

Securely track network devices and easily create firewall rules

Before you can protect a control system, you need to know exactly what devices are on the network and how they communicate with each other. Seems obvious - but on today's complex systems, getting complete and accurate information about the installed devices and protocols can consume a huge amount of effort without the right tools. Like radar, Tofino's Secure Asset Management (SAM) Loadable Security Module (LSM) tracks every device that communicates through your Tofino Security Appliance. However, it does it without using traditional scanning techniques that cause process disruption. Tofino SAM identifies devices so you can easily create traffic rules using definitions from the Tofino CMP's database. If you need to modify traffic rules during testing, Tofino SAM's rule wizard guides you using data gathered from Tofino's security alerts. After commissioning, Tofino SAM provides ongoing protection by alerting you when new devices are discovered on the network.

Saves you money through:

- Increased reliability due to improved security
- Simplified regulatory and security standards compliance
- Reduced time and effort to get up-to-date inventory lists
- Lower engineering and IT costs due to ease of firewall rule creation
- Reduced commissioning time

Features

- Locates network devices without any process disruption using Passive Asset Discovery
- Identifies equipment and suggests firewall rules using a built-in control device database
- Guides the creation of firewall rules using "blocked traffic" reports and the Assisted Rule Generation wizard
- Reports newly-discovered assets as security alerts
- Provides current and detailed inventory lists

Applications

- Tofino installation, deployment and testing
- ISA-99 and NERC compliance via asset inventory lists and continuous monitoring
- Detection of non-approved devices (e.g. laptops) on the control network

EAGLE Tofino™ Modbus TCP Enforcer

Advanced cyber threat and safety protection for your Modbus devices

Did you know that any device with a network connection to a Modbus controller can potentially change any of the controller's I/O points or register values? Many controllers can even be reset, disabled, or loaded with new logic or firmware.
The Tofino Modbus TCP Enforcer is a content inspector for Modbus communications, checking every Modbus command and response against a list of "allowed" commands defined by your control engineers.

Saves you money through:

- Simplifying compliance to safety and security standards
- Reduced down time and production losses
- Lower maintenance costs
- Improved system reliability and stability

Features

- First-ever application of content inspection technology to industrial protocols
- Control specialist defines list of allowed Modbus commands, registers and coils
- Automatically blocks and reports any traffic that does not match your rules
- Protocol "Sanity Check" blocks any traffic not conforming to the Modbus standard
- Supports multiple master and slave devices
- Simple configuration and monitoring using the Tofino CMP
- Certified Modbus compliant by Modbus-IDA

Applications

- Oil & Gas custody transfer
- Safety instrumentation systems
- Managing PLC programming stations
- Display-only HMI panels
- Partner access to telemetry data
- Quickly and safely identify network devices and define traffic rules

EAGLE Tofino™ VPN Server and Client

A VPN system that is easy to deploy and does not risk industrial processes

Industrial facilities often want to utilize high-speed Internet connectivity in order to integrate control systems and/or people from multiple locations. How can you take advantage of this cost-effective technology without risking viruses or inappropriate access to your control and SCADA systems?
The Tofino VPN solution creates secure "tunnels" of communication over untrusted networks, such as the Internet or corporate business networks. Unlike other VPNs, the Tofino VPN is easy to deploy, test, and manage. This ensures that good security is not compromised because of configuration errors.
The Tofino VPN also supports legacy automation devices and protocols, and is industrially hardened. Best of all, it can be combined with other Tofino LSMs, such as the Tofino Firewall LSM or the Tofino Modbus TCP Enforcer LSM, to provide a comprehensive security solution.

Saves you money through:

- Reduced telecommunication and travel costs
- Reduced implementation, engineering and IT costs due to ease of deployment
- Leveraging investments by enabling communications to legacy non-IP devices

Features

- Creates highly secure tunnels using Secure Sockets Layer (SSL) technology to protect control system integrity
- Easy to deploy, test, and manage with drag and drop configuration interface
- Allows testing of the VPN tunnel without committing control traffic to it
- Supports legacy automation protocols
- Interoperates seamlessly with other Tofino LSMs to provide fine grained VPN access and SCADA-capable firewall protection
- Industrially hardened

Applications

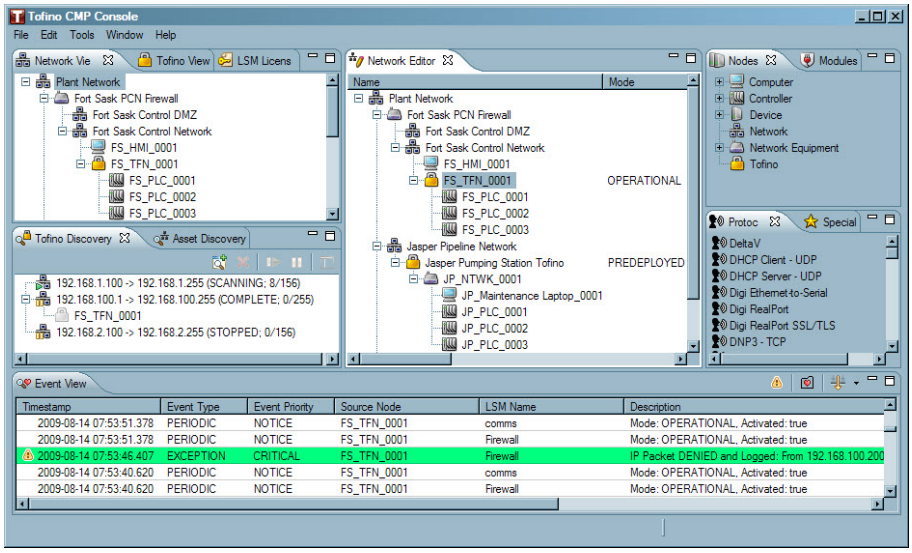
- Manage remote plants from a central facility
- Provide secure access to plant facilities for remote personnel
- Interconnect legacy non-IP equipment
- Secure communications between critical controllers

EAGLE20 Tofino™ Security Appliance

Protect your control system against network problems and cyber threats

The electrical, environmental and operational requirements of SCADA and control systems make IT-focused security solutions unsuitable for use in industrial networks. As a result, the vast majority of these systems are operating with little or no protection against accidental or malicious cyber attacks. Even a single infected USB key can shut down an entire plant.
The EAGLE20 Tofino Security Appliance provides leading-edge Zone Level Security™ - tailored protection for groups of PLCs, DCSs, RTUs and HMIs, as recommended in ANSI/ISA-99 Standards. Tofino can be installed and implemented in a live network with no special training, no pre-configuration, and most importantly, with no system downtime.
Tofino is designed from the ground up with a rugged environment, staff skills and needs of industry in mind, and it protects better and is easier to install than IT firewalls and other security products.

EAGLE20 Tofino Security Appliance



Central Management Platform

Order Information

Designation	Part No.	Product Description
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

Always the right solution

Belden is one of the world's leading suppliers of signal transmission solutions including cable, connectivity and active components for mission-critical applications ranging from industrial automation to data centers, broadcast studios, and aerospace. Belden offers an extensive and highly specialized product portfolio of signal transmission solutions for information, control and field levels, which the company produces and markets under its proprietary Belden®, Hirschmann™ and Lumberg Automation™ brands.

We would welcome the opportunity to tell you more about our extensive industry portfolio and Belden worldwide service. Further information and technical data are available online at www.beldensolutions.com. You can also contact our sales team directly by dialing +49 7127 14 1809.

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