Trend Micro Cloud Edge 70
Competitive UTM Assessment

11 January 2017

Miercom
www.miercom.com

Contents

Executive Summary

Unified Threat Management (UTM) systems are designed to have the protection of a firewall and other security functions in a single system. Many UTM vendors will boast about either high performance or security numbers on their datasheets, but an accurate analysis of both these factors is required in a real-world deployment scenario.

There usually is a trade-off: high performance with low security, or high security with lower performance. The balance is important in a network and should evaluate constraints such as service provider bandwidth caps or stringent network policies. This report reviews multiple UTM products for their ability to handle security attacks while maintaining a reasonable performance so they are useful in a high traffic environment.

This January 2017 Industry Assessment was commissioned by Trend Micro as part of an ongoing study of UTM capabilities. Miercom has independently and comparatively tested the Trend Micro CE70, Dell SonicWall TZ300 and Fortinet FortiGate 50E UTM products in October 2016. Our objective was to run security, performance and subjective out-of-box assessments of the UTM products, identifying the areas of strength and weakness. Additionally, we looked at the unique features of the Trend Micro CE70 for its cloud-based capabilities which set it apart from physical, local-only devices.

Key Findings of the Trend Micro CE70

- Stateful HTTP throughput performance, performed over WAN to LAN, was the highest of all vendors for Application Control, Intrusion Prevention System, Antivirus and UTM
- Highest UTM performance at 471Mbps, 24% higher than its closest competitor
- Malicious URL detection determined 97% of samples were harmful
- All malware samples found over HTTP were equally identifiable with both encrypted HTTPS transport and email protocols, where some other vendors saw a degradation in detection efficacy

Robert Smithers

CEO

Miercom

Test Summary

The following tables summarize the results of testing.

Table 1: Summary of UTM Security Results

Tests			Vendors		
Security Efficacy (% blocked)		Page	Trend Micro CE70	Dell SonicWall TZ300	Fortinet FortiGate 50E
Malware	Active Threats	11	91	92	84
	AET	11	100	100	11
	APT	11	97	95	94
	Botnet	11	90	81	90
	Legacy	11	100	87	97
	Malicious Docs	11	72	88	51
	RATs	11	70	80	100
Email	Malware	12	89	89	75
HTTPS	Malware	13	89	84	72
URLs	Malicious URLs	15	97		95

≥85% 50-84% ≤50%

Table 2: Summary of UTM Performance Results

Tests			Vendors		
Performance (Mbps)		Page	Trend Micro CE70	Dell SonicWall TZ300	Fortinet FortiGate 50E
UTM with Stateful Traffic	FW Only	17	820	847	1019
	FW + AppCtrl	17	820	372	494
	FW + AppCtrl + IPS	17	606	360	467
	FW + AppCtrl + AV	17	615	364	166
	FW + AppCtrl + IPS + AV	17	471	360	160

Highest Lowest

Introduction

UTM devices are the latest, evolving class of network edge security platforms which incorporate and perform multiple security functions in a single appliance. UTM devices perform similarly to Next Generation Firewalls and Secure Web Gateways, but are designed for small and mid-sized businesses.

When considering a UTM device, there needs to be a balance between network performance and security. As the security effectiveness increases, throughput performance may worsen. By testing both security and performance, these results provide an intelligent comparison of security versus performance.

The devices tested for this report include, at a minimum, four security functions: Firewall, Intrusion Prevention System, Application Control and Antivirus. These key security features are found in UTM products and are described in detail below.

Security Function	Acronym	Description
Firewall	FW	Controls and filters the flow of traffic, providing a relatively low-level barrier to protect a trusted internal network from an unsecure network (Internet)
Intrusion Prevention System	IPS	Monitors all network activity, looking for malicious behavior based on known-threat signatures, statistical anomalies, or stateful protocol analysis. If malicious or highly suspicious packets are detected, they are identified, logged, reported and, depending on IPS settings, automatically blocked from access to the internal network.
Application Control	AppCtrl	Enforces policies regarding security and resources (network bandwidth, servers, etc.) by restricting or controlling which application traffic can pass through the UTM, usually in either direction. Security-wise, Application Control is intended to reduce occurrences of infection, attacks and malicious content.
Antivirus	AV	Prevents, detects and removes malicious software, viruses, spyware and other online threats.
Unified Threat Management	UTM	An all-inclusive security setting, where multiple functions are performed by the same, single security device. The functions typically include: firewalling, IPS, AV, VPN (control of virtual private network tunnels), content filtering, and data loss prevention.

The firewall scanning passing traffic is the most basic form of protection. By enabling security features, a degradation of performance is expected on the firewall throughput rate. Throughput is one metric, however security efficacy enables a better real world picture of the true capability of the product.

How We Did It

Miercom's hands-on testing replicates real-world threat environments, to challenge and provide a realistic assessment of a product's security efficacy and performance.

Testing identified the strengths and weaknesses of each device under test (DUT). In addition to traffic patterns and attacks provided by our test tools, we used our unique, verified malicious samples for a more customized, open source approach. High detection efficacy against this blend of malicious samples indicates well-rounded protection from multiple attack vectors.

Security Efficacy

Malware

Malware samples were delivered to a target host, protected by an End Point Protection (EPP) solution to verify each sample as malicious. The EPP solution was for verification purposes only.

Once verified, samples were delivered to an unprotected target host in the test network in which the DUT was deployed. The amount of samples detected and blocked was recorded. Missed samples were saved for later analysis.

The DUT was configured to scan all email messages for malicious content and attachments. Using a new mail account, email messages with malware attachments were sent to an unprotected target within a network where the DUT was deployed. Malware that was identified and/or blocked was recorded. The amount of samples detected and blocked was recorded. Missed samples were saved for later analysis.

Encrypted traffic with malware was sent through all DUTs, and the amount of malicious files found was recorded for each. Missed samples were saved for later analysis.

URLs

Malware samples were delivered to a target host, protected by an EPP solution. Samples were verified as malicious and delivered to an unprotected target host with the DUT. The amount of samples detected and blocked was recorded. Missed samples were saved for later analysis.

Performance

This review is based on the individual connection to WAN. Each DUT was deployed in-line with a single port pair, with egress to WAN and ingress to LAN.

Note: The datasheets of each product may not reflect the throughput results found in this report due to amount of ports used. Some products are capable of more than a single port pair, but we tested this ratio since it is more realistic. Any discrepancy between observed and published data is a result of this implementation.

Before running performance tests, we verified the flow of normal traffic through the DUT to identify interruptions after attacks were implemented. Using a client server, there were 50 clients requesting a download from 50 servers. Traffic was bidirectional.

To verify a client:

1. Connect via Active Sync (if required)
2. Send test email message and verify received.
3. Send test email with payload and verify received.
4. Send test email with malware and verify 10 out of 10 samples caught using EPP software.

Stateful Traffic

Layer-7 HTTP traffic was sent through the network using the Ixia BreakingPoint traffic generator to determine the forwarding rate of the UTM with various features applied.

Prior to testing, we use Ixia BreakingPoint Strike to verify both IPS and AV functionality. The throughput recorded is the maximum forwarding rate before packet loss occurs.

Performance is recorded for:

- FW
- FW+AppCtrl
- FW+AppCtrl+IPS
- FW+AppCtrl+AV
- UTM

From this, we determined the performance degradation on the network and the impact caused by deploying the additional features.

Test Tools

Traffic Generation

Ixia BreakingPoint Firestorm 20 generated traffic, representing a real-world, high-stress network scenario of client to server connections using high-density ports supporting stateful traffic. BreakingPoint can simulate over 200 applications and more than 35,000 live security attacks. The Firestorm performs complex simulations to test throughput of network security appliances.

Attack Generation

Ixia BreakingPoint optimizes security devices by simulating over 35,000 live security attacks and more than 100 invasions. By sending a mixture of application traffic and malicious traffic, this tool determines the ability of the IPS and AV system to detect threats and remain resilient while exposed to vulnerabilities, worms and backdoors.

BreakingPoint "Strike" uses variants, or randomized combinations of paths, to exploit. Dynamic, or "smart", exploits used are from 2010 or later. A default "Strike List" can be used to exploit hosts and applications, but lists can be customized for more specific scenarios.
This attack suite contains:

- Over 6,000 strikes (SQL injection, cross-site scripting, buffer-overflow)
- Natively implemented, as opposed to capture replay
- Over 100 evasion techniques to hide attack from security
- Over 30,000 malware
- Layer 2 through 4 DDoS in parallel with application traffic
- Fragmentation, flood and DNS reflection attacks

BreakingPoint "StackScrambler" performs fuzzing attacks by sending malformed IP, TCP, UDP, ICMP and Ethernet packets to the security device to test protocol stack. Parts of the packet are modified to represent corrupted data.

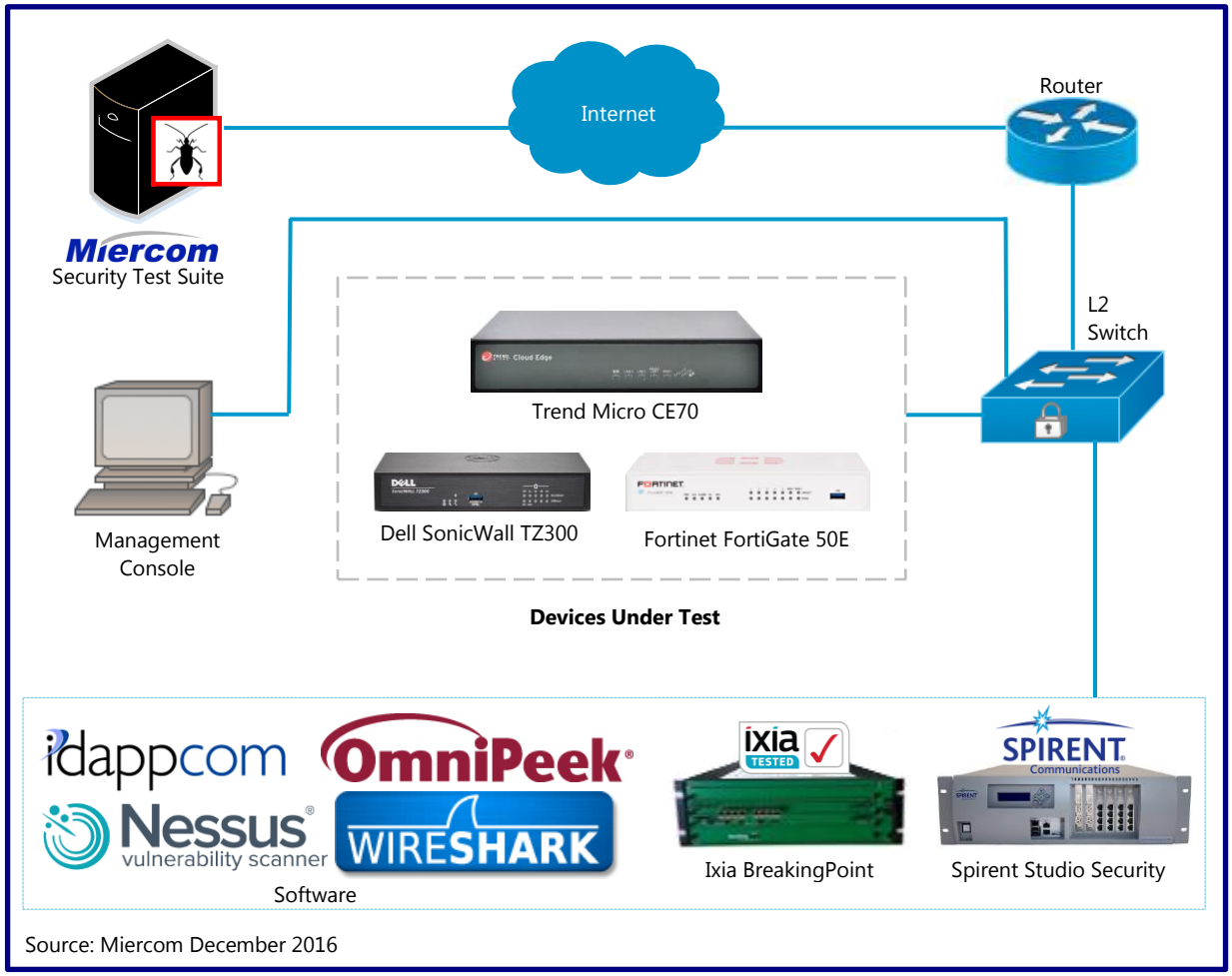
Spirent Studio Security is an attack-generation system software loaded on a Spirent Mu-8000 version 6.5.2.r48322 appliance to produce DoS attacks, mutations and other attack files. The Mu analyzer provides a complete service assurance solution for determining the reliability, availability and security of IP-based applications and services by generating protocol mutations and attacks. It also recreates many published vulnerabilities and external attacks using real-world test cases and custom scripts. This analyzer supports remediation of software flaws by providing actionable reports with complete data on any faults found.

Capture Sampling

Savvius OmniPeek captures network traffic and creates packet files for replay. Statistics can help monitor changes in real-time. By baselining normal activity, changes can be observed to analyze problem areas in the network.

Wireshark creates and analyze packet captures. It calculates application and network response times, data and network volume for over 1,200 applications.

Test Bed Overview



Source: Miercom December 2016

Test Tool/DUT	Version
Ixia BreakingPoint	3.5.0
Spirent Studio Security (Mu-8000)	6.5.2.r48322
Trend Micro Cloud Edge 70	3.8.1090
Dell SonicWall TZ300	SonicOS Enhanced 6.2.3.1-19n
Fortinet FortiGate 50E	v5.4.1 build 1064 (GA)

Security Efficacy

The DUTs were deployed in a simulated network which represented a real-world scenario of switch, firewall and endpoints. The device acted as an intermediary between untrusted and trusted zones. An attacker was sourced in the untrusted zone and attempted to deliver malware to targets within the trusted zone in order to establish communication. Each product was evaluated for its ability to block all attempted exploits and malicious activity.

Common malware were botnets, legacy, malicious documents and RATs. An emphasis was placed on Active Threats, AETs and APTs which were more complex and challenging to block. Detection results reveal individual approaches to stop different malware types.

Testing focused on detection efficacy of the following:

- **Active Threats** Complex, polymorphic malware evading detection and exploiting vulnerabilities. These unknown malware files are constantly changing and taken from external resources and private honeypots. These undetected persistent threats have undergone antivirus evasion techniques such as encryption, black packaging and payloads using normal traffic.
- **Advanced Evasion Techniques (AETs)** Combined evasion tactics that create multi-layer access
- **Advanced Persistent Threats (APTs)** Continuous hacking with payloads opened at admin level
- **BotNet** Communicating programs that collectively spam and deliver DDoS attacks
- **Legacy** Variants of known malware older than 30 days (e.g. virus, worms)
- **Malicious Documents** Mix of Microsoft and Adobe documents with Macro viruses, APTs, worms
- **Remote Access Trojans (RATs)** Trojans disguised as legitimate software, remotely control victim

Different protocols were used to examine each UTM product for its security efficacy: FTP, HTTP, HTTPS and SMTP-IMAP.

Miercom's malware suite was used for detection testing. Baseline efficacy is determined using HTTP transport. Successive testing is expected to results in the same, or degraded, detection efficacy.

Then malicious URLs were run through each UTM for HTTP transport analysis and reputation, or behavioral, based detection efficacy.

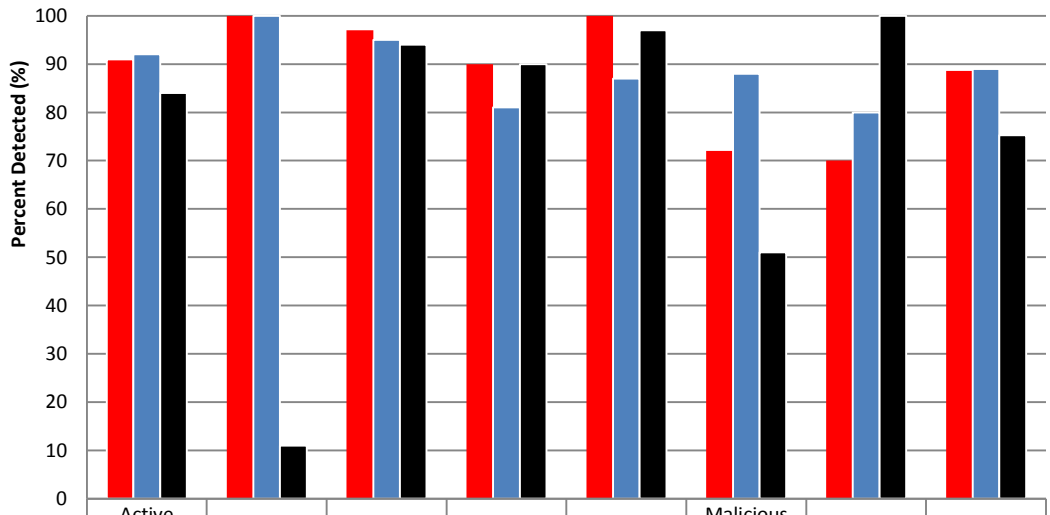
Miercom Malware Detection

Description

Malware steals the credentials of FTP programs to execute attacks. Popular FTP clients such as FileZilla and CoffeeCup are accessed and ran to transfer malicious files. This is a very direct method of transferring malware and is expected to yield the best results.

All malware samples were delivered to a target host using an FTP server. The same efficacy was found whether using HTTP GET or FTP. The test results in the charts below are regarded as HTTP transport. Samples detected in this test will be used as the sample set for the next tests: email protocols and HTTPS. The difference in detection will identify the problem areas of the UTM to find malware using other protocols. Realistically, traffic is transferred in many ways across the network. A summary of these detection efficacies will reflect its real-world deployment.

Results



	Active Threats	AET	APT	Botnet	Legacy	Malicious Docs	RAT	Average
Trend Micro CE70	91	100	97	90	100	72	70	89
Dell SonicWall TZ300	92	100	95	81	87	88	80	89
Fortinet FortiGate 50E	84	11	94	90	97	51	100	75

Source: Miercom December 2016

Trend Micro had the highest and most well-rounded malware detection. While Trend Micro and Dell both had excellent efficacy for the complex threats (Active Threat, AET, APT), Trend Micro was able to detect 100% of the Legacy samples. Legacy malware is known and highly reputable. Detecting both common and complex malware proves that Trend Micro utilizes both signature-based and behavioral detection. All vendors struggled with Malicious Documents. The average detection efficacy of malware transported over HTTP was 84%.

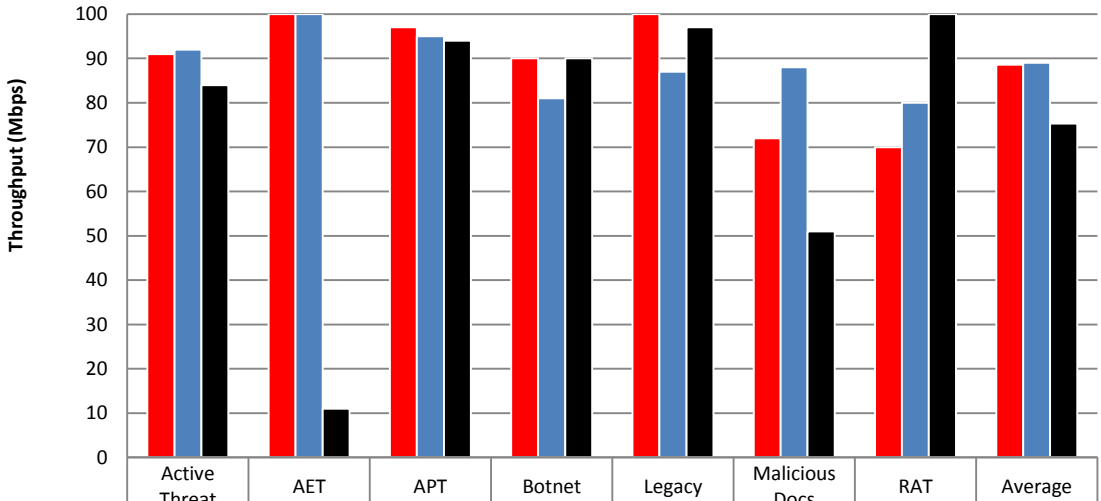
Email Malware Detection

Description

Last year, over 200 billion emails were sent and received per day. Attackers see this medium as a convenient way to access and manipulate an organization. Security product should inspect emails for malicious payloads delivered via protocols such as SMTP/S, POP3/S and IMAP/S. Malicious content and attachments should be blocked; spam emails should be blocked or marked accordingly.

External email accounts were created and used to deliver legacy malware samples to an unprotected target behind the UTM. Samples used in this test were those detected in the previous test when transferred using HTTP. An equal or lower efficacy is expected, implying the UTM under test is detecting at a similar or degraded rate for the email vector.

Results



	Active Threat	AET	APT	Botnet	Legacy	Malicious Docs	RAT	Average
Trend Micro CE70	91	100	97	90	100	72	70	89
Dell SonicWall TZ300	92	100	95	81	87	88	80	89
Fortinet FortiGate 50E	84	11	94	90	97	51	100	75

Source: Miercom December 2016

All vendors were able to detect the same amount of samples over email protocols (SMTP-IMAP) as they had over HTTP, resulting in the same averages. This shows that the email protocols bear no effect on the way each product detects malicious activity. The average detection efficacy of malware sent via email was 84%.

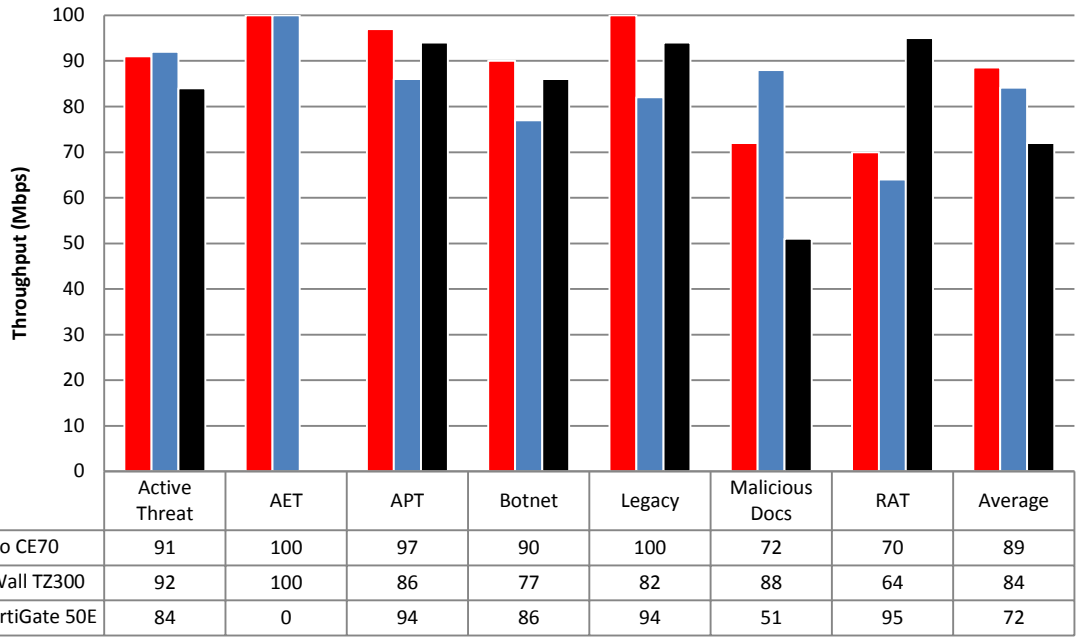
HTTPS Malware Detection

Description

While SSL and TLS encryption was intended to protect privacy, it is used as a countermeasure of attackers who disguise malware transfers as legitimate processes. In the past year, the amount of attacks from this vector has increased dramatically. Although not as obvious as HTTP and Email, the attacks via HTTPS should be detectable.

Similar to email security testing, the sample set for this test was the same as that used during HTTP transport. Efficacy is expected to be equal to or lower than HTTP and email security.

Results



	Active Threat	AET	APT	Botnet	Legacy	Malicious Docs	RAT	Average
Trend Micro CE70	91	100	97	90	100	72	70	89
Dell SonicWall TZ300	92	100	86	77	82	88	64	84
Fortinet FortiGate 50E	84	0	94	86	94	51	95	72

Source: Miercom December 2016

Trend Micro was able to detect 100% of the samples as it had in the previous tests, giving it an average of 89% malware detection efficacy over HTTPS. Detection of botnets, legacy malware and RATs were slightly lower for Dell and Fortinet over HTTPS. Dell also saw 9% less detection of APTs, and Fortinet missed 11% of the AET samples it had detected before. The average detection for encrypted malware transfer was 82%, 2% lower than HTTP and email security.

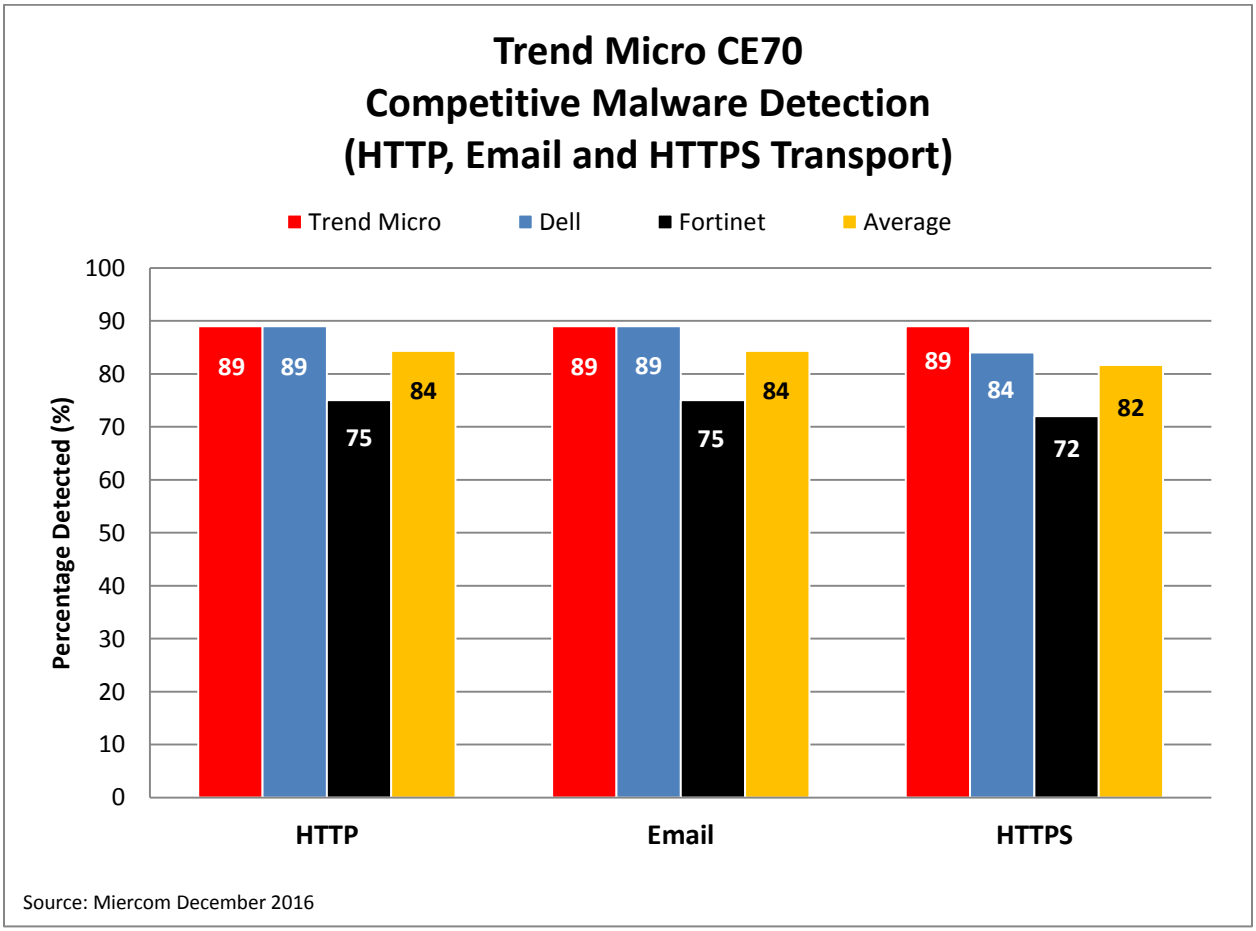
Summary of Malware Detection

Description

Malware delivered on different protocols were averaged and compared for each vendor. Detection was analyzed using the same malware set for file transfer, email communications and encrypted traffic.

The initial malware test was performed using HTTP. The samples detected in this test were sent through each DUT using email protocols (SMTP for sending, IMAP for receiving) and HTTPS. Since we are sure these samples are detectable by the DUTs, any failure to detect using a protocol other than HTTP will imply the true inability to identify malware. If this is the case, it is up to the vendor to remediate this vulnerability.

Results



Source: Miercom December 2016

Trend Micro was the only vendor to not see any degradation in malware detection for HTTP, email and encrypted protocols. Dell and Fortinet saw a decrease in malware protection over encrypted traffic, but fell by no more than 5%. Different protocols affected the way that the UTM products, except Trend Micro, treat incoming malware.

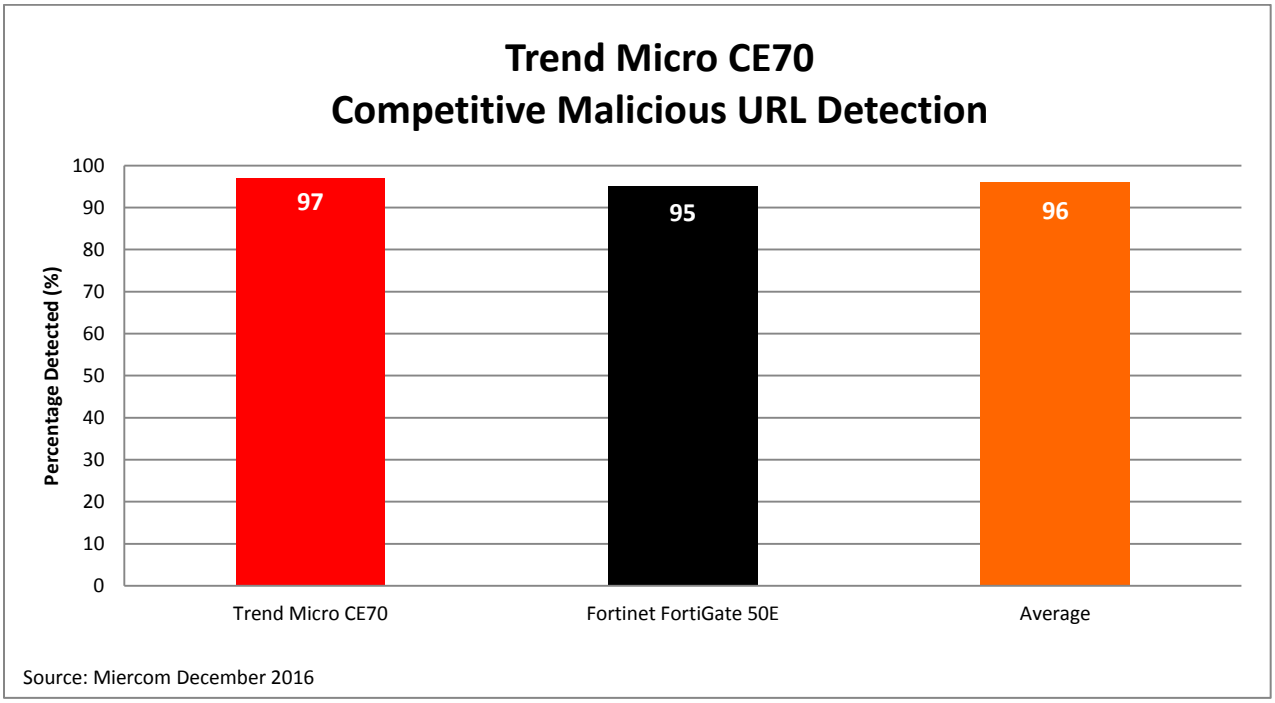
Malicious URL Detection

Description

Malicious links are the top method for delivering malware, and according to the 2016 Wombat Security *State of the Phish* report, 85% of organizations fall prey to these attacks and are up 22% from last year.

Malicious URLs consist of more than just phishing; they include browser hijacking and obfuscated redirects injected in code, such as a hacked *.htaccess* file which makes a personalized site both unreachable and blacklisted while sending users to a malicious site. Without protection against these malicious links, a targeted host could be subjected to attackers directly or used as an endpoint in botnet or DDoS attacks.

Results



All vendors except Dell were capable of detecting malicious URLs. Despite repeated efforts, Dell was unable to detect any samples due to a potential vulnerability; this vendor has been notified of this issue. The average featured above excludes the 0% detected by Dell to better represent the remaining vendors who could detect URL samples. Trend Micro had the highest detection, stopping 97% of malicious URLs.

Throughput Performance

Network performance is dependent on the amount and quality of processes taking place. To enhance security, performance must be sacrificed. The goal of a UTM product is to keep the performance load as minimal as possible while offering competitive security measures. This engineering design is critical for those considering a UTM device for their organization.

Stateful traffic was sent through the DUT and recorded for firewall, firewall and individually enabled features and then for full UTM mode. Its firewall was expected to yield the highest throughput and UTM the lowest because of the load security processing places on performance.

UTM Forwarding Rate (Stateful Traffic)

Description

Processing of stateful traffic is a realistic indicator of how the UTM will operate in a real-world environment. Making connections and having acknowledged packet forwarding requires additional processing, placing an additional load on the performance. All vendors were tested using a single port pair with bidirectional traffic over WAN to LAN. Being as Trend Micro is a cloud-based product, sNAT had to be disabled for testing with Ixia BreakingPoint.

For each vendor, throughput was tested over HTTP for firewall, firewall with individual security features, and lastly, UTM mode. Although HTTP is not inherently stateful, the TCP connections made on the transport layer are stateful. Payloads used to verify certain features, such as IPS or AV, typically use UDP.

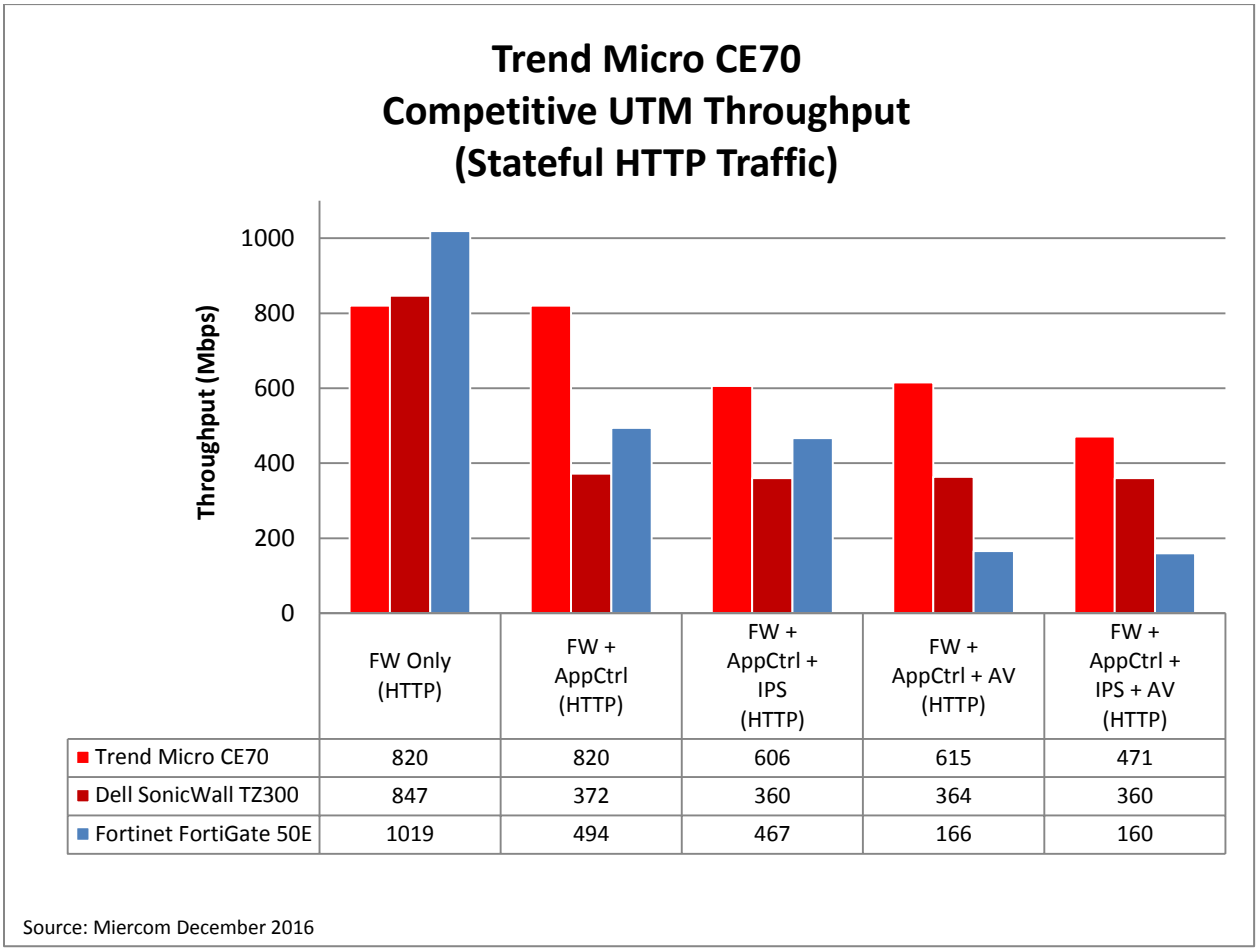
Before testing firewall and IPS or AV, we verified functionality of these features using the Ixia BreakingPoint *Strike List* of IPS or AV attacks, as applicable. If the efficacy was low against these attacks when either feature was in effect, we assumed the feature is not enabled or incorrectly configured. This was corrected before testing throughput.

Results

Trend Micro showed a higher throughput than its competitors when AppCtrl, IPS, AV and UTM mode were enabled. IPS and AV functionality was verified as blocking 42/183 and 528/528 attacks, respectively, prior to throughput testing. UTM mode performance was 471Mbps, 24% better than its best competitor.

Dell had 847Mbps firewall throughput performance which was 11.5% higher than the rate published in its datasheet. Prior to testing IPS and AV features, Dell was able to block 127/183 attacks with IPS and 527/528 attacks with AV. Its performance for IPS enabled was 360Mbps, 16.7% higher than its datasheet. With AV enabled, its throughput was 72.5% higher than its datasheet at 364 Mbps. Its UTM throughput was 360Mbps, trailing 111Mbps behind Trend Micro's UTM performance.

Fortinet had a firewall throughput of 1Gbps. When AppCtrl was enabled, this throughput dropped to 494Mbps but was still 29.1% higher than its datasheet performance. Its IPS and AV features were verified for functionality and blocked 182/183 and 528/528 attacks, respectively. Its IPS throughput was 41.6% lower than its datasheet throughput at 467Mbps. Its UTM performance was exactly as listed on its datasheet at 160Mbps.



	FW Only (HTTP)	FW + AppCtrl (HTTP)	FW + AppCtrl + IPS (HTTP)	FW + AppCtrl + AV (HTTP)	FW + AppCtrl + IPS + AV (HTTP)
Trend Micro CE70	820	820	606	615	471
Dell SonicWall TZ300	847	372	360	364	360
Fortinet FortiGate 50E	1019	494	467	166	160

Source: Miercom December 2016

Trend had the highest AppCtrl, IPS, AV and UTM throughput of its competitors. Throughput for FW Only and FW+AppCtrl were the same because AppCtrl is always on by default for the Trend CE70 UTM. Fortinet showed the highest FW throughput, but once AppCtrl was enabled, it dropped by over half of this performance and was comparatively low for AV and UTM mode. While additional features were expected to degrade performance, Trend Micro and Dell were the most consistent in performance as security layers were applied.

Quality of Experience

Two or more products may be excellent in terms of security and speed, but the quality of experience (QoE) an administrator has while using the product differentiates it as a top choice for deployment. This section addresses the front end experience of the out-of-box set up, console visibility and use of provided reports of each device tested.

Management and Deployment

Out-of-the-box deployment and management is expected to be simple with intuitive navigation. We first looked at how product setup, noting the time and effort required. Next, we evaluated the dashboard console for organization, visibility and aesthetic. Even if a product provides a lot of information in an organized manner, the console can be overwhelming for a business customer. It is important that the end user can easily navigate through a management-friendly interface.

	Trend Micro CE70	Dell SonicWall TZ300	Fortinet FortiGate 50E
Cloud-based	●		●
Automatic Updates	●	●	●
Centrally Managed Console	●	●	●
Easy Installation	●	●	●
Network Setup Wizard	●	●	●
Default Protection Enabled	●		●
Easy GUI Navigation	●	●	●
Useful Help Menu	●		●
Concise Dashboard	●	●	●
Event/Policy Display	●	●	●
Data/Search Filter	●	●	●
Malware Security	●	●	●
Malicious URL Security	●		●
Email Security	●	●	●
Email Spam Filtering	●	●	●
VPN Management	●	●	●
MSP-Friendly	●	●	●
Visible EULA	●		●

Logging and Reporting

Whenever a policy is violated or security event is triggered, the admin should be notified. All reports should be searchable, saved, exportable and logged in real-time for later analysis. Visibility should be granular and help remediate.

	Trend Micro CE70	Dell SonicWall TZ300	Fortinet FortiGate 50E
Cloud-based Reporting	●		●
Event/Policy Violation Log	●	●	●
High-level Detailed Log	●	●	●
Graphical Charts	●	●	●
Intuitive Interface	●	●	●
Data Filtering	●	●	●
Exportable Data	●	●	●

Unique Features

The Trend Micro CE70 is a cloud-based product which differs from leading UTM devices through its methods of alerting, managing and scanning. These features were evaluated for their ease of use and contribution to the uniqueness of the CE70.

Tagging

In addition to email security measures, any malicious content in an email resulted in the inclusion of a tag; informing the sender and receiver that malware had been detected and removed. The console gives a real-time update that the malware had been found, showing an increase in the Email Anti-Malware count.

This feature is helpful because it show them where malicious content came from. Adding a tag gives more versatility to email security by allowing the administrator to set rules to specific end users or groups. Emails are cleaned of the malicious attachment, the subject is tagged and the body of text includes a statement regarding the content removal. But the send may not always be a reason to exclude emails. It may just be the file they are sending. Tagging gives more flexibility to email security.

An individual, or group, within the company may still need the text of the email, regardless of the malicious attachment. Tagging avoids deleting the entire message and quarantines the emails instead. End users are aware of the malware removal process from these notifications.

Cloud Console and Scanning

We observed that the WAN does need to be manually set up, but LAN configuration is automatic, when employing the Cloud console in a network environment. Cloud-based management is, in fact, accessible from any location provided the admin has the proper credentials. Log analysis was available and reports could be customized based on the user's needs. Policies could also be updated using the Cloud console.

Email and websites were monitored and scanned for malicious attachments and content for security violations. The addition of email, site and spam protection is crucial for a centralized management product, and in this case Trend Micro provides these features without requiring extra licenses.

Email Spam Filter

The Trend Micro CE70 offers spam filtering capabilities in addition to its UTM solution. Trend Micro's method pushes all emails through its Cloud Edge device, similar to a firewall, and tags spam using email and IP addresses from a constantly updated list of known spammers. Using machine-learning algorithms, it differentiates between spam email and regular email by comparing each aspect of one type of email to another.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom 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 Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This report was part of Miercom's continuous Industry Assessment of UTM products. Each vendor featured is allowed to participate before, during and after testing. Results published may be refuted, retested and republished should a featured vendor choose to participate.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.