Miercom

Lab Testing Summary Report

March 2010

Report 100331

Product Category:

Email Security Appliance

Vendor Tested:

WatchGuard

Product Tested:

XCS 570 Appliance

Miercom PERFORMANCE VERIFIED™

Key findings and conclusions:

- **WatchGuard XCS 570 platform blocked 99% of spam when a live production email stream was used**
- **99.3% of infected email attachments were detected**
- **XCS 570 registered only four false positives in a one-week deployment without training or tuning the spam filter**
- **WatchGuard ReputationAuthority rejected 90% of unwanted traffic at the connection level, increasing network performance**

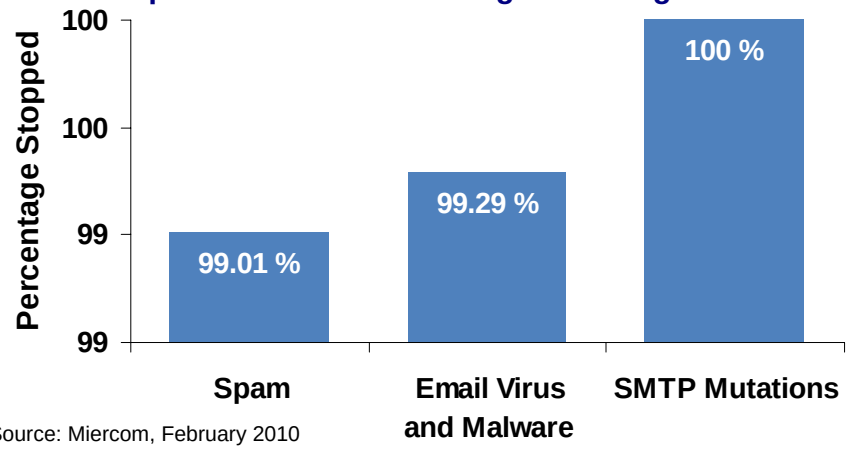
WatchGuard Extensible Content Security XCS 570 appliance was evaluated by Miercom as part of an ongoing assessment of email security products. We analyzed the effectiveness of the appliance based on content-analysis accuracy, and email virus and malware detection. The appliance combines multiple email protection capabilities in one platform to protect the network against spam and email-delivered threats. The XCS 570 is designed for small business to mid-size enterprises of up to 1,000 users and can process up to 40,000 email messages per hour.

Testing was conducted with a live production email stream receiving approximately 3,000 emails per day. Offensive security tests included email virus and malware tests, and SMTP mutations. The WatchGuard XCS 570 was deployed in an out-of-the-box configuration, without any quarantine conditioning or training of the spam filter. The following sections describe the results obtained from the specific tests.

Spam Filtering Effectiveness

To measure the percentage of spam caught and the number of emails incorrectly identified as spam, we evaluated the spam email block rate and content analysis precision of the XCS 570. The appliance was deployed in a live production email environment using an incoming email stream consisting of 90% spam. The balance was legitimate email and legitimate email with spam characteristics.

Figure 1: WatchGuard Extensible Content Security XCS 570 Spam and Threat Blocking Percentages



Source: Miercom, February 2010

The WatchGuard XCS 570 blocked 99% of spam, 99.3% of archived virus attachments and recorded no faults when attacked with SMTP mutations.

Test results showed that the WatchGuard XCS 570 blocked 99% of spam and registered only four false positives when placed in a live production environment without training or tuning. By using WatchGuard ReputationAuthority technology, 90% of the spam was rejected at the connection level. Rejecting spam at this level, WatchGuard ReputationAuthority serves as a perimeter security device, keeping email-delivered threats from entering the network and eliminating the need to process and archive unwanted traffic.

Email Virus and Malware Protection

With the constant emergence of new threats and attack vectors, email security solutions need to maintain a database with frequent updates and stay current with the tools and techniques being used. To ensure that the WatchGuard appliance could defend a network from the latest email threats, we tested the XCS 570 with a mix of Win32 malware samples, zero day and in the wild viruses. These were archived, compressed and emailed as 5 MB attachments. Over 100,000 samples of malware were used to complete this test scenario.

Virus-infected emails from our Linux-based attack platform were originally rejected by WatchGuard ReputationAuthority due to missing MX records, before being scanned by the anti-virus engine. In addition, the threat prevention feature that determines the threat level of connecting to an IP address using historical statistics, blocked our attack emails after receiving ten infected emails. In order to make an accurate evaluation of the appliance's anti-virus engine, WatchGuard ReputationAuthority and Threat Prevention were disabled during this phase of anti-virus testing.

The XCS 570, employing the Kaspersky anti-malware engine, achieved a block rate of 99.3% against archived viruses and malware sent as email attachments. Even after disabling the ReputationAuthority and Threat Prevention features, this block rate was maintained. See *Figure 1 on page 1*.

SMTP Mutations Analysis

Our analysis included highly specific, stateful test cases that were built based on the state, structure and semantics of protocols, as well as their interdependencies on other protocols. Secure and robust targets should handle protocol mutated packets by either dropping them or sending an error message, but an insecure target with protocol implementation flaws would respond abnormally or not at all. Miercom has observed in other test cases minor interruptions in legitimate traffic to complete appliance reset or lock-ups from mutation attacks.

Our SMTP mutation attack consisted of 43,700 different stateful and stateless variants and attack vectors. Each variant/attack vector carried a single protocol mutation directed at the XCS 570. The different variants were implemented for SMTP Banners, DATA, EHLO, HELO, MAIL FROM, and RCPT- TO messages.

All attack vectors were handled successfully and no faults were reported. The XCS 570 detected and rejected all mutated packets and non-compliant messages and actively scanned each SMTP header for malformed and inappropriate content.

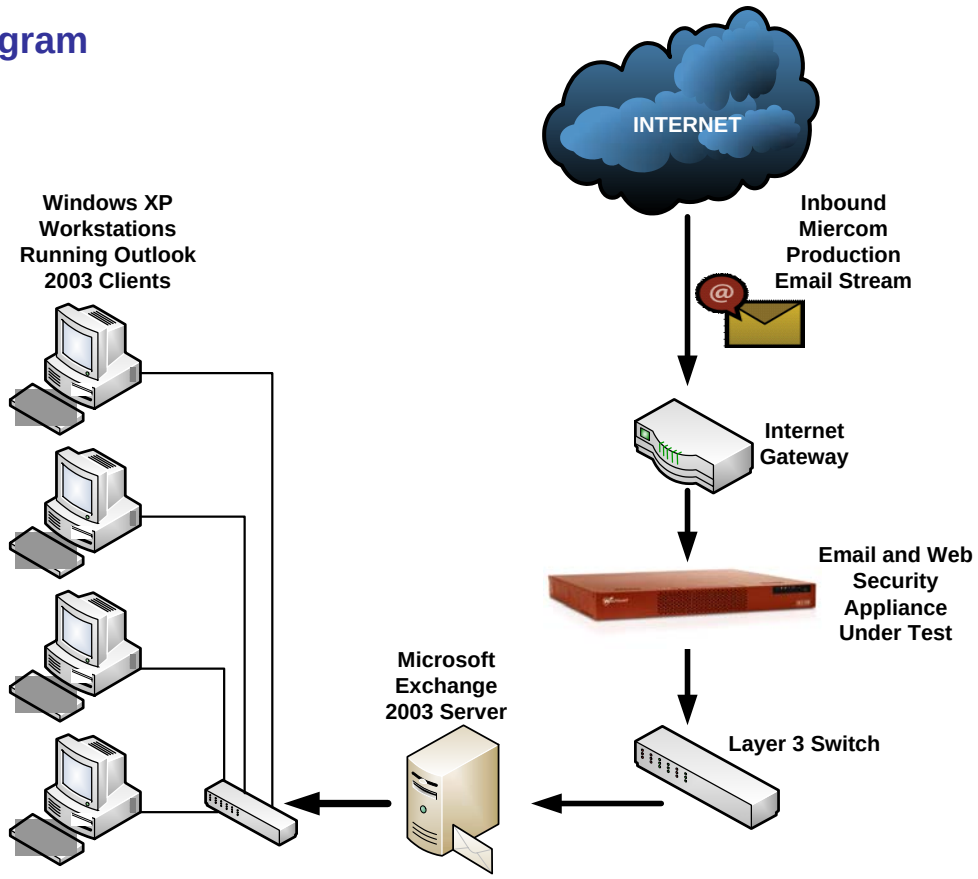
Privacy and Compliance

A noteworthy feature of the XCS 570 is prevention or thwarting of phishing attempts. The XCS 570 supports Data Loss Prevention (DLP) with its ability to automatically block, quarantine, reroute, Bcc or allow messages based on user-defined policies. For digital security standards, the XCS 570 includes predefined regular expression for matching patterns of text. Several default credit card types are provided that allow the administrator to search for these patterns in incoming and outgoing messages and attachments. Miercom engineers observed that the XCS 570 supports email encryption, as an optional add-on, securing confidential messages to any recipient. Through data discovery and classification profiling, the system trained itself on what to look for and what actions to take when such data was discovered in an outbound connection.

Bottom Line

Test results demonstrated the WatchGuard XCS 570 provides enterprise class email security services to defend businesses against spam and email-borne threats. By rejecting unwanted email at the connection level, ReputationAuthority serves as a front line defense to keep spam, threats, undeliverable mail and network attacks from entering the network. Employing over two million signatures and utilizing the best of breed Kaspersky anti-malware engine, the XCS 570 has an extensive virus and malware database to protect a network from electronic threats.

Test Bed Diagram



How We Did It

All testing was conducted at Miercom Labs in New Jersey. The WatchGuard XCS 570 appliance was deployed in an out-of-the-box configuration without tuning or training the spam filter, and without any quarantine conditioning. The appliance was deployed in a production environment receiving 3,000 to 4,000 emails per day. This type of deployment was essential to accurately evaluate the behavior and performance of the product when deployed in an enterprise network. Once the messages were received, each was manually read and classified as spam or legitimate email. The spam blocking percentage and the total number of false positives was calculated.

To test for email malware detection capabilities of each product, we used automated scripts to send tens of thousands of emails with archived virus attachments. The attachments were not more than 5 MB in size with the XCS 570 platform configured to receive attached files no larger than 10 MB. Filtering by attached file type or extension was disabled to record the accurate malware detection proficiency of the device. The WatchGuard XCS 570 platform was tested with 106,030 samples of malware and viruses, including zero day and in the wild viruses.

We used the Mu Test Suite by Mu Dyamics (www.mudynamics.com) to perform security effectiveness assessments. This program was employed to conduct SMTP scans and mutation analyses with thousands of variations on valid service-level traffic.

The Ixia (www.ixiacom.com) IxLoad was used to generate SMTP traffic during vulnerability testing of the WatchGuard XCS 570. IxLoad is a scalable solution for testing converged multiplay services and application delivery platforms. IxLoad emulates data, voice, video and protocols for performance testing.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measuring equipment. Contact reviews@miercom.com for additional details on the configurations applied to the system under test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study, and test specifically for the expected environment for product deployment before making a selection.

Miercom Performance Verified

Based on our assessment of email security products, the WatchGuard XCS 570 is awarded Performance Verified for its ability to detect spam and infected attachments, as well as SMTP mutated packets.

Using its out-of-the-box configuration, the XCS 570 blocked spam, virus and malware attachments, and prevented SMTP mutation attacks from entering the network.

This enterprise email security appliance offers superior filtering capabilities that allow only safe email traffic to an email server.

WatchGuard XCS 570

WatchGuard Technologies, Inc.
505 Fifth Avenue South
Seattle, WA
1-800-734-9905
www.watchguard.com

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report. Consult with professional services such as Miercom Consulting for specific customer needs analysis.