SOLUTION BRIEF

FireEye

Waterfall Unidirectional Security Gateway with FireEye Network Security

HIGHLIGHTS

- Provides a way to move any type of structured or unstructured data into highly secure, sensitive networks
- Identifies and blocks known attacks with both signature-based and intelligence-based intrusion detection with Intelligence-Driven Analysis (IDA)
- Identifies and blocks never-seen-before malicious files with the signature-less Multi-Vector Virtual Execution™ (MVX) engine
- Provides protection against data leakage from the protected network with Unidirectional Security Gateways

Waterfall Security Solutions and FireEye are teaming together to protect critical government and law-enforcement networks from the most advanced cyber threats. The joint solution integrates FireEye Network Security with Waterfall's Unidirectional Security Gateways. It enables critical government networks to collect data from multiple untrusted sources securely. The joint solution combines powerful, proven technologies to filter content, intercept malware and help physically prevent information from leaking to less-trusted networks.

Malware and Data Leakage

Federal, state and local law enforcement and governmental agencies operate vital networks. These important networks are used to track investigations, gather intelligence, authorize sensitive decision processes and analyze, manage and coordinate critical logistics. These networks contain highly sensitive data along with command, control and analysis systems for national security and law enforcement investigations. These networks typically need to quickly and securely consume large volumes of data.

Sending information into such networks presents two challenges. First, the information entering the network must be free of malware that might impair the operation of the network or exfiltrate sensitive information. Detecting incoming malware can be very difficult when the malware exploits zero-day vulnerabilities, changes frequently or has been custom-developed for a specific attack. Second, essentially all firewalled connections used to send information into sensitive networks are vulnerable to software-based, social-engineering and other types of sophisticated attacks that can result in the loss of sensitive information.

WATERFALL®
Stronger Than Firewalls

FireEye Network Security and Waterfall Unidirectional Security Gateways

FireEye Network Security uses the MVX engine and IDA to protect networks by detecting and quickly stopping advanced, targeted and evasive attacks. MVX is a signatureless, dynamic engine that inspects suspicious traffic to identify attacks that evade traditional signature- and policy-based defenses. IDA is a collection of contextual, rule-based engines that detects and blocks malicious activity based on the latest machine, attacker and victim intelligence.

Waterfall Unidirectional Security Gateways are a combination of hardware and software. The gateway hardware can physically transmit information in only one direction, into the sensitive, protected network, thus helping prevent data leakage. The gateway is physically unable to send any signal or message back into less-trusted networks. Unidirectional Gateway software integrates with FireEye Network Security deployments to transmit content analyzed by Network Security into protected networks.

Waterfall's Unidirectional Gateways have achieved Common Criteria EAL 4+ certification and are trusted by organizations around the world to secure sensitive industrial networks, such as nuclear reactor control networks and railway switching systems, as well as government, law enforcement and intelligence networks.

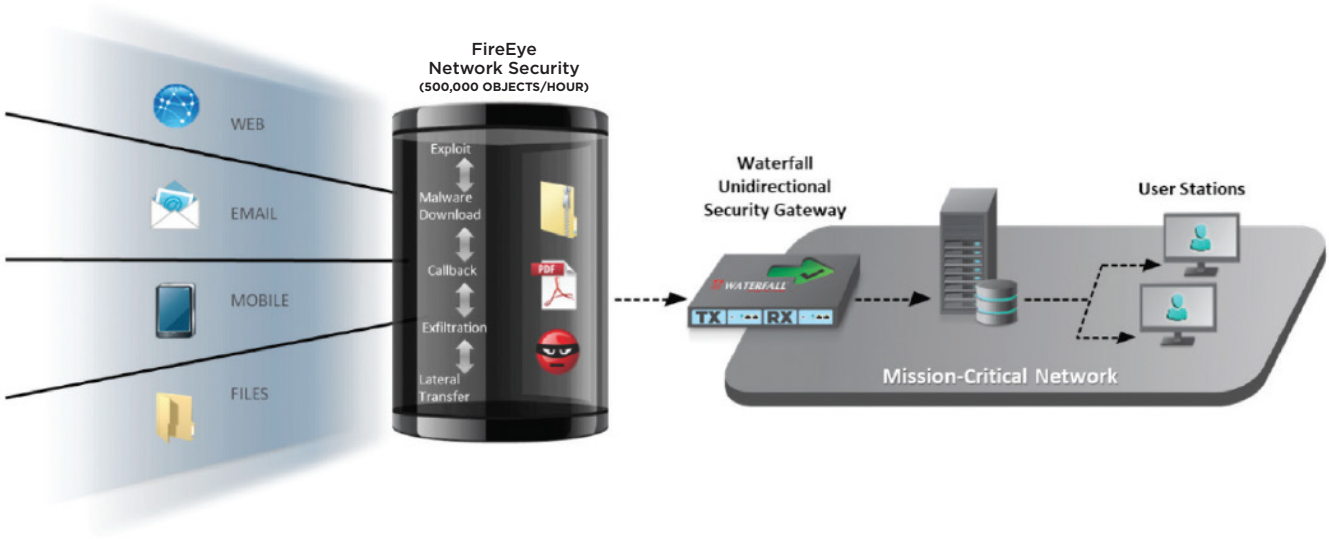

Figure 1. Joint solution from FireEye and Waterfall for mission-critical networks.

Summary

This joint solution from FireEye and Waterfall provides organizations with a way to securely import large volumes of data into their most important and mission-critical networks. Agencies can feel confident that the joint solution provides robust and preventative protection from malware from and data leakage to less-trusted networks.

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®