SOLUTION BRIEF

FireEye

Waterfall Unidirectional CloudConnect® with FireEye Helix and FireEye Managed Defense

HIGHLIGHTS

- Identify high-risk activity in industrial networks in real time
- Prioritize alerts based on enterprise-wide, cross-site industrial and enterprise correlations
- Use an in-house or FireEye security team with a consolidated, comprehensive view of enterprise and industrial networks and security conditions
- Serve as the foundation of both Industrial Internet of Things (IIoT) and traditional defense-in-depth industrial security programs and network designs
- Dramatically simplify compliance with industrial cyber-security standards and best-practice guidance, including NERC CIP, NRC 5.71, NEI 08-09, ANSSI, NIST 800-82, IEC 62443

Waterfall Security Solutions and FireEye have partnered to integrate the cloud-based FireEye Helix and FireEye Managed Defense solutions with reliability-critical and safety-critical industrial control system (ICS) networks. Populating these offerings with live data from ICS networks via Waterfall's Unidirectional CloudConnect enables security analysts and audit teams to identify and respond to critical security incidents. The integrated solution also helps ICS owners and operators be confident that even sophisticated attacks won't impair operation of critical systems.

ICS security best practices emphasize the importance of a defense-in-depth security strategy that requires monitoring and analyzing security conditions on ICS networks in real time. It is often unrealistic and cost-prohibitive for owners and operators to deploy cyber security experts at every industrial site. But potential security problems from simple errors and omissions to sophisticated attacks must still be monitored and analyzed. Logs, alerts, network traffic and other security relevant information must be reliably and securely transmitted to a centralized security operations center (SOC) for expert analysts to see, understand and act upon. While the connections that enable such communications offer certain security benefits, they often introduce additional attack paths and failure modes.

Waterfall Security Solutions and FireEye provide industry-leading cloud-based threat detection for the most sensitive industrial networks. Waterfall offers Unidirectional CloudConnect and a decade of experience deploying their world-leading unidirectional gateway technology at many industrial sites. FireEye offers the industry-leading cloud-based Helix security monitoring and analysis platform with the option of 24x7 FireEye expert support to secure industrial systems.

WATERFALL®
Stronger Than Firewalls

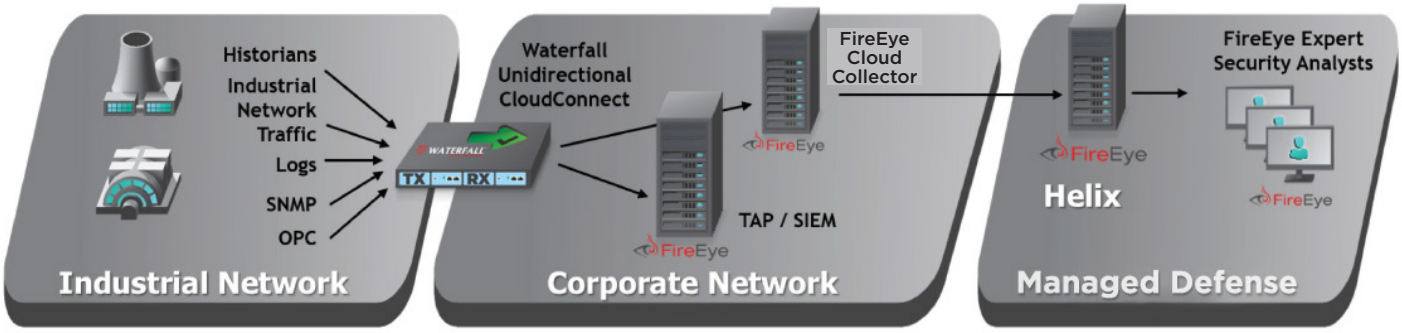

Figure 1. Solution overview.

Waterfall Unidirectional CloudConnect

Waterfall's Unidirectional CloudConnect offers a secure, effective way to provide visibility into ICS networks for FireEye monitoring and analytical tools. Unidirectional CloudConnect hardware can physically transmit information in only one direction from the protected ICS network out to external IT, Internet and cloud networks. It has achieved Common Criteria EAL 4+ certification. Designed specifically to work with even the most sensitive industrial equipment, it helps ensure that even sophisticated external network attacks are less likely to defeat this physical protection to enter the industrial network.

FireEye Helix and Managed Defense

An organization's security team can gain unified, real-time visibility into its ICS networks with the joint FireEye and Waterfall solution and compare situations, threats, incidents and intelligence between sites, organization-wide.

FireEye Helix is a comprehensive monitoring, detection, analytics and response platform designed to simplify, integrate and automate security operations. FireEye understands cyber attacks better than anyone else, and applies that knowledge to remove complexity from security. FireEye's intelligence-led approach builds on the innovative security technologies, nation-grade FireEye iSIGHT Intelligence and world-renowned expertise from Mandiant, a FireEye company.

FireEye Managed Defense is a managed detection, investigation and response service that minimizes the potential business impact of increasingly sophisticated and targeted cyber-attacks. A FireEye team of experts with deep knowledge of both IT and ICS environments monitor, analyze and respond to your entire enterprise, enabled by the partnership between Waterfall and FireEye. The FireEye team of expert threat analysts monitors your environment with the latest intelligence and proprietary hunting methodologies to systematically search for signs of compromise. When an alert is triggered, FireEye threat analysts investigate to determine the extent of the compromise by inspecting the network traffic and endpoints. Using FireEye intelligence, expert analysts can identify the timeline across the kill chain to reveal when and how an attack occurred, who was behind it and what the attack was targeting. New intelligence is generated in part by FireEye technologies, which perform more than 50 billion virtual machine analyses and process 400,000 unique malware samples each day.

Secure and Reliable ICS Integration

Waterfall's CloudConnect extends FireEye's visibility for Helix and Managed Defense into industrial networks. The CloudConnect securely interacts with sensitive safety-critical, reliability-critical industrial networks, and makes security insights from those networks available to FireEye services. FireEye Helix correlates this information with other threat intelligence, real-time information connected from other industrial sites, and from throughout an enterprise, to identify the most critical security threats. Managed Defense applies FireEye's expert industrial and enterprise cyber security analysis to analyzing, interpreting and acting on security situations.

The joint solution from FireEye and Waterfall:

- Provides enterprise-wide, real-time visibility to identify and investigate critical security threats associated with industrial processes and activities
- Enables enhanced forensics analysis and evidence collection by drilling-down into industrial cloud datasets to understand the true nature and scope of a security event
- Provides a method to move critical ICS security data out of the ICS network, which guarantees the protection of industrial networks from attacks originating on external networks
- Is the foundation of a sound, industrial defense-in-depth plan, as recommended by and required by national authorities and international standards bodies, worldwide
- Supports emerging IIoT deployments, as well as traditional ICS network designs

Waterfall gives the FireEye team the vital ICS operational and security information they need to integrate industrial operations and networks into holistic security views and decisions.

Standard and Best Practices

Together, the joint Waterfall and FireEye solution helps companies achieve of the defense-in-depth security posture recommended by industrial cyber security best practices, standards and regulations worldwide. For example:

- North American NERC CIP standards for security in the bulk electric system recognize the strength of safe integration with unidirectional gateway technology and require real-time monitoring of intrusion detection systems on important sites in the electric system.
- French ANSSI standards recommend both unidirectional connectivity and real-time monitoring of intrusion detection systems for important industrial networks and require such approaches for the most important networks.
- U.S. and Canadian nuclear generation cyber security regulations forbid firewalls and permit only unidirectional connectivity into safety-critical and reliability-critical networks and require intrusion detection and real-time monitoring of detection systems for such networks.
- NIST 800-82, ISA/IEC 62443, the Industrial Internet Consortium (IIC) Security Framework and many other standards and best practice guidance documents also recognize the value of both safe, unidirectional IT/OT integration and real-time insights into cyber security alerts and situations at industrial sites.

Summary

The partnership of Waterfall Security Solutions and FireEye enables organizations to focus their efforts and resources on identifying the most significant risks to their highest priority enterprise and industrial systems. The joint solution supports a safe and comprehensive approach that provides cloud-based unified visibility into industrial operations for centralized, expert security monitoring and analysis. This monitoring and analysis can be conducted by in-house staff or with FireEye Managed Defense. The joint solution effectively arms an organization with the information needed to identify and respond to the most critical incidents enterprise-wide, and meets demanding enterprise and industrial security compliance requirements.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye helps eliminate the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

About Waterfall

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases and protocols in the market. For more information, visit www.waterfall-security.com

WATERFALL®
Stronger Than Firewalls

FireEye®