Trend Micro Cloud Edge 50 & 70
Competitive UTM Assessment

April 2018

DR180314F

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Unified Threat Management (UTM) systems incorporate multiple security functions into a single system. These products offer firewall, intrusion prevention, antivirus, email scanning and application control capabilities while keeping network performance degradation at a minimum.

But there is usually a trade-off in security products: more security means more processing, and this lowers data throughput. UTM products aim to make this drop in throughput as low as possible, and a real-world deployment can reveal how well these products actually achieve this.

Trend Micro engaged Miercom to independently assess and compare its Cloud Edge UTMs, the CE50 and CE70 to the following UTM products: Fortinet FortiGate 50E and SonicWall TZ300. Results were observed for security, performance and subjective out-of-box evaluations to identify strengths and unique qualities. Additionally, we looked at differentiating features of the Cloud Edge series – email tagging, cloud-based management, machine learning and Business Email Compromises detection – which set it apart from local-only, physical devices.

All UTM devices were deployed in a realistic business network, where malware over multiple protocols, malicious URLs and advanced exploits were sent through to victim computers. Each device was observed for its security efficacy against a range of threats and for the ability to differentiate false positives from true malicious samples. The performance of each UTM's firewall and individual security features was recorded for stateful HTTP traffic to determine the realistic effect of security on network bandwidth.

Key Findings of the Trend Micro Cloud Edge Series (CE50 and CE70)

- Observed highest detection rate of 83 percent for malware delivered over HTTP and as much as 82 percent delivered over FTP
- CE50 and CE70 detected the most malware samples at 79 and 81 percent efficacy, respectively, over email protocols such as SMTP, POP3 and IMAP
- Prevented 81 percent of malware from encrypted emails, outperforming other vendors by at least 23 percent
- Blocked the most samples delivered over HTTPS, detecting as much as 36 percent higher than its competition
- Differentiated two-thirds of the false positive samples when sent with actual malware
- Superior detection of malicious URLs, blocking 98 percent of samples
- With firewall enabled, the CE50 achieved 750 Mbps and the CE70 reached 1 Gbps of throughput for Layer 7 traffic

- Outperformed its competition for every security feature enabled over stateful traffic – with no degradation on either the CE50 or CE70 with application control applied, zero effect on CE50 performance with antivirus enabled, and the least degradation with full UTM mode enabled
- CE 70 UTM throughput outperforms the competition at 400 Mbps; CE50 at 350 Mbps; with the lowest competitor achieving only 15% of Trends' outstanding performance
- Easy-to-use dashboard can be configured using pre-defined widgets to show customizable, graphical displays of events
- Cloud-based reporting supports detailed logs of events and violations, data filtering, and an exportable data feature from an intuitive interface
- Email tagging feature allows an administrator to remove malicious content from a flagged email, pass the remaining content and give a real-time update of the malware source
- Unique, centrally managed Cloud Console gives remote access to multiple UTM devices for off-site universal or individual configuration and remediation in minutes
- Machine learning uses predictive technology to analyze and detect unknown threats
- Email threats against C-level users are blocked and logged to avoid costly consequences
- Enhanced troubleshooting support offered through local device management, displaying traffic logs by packet or packet capture

Based on our findings, the Trend Micro Cloud Edge 50 and 70 Unified Threat Management products demonstrate excellent security efficacy and performance with respect to similar competing devices. We proudly award the Trend Micro Cloud Edge 50 and 70 the ***Miercom Certified Secure*** certification.

Robert Smithers

CEO

Miercom

2.0 Test Summary

Summary of UTM Test Results: Security Efficacy and Performance

Tests	Page	Vendors			
Security Efficacy	11	Trend Micro CE50	Trend Micro CE70	Fortinet FortiGate 50E	SonicWall TZ300
Malware Detection (HTTP)	13	83	83	45	52
Malware Detection (FTP)	14	81	82	43	48
Malware Detection (Unencrypted Email)	16	79	81	56	57
Malware Detection (Encrypted Email)	16	81	78	56	58
Malware Detection (HTTPS)	18	82	82	46	51
False Positive Selective Avoidance	20	67	67	50	67
Malicious URL Detection	21	98	98	95	62
Average Security Efficacy	-	81.6	81.6	55.9	56.4
≥80 percent		51-79 percent		≤50 percent	
Performance	22	Trend Micro CE50	Trend Micro CE70	Fortinet FortiGate 50E	SonicWall TZ300
Stateful HTTP – FW	23	750	1000	1000	200
Stateful HTTP – FW + AppCtrl	23	750	1000	785	80
Stateful HTTP – FW + AppCtrl + IPS	23	400	490	350	80
Stateful HTTP – FW + AppCtrl + AV	23	400	450	250	75
Stateful HTTP – FW + AppCtrl + IPS + AV (UTM)	23	350	400	117	60
Highest		Mid-Range		Lowest	

3.0 Introduction

Small and mid-sized business organizations encounter threats from many vectors. End users use web browsers, file sharing programs, email and other communications that open the network to attack. For full protection, networks require a Unified Threat Management (UTM) solution, which harnesses the power of a next generation firewall and secure web gateway, to block malicious activity from all vulnerable points of the local network.

Increased security processing puts a load on data throughput, making the balance between performance and security crucial. Miercom tested four UTM devices to provide an intelligent comparison of security efficacy and its effect on overall 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, such as the 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 and reported. Depending on IPS settings, access can be blocked to the internal network
Application Control	AppCtrl	Enforces policies regarding security and resources – such as network bandwidth and servers – by controlling which application traffic passes through the UTM, usually in either direction. Application Control is also 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, Virtual Private Network (VPN) tunnel control, content filtering, and data loss prevention.

The firewall is the most basic form of protection. When additional security features are enabled, the performance is expected to see degradation effects.

4.0 How We Did It

Miercom's hands-on testing replicates real network environments to challenge and provide an accurate assessment of a product's security efficacy and performance.

Testing identifies the strengths and weaknesses of each Device Under Test (DUT). In addition to generated traffic patterns and attacks from industry leading test tools, we use our own 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

Using more than a thousand samples, we assess the antivirus engine of each DUT. The sample set includes a broad scope of malware, to determine protection techniques against different attack methods.

Samples are delivered over nine protocols used in typical business network communication: HTTP, HTTPS (TLS version 1.2, 1.1 and 1.0), FTP, SMTP, SMTPS, POP3, POP3S, IMAP and IMAPS. Transfers are made from WAN to LAN to a victim computer through the DUT, or downloaded from the simulated WAN server through the DUT. All DUTs have continuous access to the internet allowing for automated updates from each vendor.

A missed sample is any malware file successfully transferred to the target. Results are reported as a percentage of blocked malware samples.

Malicious URLs

The DUT is the first line of defense when accessing the Internet by preventing users from reaching malicious locations which put the network at risk for infection. The DUT should block known, harmful locations regardless of its technique to bypass the antivirus scanner.

A fresh set of malicious URLs is used. Malicious locations change quickly, so products were assessed simultaneously, to ensure comparable URL filtering results.

This test used automated scripts that attempt to access each web site through the DUT. If the site can be reached, it is considered a fail. If the DUT causes the site to be inaccessible or a block page is displayed, the sample is considered a pass. The overall results are reported as a percentage of blocked URL samples.

Performance

Throughput tests were performed with the DUT deployed inline using a single port-pair, with egress to WAN and ingress to LAN. While some products are capable of more than a single port pair, most UTM deployments use the single 1x1-Gigabit Ethernet (GbE) port configuration. It must be noted that any discrepancy between observed and published datasheet values are a result of this implementation.

Before running performance tests, normal traffic flow through the DUT is verified.

Stateful Traffic

Application Layer (L7) HTTP traffic was sent through the network using the Ixia BreakingPoint traffic generator to determine the throughput of the UTM device with multiple security features applied. Both IPS and AV functionality are verified prior to testing using Ixia BreakingPoint Strike exploit packs. Throughput was recorded as the maximum rate before packet loss occurs.

Performance was recorded for:

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

The impact of deploying the additional features is quantified as observed performance degradation associated with each security configuration.

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.

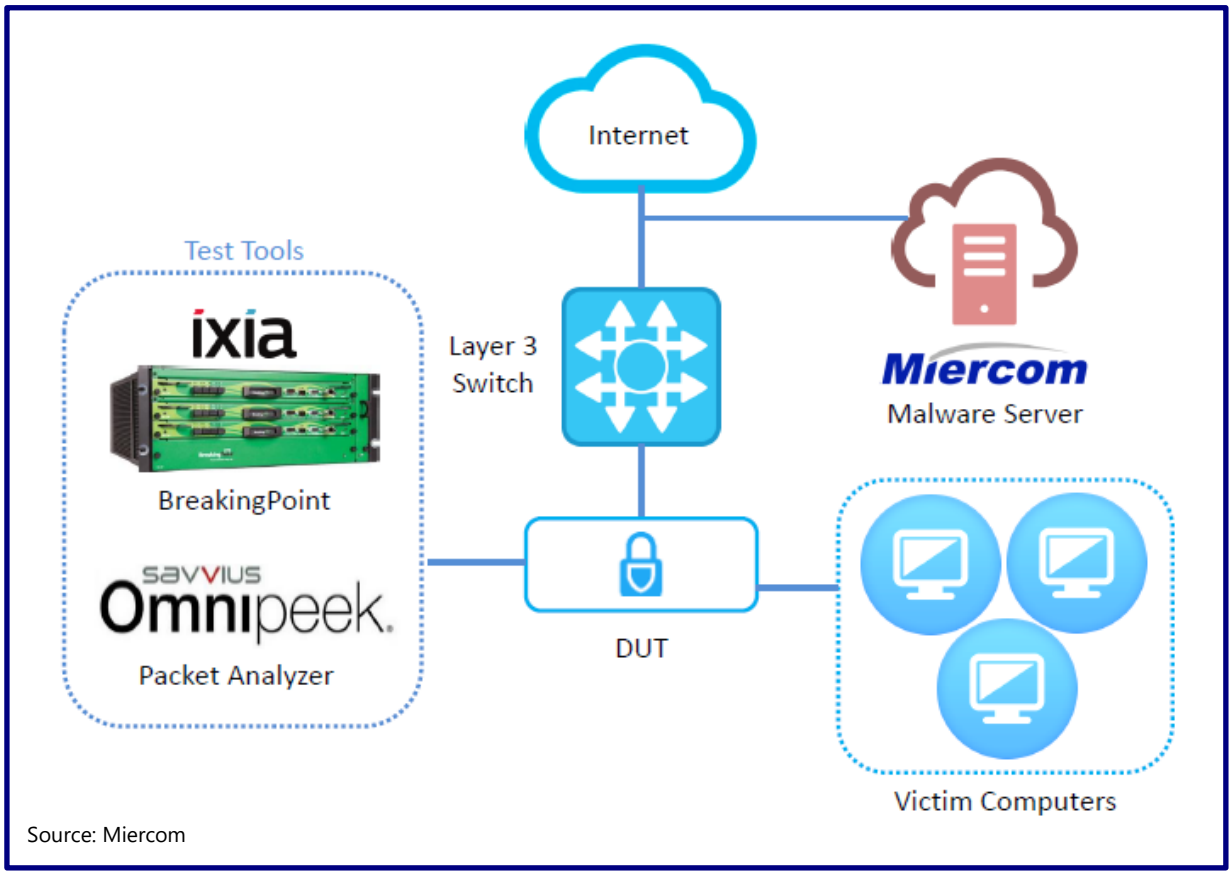
Attack Generation

Ixia BreakingPoint optimizes security devices by simulating live security attacks and 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.

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.

Test Bed Overview



Source: Miercom

Test Tool/DUT	Version
Ixia BreakingPoint	3.5.2
Trend Micro Cloud Edge 50	5.2
Trend Micro Cloud Edge 70	5.2
Fortinet FortiGate 50E	FortiOS v5.6.3 build1547 (GA)
SonicWall TZ300	SonicOS Enhanced 6.5.0.2-8n

5.0 Security Efficacy

5.1 Malware Detection

The DUT was an intermediary between untrusted and trusted zones of a simulated network, representing real-world deployment of a switch, a firewall and end point devices. An attacker in the untrusted zone attempted to deliver malware to the trusted zone in order to establish communication. Each DUT was evaluated for its ability to detect, block and notify the administrator of malicious activity.

Common malware are botnets, legacy, malicious documents and RATs. An emphasis is 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 by constantly changing, sourced from external resources and private honeypots, which have undergone antivirus evasion techniques such as encryption, black packaging and payloads using normal traffic
Advanced Evasion Technique (AET)	Combined evasion tactics that create multi-layer access
Advanced Persistent Threat (APT)	Continuous hacking with payloads opened at admin level
Backdoor	Remote access attacks that use port binding, control and command servers, and dormant malware to infiltrate networks using legitimate programs or platform to go unrecognized
Botnet	Communicating programs that collectively spam and deliver Distributed Denial-of-Service (DDoS) attacks
Legacy	Variants of known, older malware
Malicious Document	Mix of Microsoft and Adobe documents with Macro viruses, APTs, worms
Remote Access Trojan (RAT)	Trojans disguised as legitimate software, remotely control victim

Malware samples were delivered first using HTTP transport. Delivering over other protocols was expected to result in the same, or degraded, efficacy under the assumption that no additional settings are applied; for example, the enabling email blocking of all executable files. Other protocols tested are FTP, HTTPS, SMTP, SMTPS, POP3, POP3S, IMAP and IMAPS.

After looking at all types of malware, we used false positive selective avoidance testing to determine the detection sensitivity to true positives mixed with suspicious, yet clean, samples.

5.1.1 HTTP and FTP Transport

Description

This section outlines the malware efficacy results for each DUT when accessing malicious files via HTTP and FTP protocols. These two protocols are currently some of the most commonly seen vectors for an end user to accidentally infect themselves when accessing the internet.

All samples are hosted on a public server containing both a web server and an FTP server. The victim computer for each DUT attempts to download the sample set via HTTP and FTP.

Test Setup

All DUTs were configured using the default AV and IPS settings. Some DUTs require alterations to the baseline configuration in order to accurately obtain results for this test.

The table below lists configuration changes:

UTM	Configuration Changes
Trend Micro Cloud Edge 50	Web filtering disabled
Trend Micro Cloud Edge 70	Web filtering disabled
Fortinet FortiGate 50E*†	Web filtering disabled, test speed decreased significantly
SonicWall TZ300**	Web filtering disabled

All devices required web filtering to be disabled when running the HTTP testing. Trend and Fortinet devices flagged the test domain as malicious and began blocking all access to the site. The blacklisting of the domain artificially prevents file downloads. The act of blocking a download based on URL is assessed in the Malicious URL Detection section, and is not considered applicable to this test.

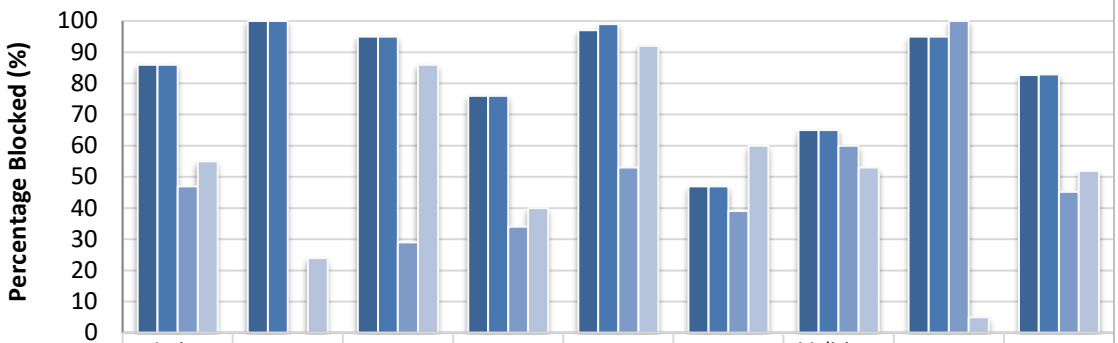
* *The sample delivery rate for the FortiGate 50E was altered due to device capabilities. When delivering the samples in quick succession, the CPU on the FortiGate 50E stays at 100 percent and the device no longer allows network communication. When analyzing the processes running on the device, the "scanunitd" process is observed to use all available CPU processing power. With a much slower malware delivery, the samples could be successfully analyzed allowing the collection of accurate results.*

† *The FortiGate 50E was observed to seemingly divert what was previously premise detection to its cloud service, resulting in lower malware detection than expected or seen in previous detection. There is an apparent limitation on the number of samples it can process, and while Fortinet continues to improve after repeated tests, this limitation likely contributes to its low detection rate.*

*** When running the HTTP samples for the first time, the SonicWall TZ300 Capture ATP engine did not analyze all unknown samples. The observed results for this run are lower than expected and required additional retests. Each consecutive run delivered more samples to the ATP engine. When reviewing the results produced by the ATP engine, 98 percent of the delivered files are marked as malicious. Miercom projects that this engine will increase the efficacy of the TZ300 when all unknown samples are delivered properly. The effect of the ATP engine is quantified using a comparison between two consecutive sample set deliveries using HTTP protocol in the next section.*

Results

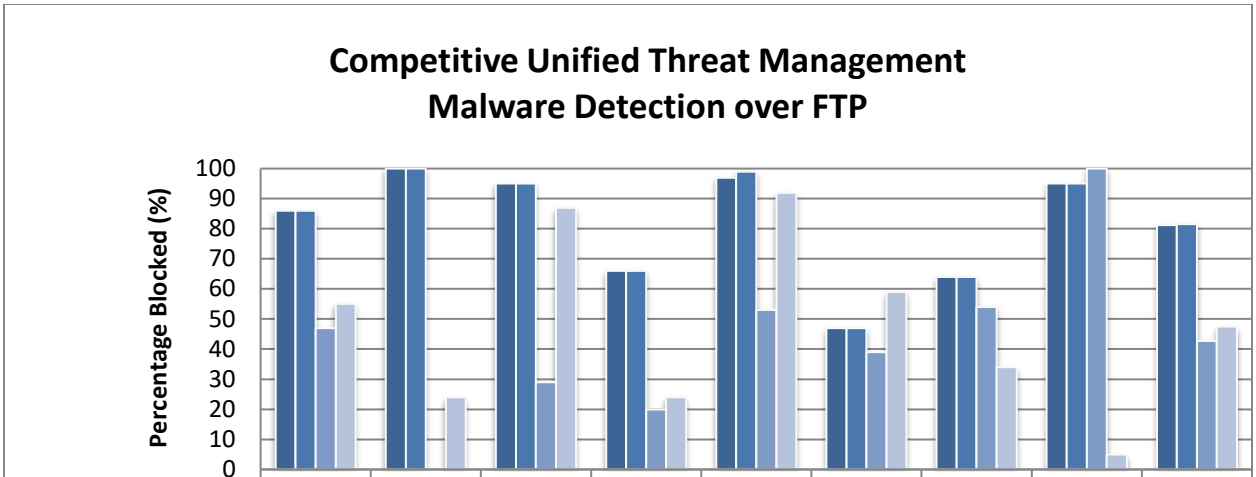
Competitive Unified Threat Management
Malware Detection over HTTP



	Active Threat	AET	APT	Backdoor	Botnet	Legacy	Malicious Doc	RAT	Average
Trend Micro CE50	86	100	95	76	97	47	65	95	83
Trend Micro CE70	86	100	95	76	99	47	65	95	83
Fortinet FortiGate 50E	47	0	29	34	53	39	60	100	45
SonicWall TZ300	55	24	86	40	92	60	53	5	52

Source: Miercom

Trend Micro UTM devices had the highest detection of malware over HTTP. Trend Micro CE50 and CE70 had nearly identical detection rates over HTTP, only differing for the botnet malware category where the CE70 had 2 percent higher efficacy to collect 99 percent of all samples. Both Trend Micro UTMs had an average of 83 percent malware detection efficacy, with highest rates against advanced threats like AET and APT samples, and detected many botnet and RAT samples. Trend Micro products saw improvement in detection by as much at 10 percent for botnet and 25 percent for RAT samples since prior testing. Most vendors had below average detection of backdoors, legacy files and malicious documents.



	Active Threat	AET	APT	Backdoors	Botnet	Legacy	Malicious Docs	RAT	Average
Trend Micro CE50	86	100	95	66	97	47	64	95	81
Trend Micro CE70	86	100	95	66	99	47	64	95	82
Fortinet FortiGate 50E	47	0	29	20	53	39	54	100	43
SonicWall TZ300	55	24	87	24	92	59	34	5	48

Source: Miercom

While Trend Micro UTM products had the highest detection, overall rates for FTP were lower than that of HTTP transfer of malware. As with HTTP, the Trend Micro CE70 detected 2 percent more botnet samples than the CE50. The Trend Micro products' average detection was similar at 81 percent for the CE50 and 82 percent for the CE70. Similarly, both products showed high detection rates for advanced threats, botnets and RATs; most vendors' detection was below average for backdoors, legacy malware and malicious documents.

Summary

Both Trend Micro UTM devices had an average malware detection efficacy of 83 percent, with highest block rates for advanced threats. Most vendors struggled with backdoor, legacy and malicious document threats. The same malware set delivered over FTP yielded lower results for all vendors. Trend Micro CE50 and CE70 had detection rates of 81-82 percent over FTP.

5.1.2 Email Transport

Description

Over 260 billion emails are sent each day, making it a convenient medium for attackers to access a network. And when a majority of professionals prefer email as their means of communication, business networks would be wise to use a security product for email inspection of malicious payloads over SMTP/S, POP/S and IMAP/S protocols. Malicious content and attachments should be blocked.

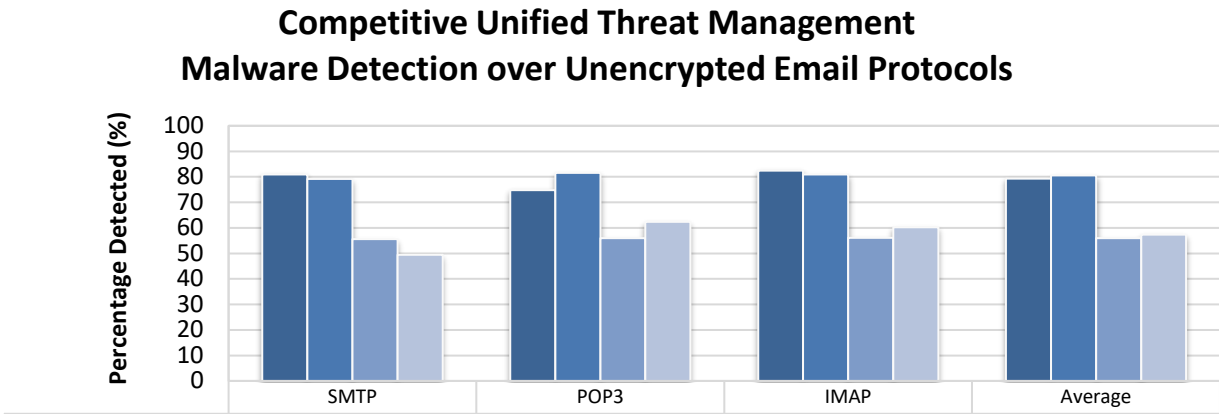
Test Setup

Email servers and accounts were configured on both a malware server and a victim computer. The full sample set was delivered using SMTP, SMTPS, IMAP, IMAPS, POP3 and POP3S. For this testing, SMTP uses port 25, SMTPS uses port 25 and STARTTLS, IMAP uses port 143, IMAPS uses port 993, POP3 uses port 110 and POP3S uses port 995.

The default email filtering settings are used for each DUT, with the exceptions listed below. An important differentiator that must be taken into consideration is the filtering of executables. Many of the samples used are executables and are automatically blocked by the Fortinet Device. In order to assess the DUT's true filter capabilities, the automatic identification of executables as malicious is disabled.

UTM	EXE File Restriction
Trend Micro Cloud Edge 50	N/A
Trend Micro Cloud Edge 70	N/A
Fortinet FortiGate 50E	Disabled setting for Executable Email Attachments Treated as Viruses
SonicWall TZ300	N/A

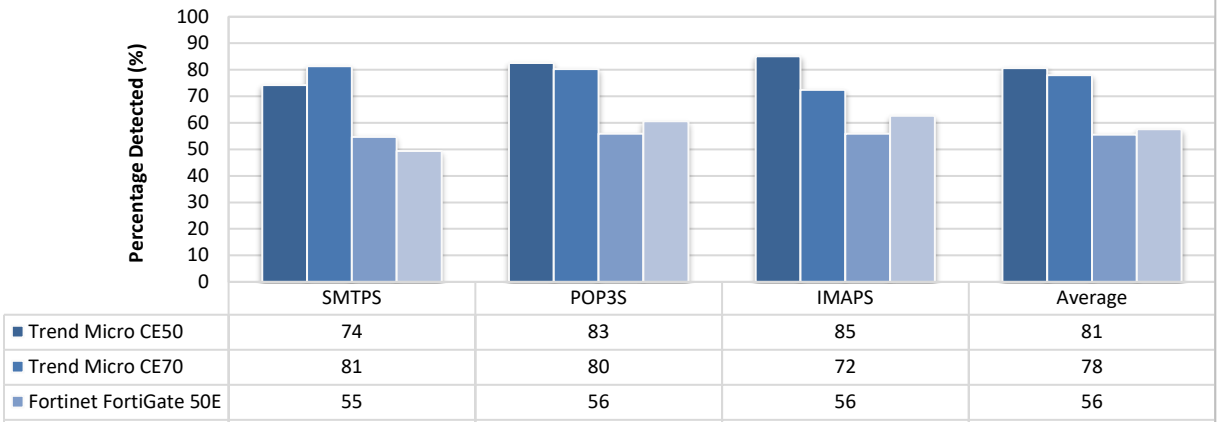
Results



	SMTP	POP3	IMAP	Average
Trend Micro CE50	81	75	82	79
Trend Micro CE70	79	82	81	81
Fortinet FortiGate 50E	56	56	56	56
SonicWall TZ300	50	62	60	57

Source: Miercom

The Trend Micro products had above average rates of detection for all email protocols.



	SMTPS	POP3S	IMAPS	Average
Trend Micro CE50	74	83	85	81
Trend Micro CE70	81	80	72	78
Fortinet FortiGate 50E	55	56	56	56
SonicWall TZ300	49	61	63	58

Source: Miercom

Malware detection over encrypted email was slightly higher for the Trend Micro CE50 but slightly lower for the CE70. Fortinet's detection remained the same. SonicWall's detection improved by 1 percent.

Notable Observations

Mail clients use different methods of retrieving emails from a mail server. For this testing, IMAP and POP3 protocols were used to accomplish this.

SonicWall TZ300:

- Automatically deletes mail identified as malicious from the mail server when retrieved via POP3 protocol. The "Disable POP3 Auto Deletion" override in the "/diag.html" section of the user interface did not successfully disable this behavior. The autodeletion did not impact the reported results.
- Additional steps are required for scanning SMTPS email. When configuring the internal mail server, the Public Server Guide quick configuration is a quick and uncomplicated tool to configure the internal mail server. With this configuration complete, outbound SMTP mail will be scanned; however, the DPI-SSL/TLS Server section requires configuration to ensure that encrypted inbound SMTPS email is scanned. The DPI-SSL/TLS Client configuration allows the encrypted outbound mail to be scanned. Miercom's engineering team believed this can be considered an easy oversight when configuring the UTM to handle encrypted email and wanted to ensure that system administrators are aware of this nuance when configuring an internal mail server.

Summary

Trend Micro CE50 and CE70 had above average rates of detection for unencrypted and encrypted email protocols.

5.1.3 HTTPS Transport

Description

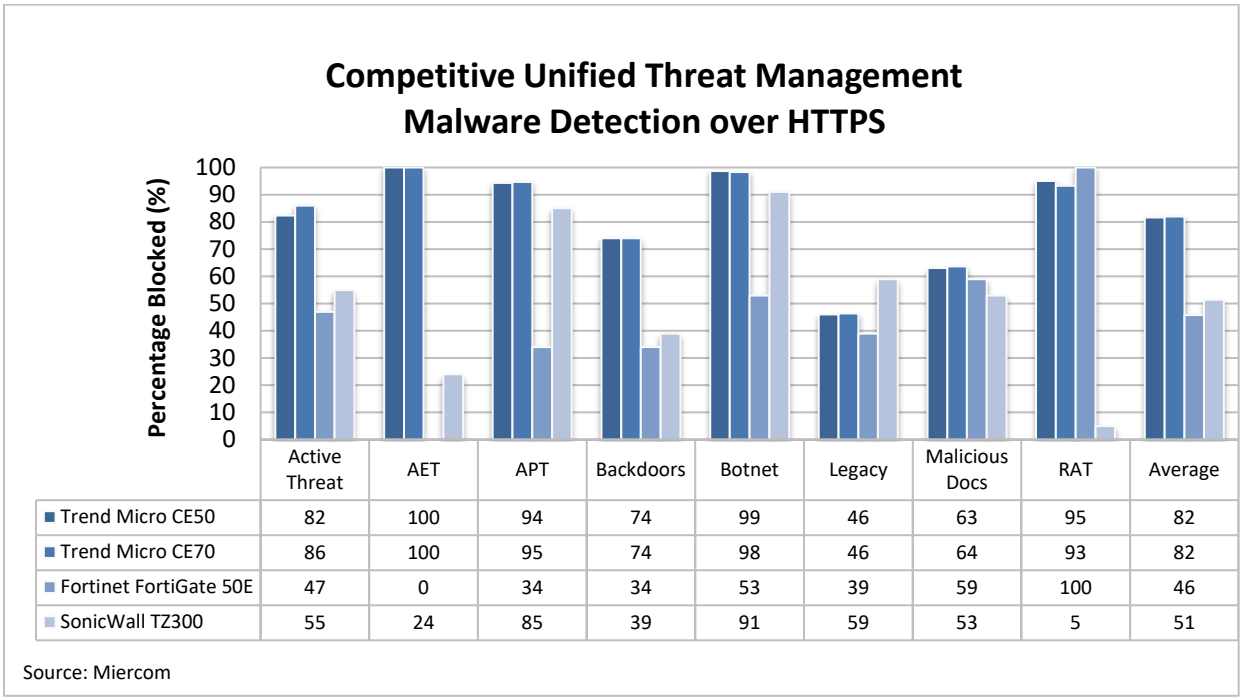
Encrypted web communications protect privacy and continuously account for a larger portion of Internet traffic. While data is secured through this protocol, it also makes transactions more difficult to be scanned for malware. Most sites today use a default HTTPS page, and attackers increasingly use encrypted malware delivery methods.

The most common defense against this is configuring a UTM product to operate in proxy mode, acting as middle man for the data transfer. To scan traffic for threats, the UTM decrypts incoming traffic, scans it, and then re-encrypts before delivering data to the client.

Test Setup

Each DUT was configured in proxy mode and malware samples were sent from WAN to LAN using the HTTPS protocol.

Results



	Active Threat	AET	APT	Backdoors	Botnet	Legacy	Malicious Docs	RAT	Average
Trend Micro CE50	82	100	94	74	99	46	63	95	82
Trend Micro CE70	86	100	95	74	98	46	64	93	82
Fortinet FortiGate 50E	47	0	34	34	53	39	59	100	46
SonicWall TZ300	55	24	85	39	91	59	53	5	51

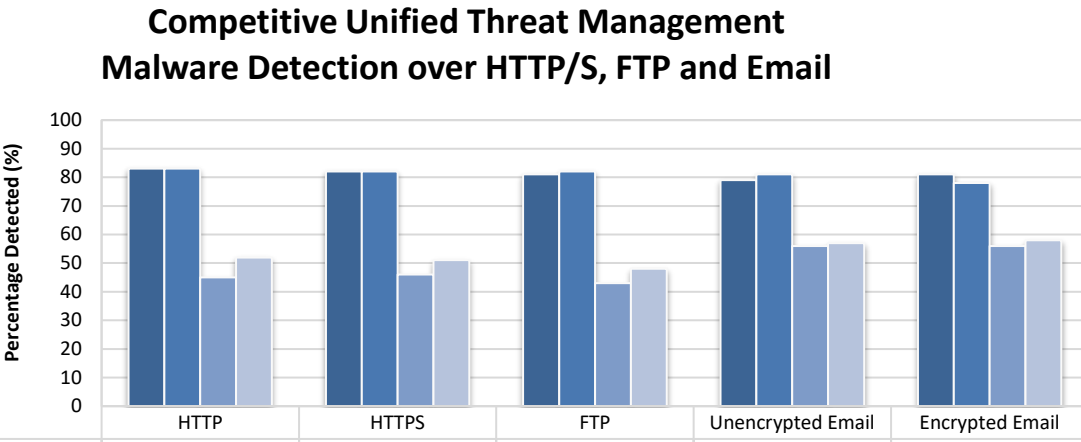
Source: Miercom

Trend Micro CE50 and CE70 had the highest malware detection over encrypted web traffic. Trend Micro UTM device saw highest detection against active and advanced threats, botnets and RAT samples.

5.1.4 Summary of Malware Detection

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

The results shown below represent the overall filtering capabilities of each device.



	HTTP	HTTPS	FTP	Unencrypted Email	Encrypted Email
Trend Micro CE50	83	82	81	79	81
Trend Micro CE70	83	82	82	81	78
Fortinet FortiGate 50E	45	46	43	56	56
SonicWall TZ300	52	51	48	57	58

Source: Miercom

The Trend Micro CE50 had the highest detection of all vendors for encrypted email delivery of malware. Of all protocols, both Trend Micro UTM products detected best over HTTP, at a rate of 83 percent. Fortinet's best detection was over unencrypted and encrypted email protocols, at 56 percent. SonicWall had its highest efficacy over encrypted email protocols.

5.1.5 False Positive Selective Avoidance

Description

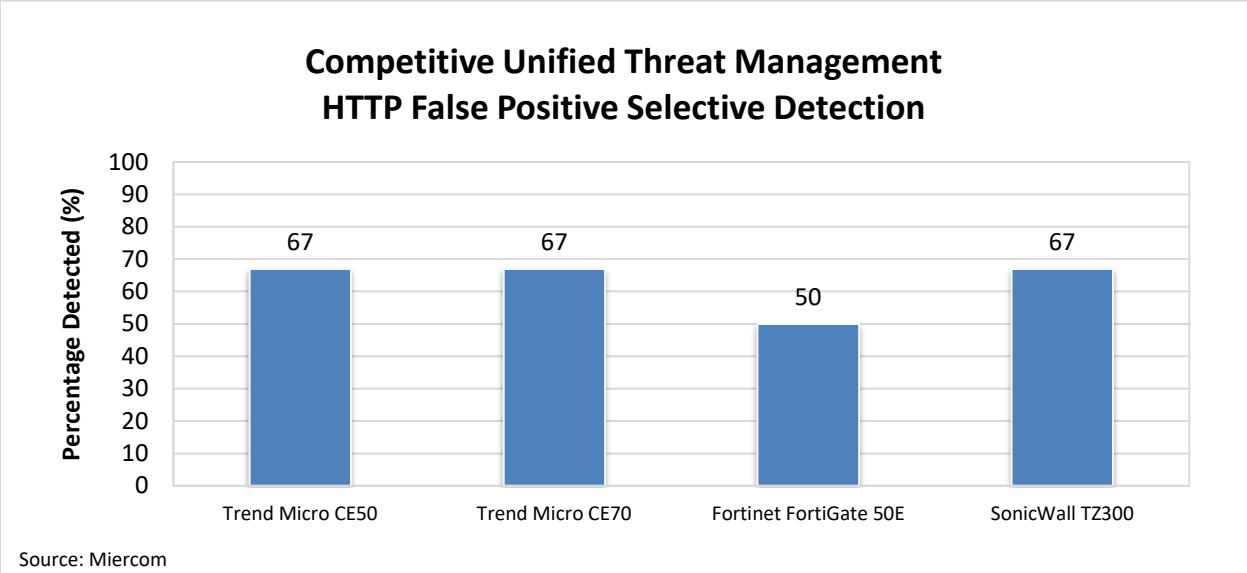
False positives are clean files that are misidentified as malicious. These files fall into a grey category due to their possible misuse on a network. An example is a password recovery tool, which while not technically a malicious program, is often flagged for its possibly malicious use.

Samples tested the granularity of the DUT's AV engine. Successful false positive selective avoidance means high rates of malware blocking with low rates of false positive blocking. High rates of blocking false positives imply the AV engine is considerably aggressive. High selective avoidance efficacy correlates to sensitive and intelligent security.

Test Setup

After sending a mixture of false positives (clean, suspicious files) and true positives (malware files) via HTTP, we measured selective avoidance of false positives. If the DUT could discern appropriately by flagging only true positives and passing false positives, it received a pass.

Results



Trend Micro CE50 and CE70 selectively avoided two-thirds of false positive samples which were not malicious, even among true malicious files. Trend Micro offers a certain level of sensitivity when identifying suspicious, but not malicious, traffic as well as granular administrative control of security stringency. The sensitivity can be increased or decreased based on the business network's needs.

5.2 Malicious URL Detection

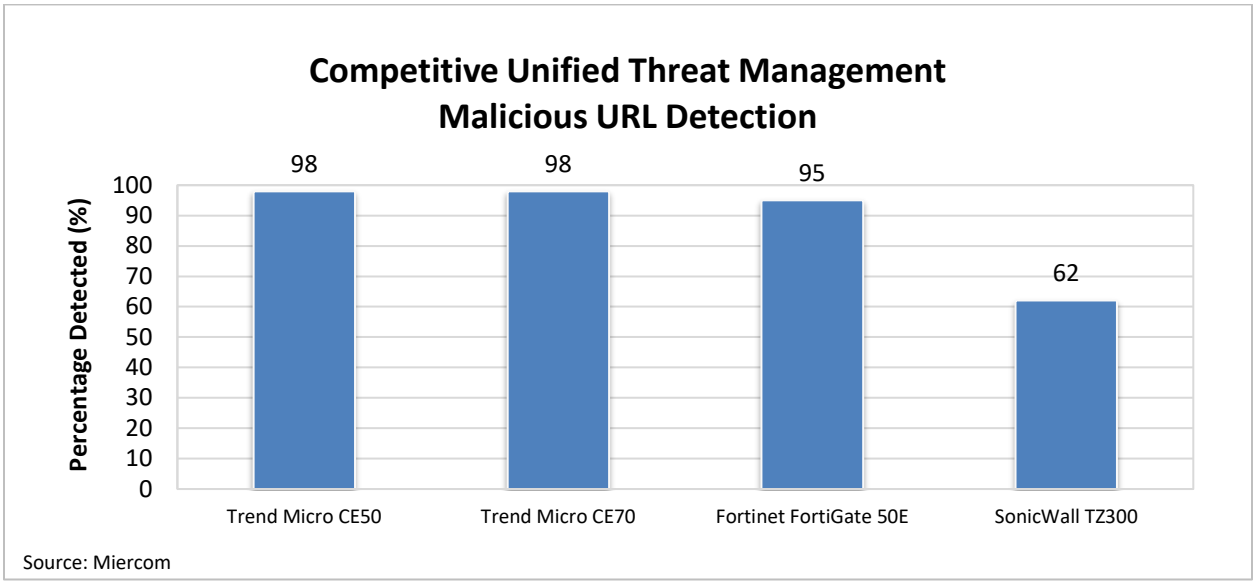
Description

Malicious URLs are 22 times more likely to infect networks than a couple of years ago. These links deliver malware through phishing, browser hijacking and hidden code of an accessed site. Victims of malicious URLs allow attackers to use their computer, and other devices in the network, for botnet and distributed attacks to spread infection at an alarming rate. Organizations that fall prey to these attacks may lose privacy of login credentials, communications and sensitive company data.

Test Setup

Using an automated test configuration, malicious URLs are attempted to be accessed through the DUT. The results are presented as a fraction of the number of sites blocked versus the total sites accessed. A site is considered "allowed" if the URL can be reached and a successful response is returned. This test does not assess anti-virus capabilities; it strictly assesses the DUT's capability to filter web locations based on reputation. Any site that is inaccessible will be removed from the results and will not count for or against the DUT.

Results



Trend Micro CE50 and CE70 had the highest average detection of malicious URL samples at 98 percent.

6.0 Stateful Traffic Performance

Description

Security features tend to have an impact on performance. With more security enabled, lower throughput is observed. A UTM product must strike a balance between performance load and competitive security measures, as both metrics are important.

Processing of stateful traffic is a realistic indicator of how the UTM will operate in a real-world environment. Establishing connections and acknowledging packet forwarding requires additional processing, placing a load on performance. 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.

The firewall throughput was expected to yield the highest performance. The UTM's security features were applied using increased stateful traffic for a realistic evaluation of security processing on traffic bandwidth. These results were expected to be lower than the firewall throughput. The amount of degradation distinguished one vendor from another.

Test Setup

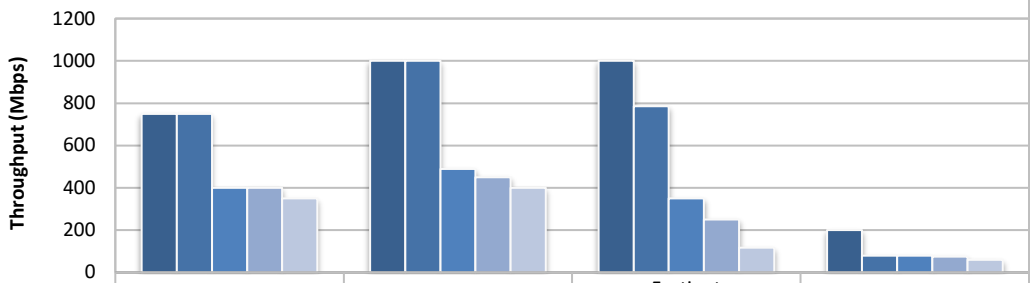
This benchmark test was performed WAN to LAN with bi-directional traffic and a single port pair through a wired connection. Firewall was enabled and a 1 MB file transaction was made as traffic was increased until transactions failed. The throughput measured before a transaction failed was the maximum HTTP throughput, recorded in the chart on the following page. Next, other security features were enabled to determine the effect on performance.

The test methodology differed from the one used for Trend Micro Cloud Edge 70 competitive assessment of last year. A larger file size was used, 1 MB increased from 100 KB. Files were transferred using 10 servers and 10 DHCP clients, in contrast to 50 servers and 50 static clients. For this round of testing, there was a single TCP connection made, one file transferred and the connection was closed. Previous testing used a single connection to transfer 10 files at a time.

The changes in file transfer methods and updated firmware may affect the throughput results for each vendor in comparison to the previous report.

Results

Competitive Unified Threat Management
Stateful HTTP Throughput (Mbps)



	Trend CE50	Trend CE70	Fortinet FortiGate 50E	SonicWall TZ300
FW	750	1000	1000	200
FW + ApplCtrl	750	1000	785	80
FW + ApplCtrl + IPS	400	490	350	80
FW + ApplCtrl + AV	400	450	250	75
FW + ApplCtrl + IPS + AV (UTM)	350	400	117	60

Source: Miercom

Trend Micro CE70 had one of the highest firewall throughput rates of 1 Gbps, and UTM throughput of 400 Mbps. The Trend Micro CE50 had the second highest throughput rates for most configurations, and its UTM performance was nearly three times that of its next best competitor at 350 Mbps.

7.0 Quality of Experience

Two or more products may be excellent in terms of security and speed, but the quality of experience (QoE) for an administrator 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.

7.1 Management and Deployment

The devices tested are intended for small business deployments. Many small businesses do not have dedicated IT resources or have limited expertise in the deployment of security devices. Therefore, the best solutions require a comprehensive and simplistic user interface.

The commands and controls for each device are slightly different for each manufacturer. We found the easiest to configure security settings and AV logs are provided by Trend Micro, and the most simplistic initial configuration is supplied by the SonicWall wizard. These differences affect the choice made by each small business when selecting a UTM product. Having the best security numbers is not helpful if the product is too complex and can be easily misconfigured.

Miercom Tip: Miercom recommends the use of a test file to test each security configuration implemented on a UTM. An example of this test consists of the delivery of the EICAR file as an email attachment to the internal mail server. If it is not detected or logged, there is a misconfiguration that could allow inbound mail to become an unprotected vector for infection. (SonicWall has a default setting to disable the detection of this file.)

The chart below shows an overview of features and capabilities that are important to device manageability and ease of use. All the DUTs had very similar capabilities when managing, but differentiators are shown below. These differentiators have different impacts for each deployment and should be considered in the context of the desired setup. For instance, cloud management is a very useful tool if the IT team works from home or the business' IT needs are fulfilled by a remote contractor.

	Trend Micro CE Series	Fortinet FortiGate 50E	SonicWall TZ300
Cloud-based Management	●	●	
Automatic Updates	●	●	●
Centrally Managed Console	●	●	●
Easy Installation	●	●	●
Network Setup Wizard	●	●	●
Additional Setup Wizards			●
Intuitive Certificate Management	●		●
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	●	●	

The following items are the positive features observed for each product. Out-of-the-box deployment and management is expected to be simple with intuitive navigation. We first looked at 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 CE Series

- Cloud management makes implementing policies on multiple devices simplistic and centrally manageable
- Dashboard can be configured using pre-defined widgets
- Event analysis is easy using the Internet Security tab in the analysis and reports section; filters can be used to look at specific devices or end points
- A customizable log can be viewed and switched to a graphical overview with a customizable timeframe
- Help Guide gathers additional information about configuration choices on current pages
- Local device management logs traffic by packet or capture in GUI for troubleshooting

Fortinet FortiGate 50E

- A smooth user interface with conventional layout of monitoring and configuration are available in one bar to the left
- Configurable User Dashboard has widgets to provide end user customization
- Simple log and report view; details about a specific event can be shown in a collapsible display on the right side of the screen; security events are assigned threat scores to help the end user understand the severity of the event
- Built-in help links and highlighting is very useful for trying to solve configuration shortcomings that are identified by the box
- Useful security audit feature for identifying configuration shortcomings

SonicWall TZ300

- Quick configuration choices make deployment very easy
- Useful breakdown of category tabs: “Monitor” “Investigate”, “Manage”, and “Quick Configuration” adds some extra navigation steps when trying to adjust settings or view system status
- Helpful advanced settings in the web-based ‘diag’ page
- Internal Packet Capture for DUT is a nice feature that can help with troubleshooting

- Ability to switch between the new and old GUI is helpful when looking at older guides and for tech support
- When a file is sandboxed, the pictures of actions can be viewed and downloaded; this is very useful when analyzing problems
- Has certificate import setting at the bottom of page

7.2 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 support remediation.

	Trend Micro CE Series	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	●	●	●

8.0 Unique Features

The Cloud Edge product line has these unique features that are investigated as a part of this testing. The CE50 and CE70 support email tagging, a cloud console, machine learning and malware detection for business emails. These features were evaluated for their ease of use and contribution to the uniqueness of the Cloud Edge series of devices.

8.1 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.

If a non-malicious email is identified as malicious and blocked, this feature allows the end user to have an alert allowing full visibility into blocked emails. This helpful feature shows where malicious content came from, and tagging gives more versatility and visibility to email security by allowing the application of rules to specific end users or groups. Emails are cleaned of the malicious attachments; the subject is tagged and the body of text includes a statement regarding the content removal. 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.

8.2 Cloud Console

The cloud console offers universal access, centralized management and universal or specific sharing of policies and firewall rules on multiple devices. Controlling multiple UTMs from the cloud interface offers more visibility and freedom to end user management. Its remote access is helpful to IT services, which may not be on-site or in the same building as the device, by eliminating the need to VPN into a network or manually visit the site. Cloud management also allows quick configuration and event tracking for multiple devices from any location. The flexibility of cloud management reduces technical support time from days or hours to minutes.

The Trend Micro CE series includes cloud management to provide a versatile solution to security device management and monitoring. Other UTMs, such as the Fortinet FortiGate 50E, provide cloud support but require a separate license that could be cost prohibitive for a small business.

8.3 Machine Learning

Trend Micro Predictive Machine Learning is an Artificial Intelligence technology deployed in the cloud. It is used to analyze and detect security risks that were not seen before, while no signatures were available.

8.4 Business Email Compromises (BEC) Detection and Emphasis

Trend Micro developed advanced technologies to detect and block Business Email Compromises (BEC) – an emerging threat against C-level executives and can lead to significant financial losses. Business email messages with malicious content were effectively blocked and properly logged.

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.