Belden and FireEye Join Forces to Secure Industrial Control Systems Against Sophisticated Cyber Attacks

New partnership brings together leaders in information technology and operational technology to provide trusted solutions for industrial networks

ST. LOUIS and MILPITAS, Calif. **–** Feb. 29, 2016 -- Belden Inc. (NYSE: BDC), a global leader in high quality, end-to-end signal transmission solutions for mission-critical applications, and FireEye, Inc. (NASDAQ: FEYE), the leader in stopping today's advanced cyber attacks, today announced a partnership to provide integrated industrial network security solutions to critical infrastructure providers around the world.

Recent cyber attacks against the Ukrainian grid confirm ICS-CERT reports of a dramatic increase in cyber attacks that penetrate industrial control system networks over the last year and points out that more of these attacks are gaining access to the control system layer of the network. Access to the ICS network layer allows attackers to impact availability, reliability and safety of mission critical infrastructure.

“Industrial control systems are built on technology designed to last for decades that can’t easily be upgraded, patched or replaced with modern systems,” said David DeWalt, chairman of the board and CEO at FireEye. “By bringing FireEye, Belden and Tripwire technology together, we’re able to add advanced detection and visibility from the enterprise edge of the network to the ICS zone, and provide the services necessary to help mitigate an attack before an adversary can take down a key piece of critical infrastructure.”

Integrated Solutions Across The Industrial Network Security Lifecycle

Belden has been a technology leader in mission critical industrial networking solutions for over 100 years. With an industry-leading portfolio of solutions including GarrettCom, Hirschmann, Prosoft, and Tofino, Belden is a trusted partner in every major industrial market. Industrial cyber security continues to be a critical and strategic initiative for Belden as evidenced by their recent acquisition of Tripwire.

“Industrial cyber security is about uptime and safety,” said John Stroup, CEO of Belden. “We are a trusted partner in the industrial market because we understand their unique requirements and focus on delivering effective, pragmatic solutions designed for mission critical systems. Our partnership with FireEye is a natural extension of our cyber security strategy and makes it easier for our customers to protect themselves against the rising tide of ICS cyber attacks.”

FireEye brings to the partnership advanced detection capabilities, targeted threat intelligence, and specialized Mandiant ICS services. From Belden’s cybersecurity portfolio, customers have access to deep visibility, endpoint intelligence and change detection from Tripwire, secure non-invasive network segmentation from Tofino and ruggedized industrial networking solutions from GarrettCom.

FireEye Technology and Offerings

The FireEye MVX Engine
The leading virtual machine-based detection technology, FireEye MVX can be deployed across key points in the infrastructure including networks, email and endpoints and detect attacks in the IT environment that bypass traditional security solutions.

FireEye Threat Analytics Platform (TAP)
FireEye TAP applies threat intelligence, expert rules tailored for ICS environments and advanced security data analytics to event data streams. By collecting security information and events from Tofino, Garrettcom and Tripwire technology solutions from Belden, TAP cuts down the noise of typical security solutions and provides industrial networking situational awareness to improve response times in the event of an attack.

FireEye as a Service (FaaS)
FireEye as a Service experts monitor customers’ FireEye environments around the clock using analysis techniques developed from 100,000+ hours of front-line experience and report back with validated threat information that details the what, when and how of the threat as well as how to respond to it. Customers who establish visibility of ICS environments can deploy the capabilities of FaaS analyst to hunt for attackers targeting ICS.

Mandiant ICS HealthCheck
The Mandiant ICS HeathCheck provides a non-invasive assessment and configuration review for industrial control systems based on both industry best practices and lessons learned from the front lines of incident response investigations. Mandiant experts identify risks such as vulnerabilities,

misconfigurations, and anomalous network communications and provide recommendations for how to address them.

Mandiant Incident Response
FireEye provides specialized services for investigating intrusions and targeted attacks against critical infrastructure providers performed by advanced threat groups. Mandiant consultants use proprietary technology, creative investigative techniques and intelligence gathered during each investigation to identify the actions of the attacker, the scope of the breach, the data loss, and the steps required to remove the attacker's access. The results are used to re-secure the network and inform other FireEye products and services such as FaaS.

FireEye Threat Intelligence
With the recent acquisition of iSIGHT Partners, FireEye is able to deliver nation-state grade threat intelligence to commercial customers who run mission-critical ICS. Though a combination of machine, victim and attacker based collection of data, FireEye is continuously monitoring for intelligence and indicators of compromise against critical infrastructure providers that informs both detection and response capabilities in the integrated Belden-FireEye solution.

Belden Technology and Offerings

Tripwire Enterprise - Proactive Endpoint Monitoring
Continuously monitors infrastructure and endpoints in order to provide deep visibility and intelligence on changes. Sophisticated analysis of baseline system behaviour makes it possible to identify and remediate high-risk and unauthorized changes that are the hallmark of a breach in progress.

Tripwire Configuration Compliance Manager (CCM)
Delivers continuous active and passive scanning to discover and audit the configurations of systems, applications, firewalls, routers and switches. CCM utilizes an agentless architecture enabling deployment across a broad range of systems where it is not possible to install an agent.

Tripwire IP360 – Risk based Attack Surface Reduction
Using a predictive risk model IP360 builds a heat map of vulnerabilities found on critical assets, ranking them by severity and likelihood of exploitation. This approach provides a triage of defensive measures necessary to proactively defend critical assets. System criticality and vulnerability severity can also be used proactively to increase the level of monitoring and logging of critical endpoints.

Tofino
The Tofino Xenon Security Appliance and its Plug-n-Protect™ technology is designed to protect special purpose industrial networks by ensuring only required protocols and expected traffic flows through to controllers. Tofino appliances are extremely ruggedized and are designed to deliver reliable industrial network segmentation for maximum protection.

GarrettCom
GarrettCom provides ruggedized industrial networking switches, routers and media converters for specialty and stressed applications. It is designed for harsh external environments and is purpose built for the specific needs of the energy and utilities.

For more information on the FireEye-Belden partnership, visit:
https://www.fireeye.com/partners/strategic-technology-partners/belden-and-fireeye-partnership.html

About Belden

Belden Inc., a global leader in high-quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis and has manufacturing capabilities in North and South America, Europe and Asia. For more information, visit us at www.belden.com; follow us on Twitter @BeldenInc.

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 4,400 customers across 67 countries, including more than 680 of the Forbes Global 2000.

Belden Media Relations contact:
Shelley Boose
(408) 398 6987
SBoose@tripwire.com

FireEye Media Relations contact:
Vitor De Souza
(415) 699-9838
vitor.desouza@FireEye.com

FireEye Investor Relations contact:
Kate Patterson
(408) 321-4957
kate.patterson@FireEye.com