Trend Micro Cloud Edge 100G2/50/SB

Competitive UTM Assessment

November 2019

DR191025C

Miercom
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 often a trade-off in security products: more security means more processing, and this lowers data throughput. UTM products aim to minimize performance impact, and a real-world deployment can reveal how well these products achieve this.

Trend Micro engaged Miercom to independently assess and compare its Cloud Edge UTM products CE100G2/50/SB to the Fortinet FortiGate 60E and SonicWALL TZ350. Results were observed for security, performance and subjective out-of-box evaluations to identify strengths and unique qualities. Additionally, we looked at some product differentiators for the Cloud Edge series – tagging, cloud console, machine learning and business email security.

All UTM devices were deployed in a realistic business network, where malware over multiple protocols, malicious URLs and advanced exploits attempted to infect 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 was recorded for stateless UDP traffic, and the performance of individual security features was recorded for stateful HTTP traffic to determine the effect of security on network bandwidth.

Key Findings of the Trend Micro Cloud Edge Series 100G2/50/SB

- Highest competitive malware detection over HTTP and email protocols at 95.4%
- Highest URL filtering protection efficacy – at 98% – against malicious websites
- Provided 100% application control to support end user management and productivity
- Among highest comprehensive security efficacy of 95.6%, which includes: malware detection, URL filtering, intrusion prevention and application control
- Highest Intrusion Prevention System detection of 100% against hundreds of lethal exploits
- Best stateful HTTP throughput for full UTM security at 552 Mbps – as much as 64% higher than competing UTM products tested
- Best stateful encrypted HTTPS UTM throughput at 240 Mbps – outperforming similar products by as much as 71% – despite the large security processing load
- Nearly 1 Gbps stateless UDP throughput for single 1-Gigabit port pair with firewall enabled

Based on our findings, the Trend Micro Cloud Edge Unified Threat Management series demonstrates excellent security efficacy and performance with respect to similar competing devices. We proudly award the Trend Micro Cloud Edge 100G2/50/SB products 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	9	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FG60E	SonicWALL TZ350
Malware Detection (HTTP)	10	95.4	89.5	94.5	93.5	56.0
Malware Detection (FTP)	11	82.4	89.5	86.5	75.4	43.8
Malware Detection (Email)	12	95.4	89.5	94.5	93.5	56.0
URL Filtering	14	98	98	98	95	65
Intrusion Prevention System	15	100	100	100	100	100
Application Control	16	100	100	100	100	100
Average Security Efficacy	-	95.2	94.4	95.6	92.9	70.1

≥85 percent	51-84 percent	≤50 percent

Performance	17	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FG60E	SonicWALL TZ350
UDP – FW	18	959	959	959	959	960
HTTP – FW	19	760	744	200	880	340
HTTP – FW + AppCtrl	19	720	744	144	650	320
HTTP – FW + AppCtrl + IPS	19	656	434	144	400	294
HTTP – FW + AppCtrl + AV	19	600	418	146	250	294
HTTP – Full UTM	19	552	379	120	200	283
HTTPS – Full UTM	20	240	107	50	135	70

Highest	Mid-Range	Lowest

3.0 Introduction

Small and mid-sized business organizations encounter threats from many vectors. End user productivity relies heavily on web browsers, file sharing programs, email and other communications that leave the network open 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.

Increasing security processes puts a load on data throughput, making the balance between performance and security crucial. Miercom tested five UTM devices to provide an intelligent comparison of security efficacy and its effect on overall performance.

The devices tested for this report include 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	Description
Firewall (FW)	Controls and filters traffic flow to provide relatively low-level barrier of protection for the trusted internal network from an unsecure network like the Internet
Intrusion Prevention System (IPS)	Monitors all network activity 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 (bandwidth, servers, etc.) by controlling application traffic passing through the UTM, usually in either direction.
Antivirus (AV)	Prevents, detect and removes malicious software, viruses, spyware and other threats.
Unified Threat Management (UTM)	An all-inclusive security setting where multiple functions are performed by the same, single security device. Function typically include firewall, IPS, AV, virtual private network tunneling, content filtering and data loss prevention.

The firewall is the most basic form of protection. When additional security features are enabled, performance is expected to degrade with respect to the default firewall throughput rate.

Testing focused on the following:

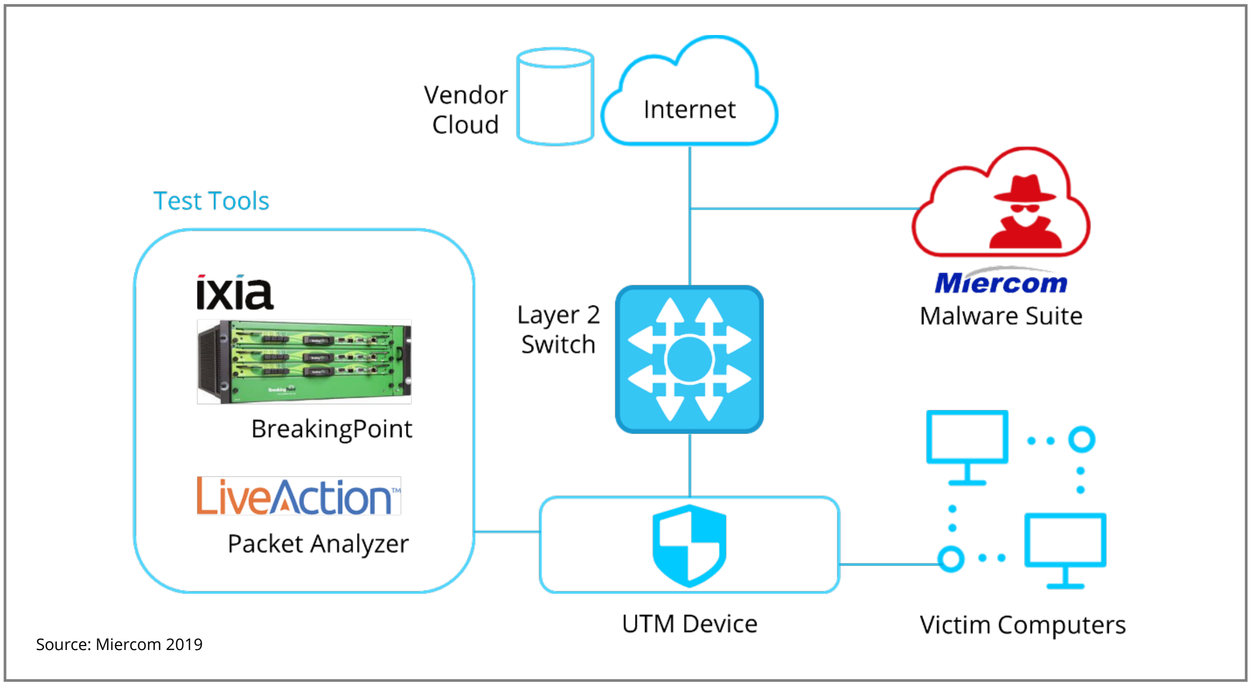
- Malware defense
- Intrusion Prevention System (IPS)
- Application Control
- Performance
- URL Filtering
- Email Security
- Ease of Use
- Management
- Reporting
- Deployment
- Unique feature

4.0 How We Did It

Our hands-on testing of UTM products used a real-world small business environment, challenging a product's security efficacy and performance in order to provide a realistic assessment of its unique features and capabilities.

We first looked at security features with a custom-crafted set of threats to determine detection efficacy. Then we performed throughput rate testing to evaluate a default throughput rate of basic firewall feature security and increased layers of protection to determine performance degradation from data processing.

Test Bed Overview



Source: Miercom 2019

In order to perform an exhaustive security review of the devices in this report, we replicated a standard Internet Service Provider (ISP) setup with DHCP IP address allocation, much like modem cable and fiber-to -provider environments. However, instead of delivering via a fiber or cable uplink, the Internet was delivered by Ethernet cables trunking straight into a high bandwidth aggregation switch previously configured to serve as the backbone of our ISP.

Connections to the "real" Internet were handled through our firewall. No external connections were used except for the vendor cloud management interfaces and basic browsing and email tests (Google, Gmail, newspaper websites to validate connectivity and more). All connectivity between the UTM devices, victims and switches were realized using Cat6 wiring with Ethernet operating in Gigabit full duplex mode. Our high performance, proprietary Security and Network Test Suite Server (NTSS) was connected via 2x10-GbE SFP to our aggregation switch.

Using a client server, we generated a random number of clients requesting a realistic snapshot of real-world HTTP, application and email traffic. For HTTP/S downloads, the number of client streams varied randomly from 1 to 500.

UTM Device	Version
Trend Micro Cloud Edge 100G2	5.5.2085
Trend Micro Cloud Edge 50	5.5.1090
Trend Micro Cloud Edge SB	5.5.1090
Fortinet FortiGate 60E	6.2.0 build 0866 (GA)
SonicWALL TZ350	SonicOS Enhanced 6.5.4.4-44n

Routing, Network, Safety & Performance – Server and “Internet” Side

Firewall Layer 3 Routing Performance

In order to test L3 Routing performance, we set up a special, low latency, high bandwidth link with our NTSS upon which we built a *qperf* and *iperf* test. *Qperf* was configured with a UDP test at 1518 bytes per frame size, while *iperf* was configured with a more realistic, 128KB TCP test. We rely on our *qperf* test to evaluate the drag race-style L3 routing performance of the UTM devices, while the TCP test provides us with a scenario closer to real-world use of the devices.

Network Test Suite Server (NTSS)

Our proprietary NTSS is a high-bandwidth, high-performance server running a highly optimized Debian Linux setup hosting the following series of tests:

- Network Performance Suite: Our Trex Traffic Generator and its support software is hosted in our NTSS; enabling us to quickly deploy it in multiple test-scenarios with minimum downtime.
- HTTP and HTTPS Load Test: Our specially crafted, multi-threaded Apache setup delivers a custom set of files designed to simulate normal web usage, with file sizes ranging from 128KB through 4MB. Files are delivered using an increasing number of clients, from 1 through 500 concurrent connections. Tested protocols: HTTP and HTTPS (with TLS V 1.3 encryption)
- FTP Load Test: Our server provides a standard installation of VSFTPd to deliver our proprietary malware test sample over FTP transports.

Tested Protocols

FTP PORT and FTP PASV

- Email Submission Test: Our standard Postfix SMTP server allows us to send emails without filtering, limiting or firewalling. Our test virtual server can simulate up to thousands of inboxes across many test domains. Tested protocols: SMTP and SMTPS (with SSL/TLS and STARTTLS)
- Email Client Test: Our standard Dovecot IMAP/POP3 server allows us to receive emails without any filtering, limiting or firewalling. Our test virtual server can simulate one to thousands of inboxes across many test domains. Each inbox is accessible via standard email protocols. Tested protocols: IMAP/ IMAPS and POP3/POP3S (with TLS encryption)

Routing, Network, Safety & Performance – Client/End User Side

The following tools are a representative list of software tools and exploits we used to carry out our analysis.

Ixia BreakingPoint

BreakingPoint optimizes security devices by simulating live security attacks and invasions. By sending a mixture of application traffic and malicious traffic, this tool determines IPS and AV capabilities for detecting threats while remaining resilient. The “Critical Strike Pack” uses variants, or randomized path combinations, to exploit. Dynamic, “smart” exploits attack hosts and applications and are customizable for specific scenarios.

Linux Attacker/Control Machine

Using Debian 10 with Kernels 4.1.x and 5.1.x. We tested using 64-bit Linux.

Linux Test Client

Using Debian 10 with Kernels 4.1.x inside KVM Virtual Machines with physical Ethernet connections via PCIE bridging. We tested using 64-bit Linux.

qperf 0.4.11

qperf measures bandwidth and latency between two nodes. It can work over TCP/IP as well as the RDMA transports. On one of the nodes, qperf is typically run with no arguments designating it the server node. One may then run qperf on a client node to obtain measurements such as bandwidth, latency and CPU utilization.

iperf 3.6

iperf3 is a tool for performing network throughput measurements. It can test TCP, UDP, or SCTP throughput.

Nmap 7.70 + Zenmap

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan networks using raw IP packets in novel ways to determine what available hosts, offered services (application name and version), running operating systems (OS versions), types of packet filters/firewalls, and dozens of other characteristics. Nmap is also useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Zenmap is an X11+GTK frontend for Nmap.

TRex-TGN 2.61

TRex is an open source, low cost, stateful and stateless traffic generator fueled by DPDK. It generates L4-7 traffic based on pre-processing and smart replay of real traffic templates. TRex amplifies both client and server-side traffic and can scale up to 200Gb/sec with one UCS. TRex Stateless functionality includes support for multiple streams, the ability to change any packet field and provides per stream statistics, latency and jitter.

Apache 2.4.38

Apache is a highly effective, reliable and secure HTTP/S server. It is responsible for 29% of all web traffic served today. It has played a key role in the growth and development of the Internet. Its ubiquitous nature in the wider internet makes it an ideal software package to test, and simulate website access and delivery, not only of content but of malware.

Postfix 3.4.7

Postfix is a free and open-source Mail Transfer Agent (MTA) that routes and delivers email. Approximately 34% of the public-accessible email servers run Postfix; making it the second most popular MTA after Exim. Postfix is compatible with SMTP, SMTPS and Submission protocols.

Dovecot 2.3.4.1

Dovecot is a free and open source IMAP and POP3 server for UNIX-like systems written with security primarily in mind. Dovecot is a lightweight, stable and easy-to-use mail server that provides IMAP/IMAPS and POP3/POP3S access to mailboxes.

VSFTPd 3.0.3

VSFTPd is the Very Secure File Transfer Protocol Daemon. It provides an open source, standards-compliant server for the FTP and FTPS protocols to be used during testing.

5.0 Security Efficacy

5.1 Malware Defense

Malware is delivered to networks using different methods. A UTM device needs to be prepared to handle any attack, on any protocol. Common malware like botnets, legacy, malicious documents and remote access Trojans should be detected. More sophisticated malware – polymorphic, evasive and persistent threats, that are not already known by any intelligence database – are more challenging to block. An emphasis is placed on the advanced threats as they are complex and harder to prevent.

Using more than a thousand samples from our proprietary malware suite, we assessed the antivirus engine of each UTM device. The Miercom Malware Suite includes a broad range of samples:

Common Malware	
Backdoor	Remote attacks use port binding, control and command servers, and dormant malware to infiltrate networks using legitimate services to go unrecognized
Botnet	Communicating programs delivering spam and distributed DoS 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 controlling victim once activated

Advanced Malware	
Active Threats	Custom-crafted, constantly changing evasive malware
Advanced Evasive Techniques (AETs)	Combined evasion tactics that create multi-layer access
Advanced Persistent Threats (APTs)	Continuous hacking with payloads opened at the administrative level
Polymorphic, Zero-Day Malware	Constantly changing, difficult to detect; exploit known vulnerabilities

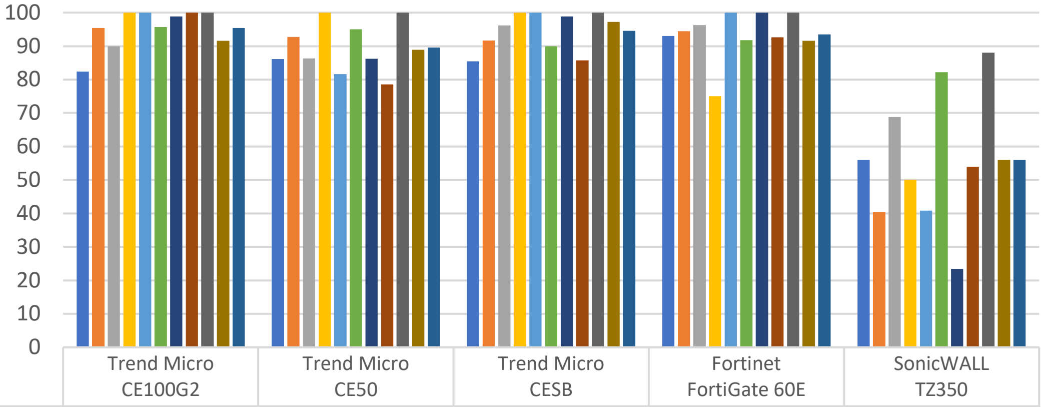
The UTM device was deployed between untrusted and trusted zones of a simulated network with a switch, firewall and endpoint devices to represent a real-world environment. An attacker in the untrusted zone (our Miercom Malware Suite) attempted to deliver malware to the trusted zone over nine protocols (HTTP, HTTPS TLS 1.2/1.1/1.0, FTP, SMTP, SMTPS, POP3, POP3S, IMAP and IMAPS).

Any sample that was successfully transferred to a target endpoint was considered a fail. Security efficacy was recorded as the percentage of samples blocked out of the total set attempted.

High detection efficacy against this blend of malicious files indicates well-rounded protection from multiple attack vectors. Blocked samples are analyzed to determine visibility and intelligence of threats on the network.

Results

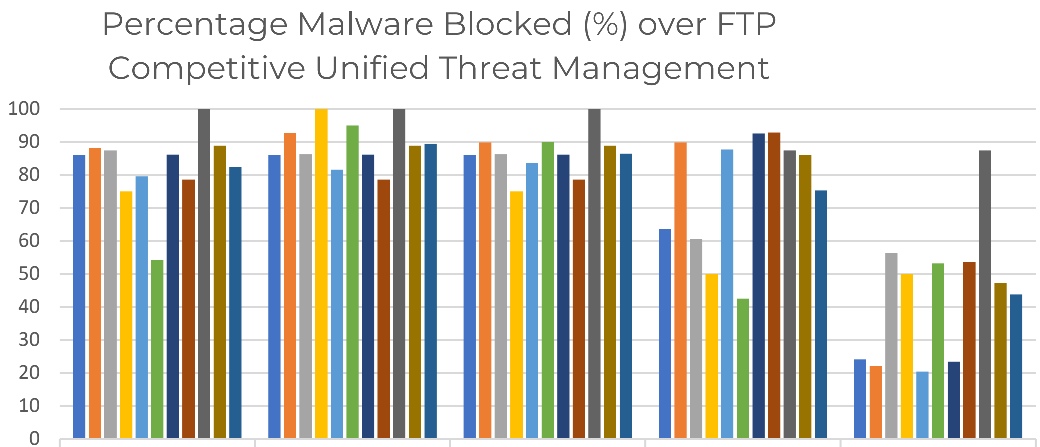
Percentage Malware Blocked (%) over HTTP/S
Competitive Unified Threat Management



	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FortiGate 60E	SonicWALL TZ350
■ Active Threat	82.4	86.1	85.5	93	56
■ AET	95.4	92.7	91.7	94.5	40.4
■ APT	90	86.3	96.2	96.3	68.8
■ Backdoor	100	100	100	75	50
■ Botnet	100	81.6	100	100	40.8
■ Legacy	95.7	95	90	91.8	82.2
■ Malicious Document	98.9	86.2	98.9	100	23.4
■ Polymorphic	100	78.6	85.7	92.6	54
■ Ransomware	100	100	100	100	88
■ RAT	91.6	88.9	97.2	91.6	56
■ Average	95.4	89.5	94.5	93.5	56.0

Source: Miercom 2019

All malware samples were delivered to target hosts using an HTTP/HTTPS server. Given the cloud-based scanning services offered by the devices under test, we expected reliable malware detection efficacy of 85 percent or better. Trend Micro scored the highest efficacy overall at 95.4 percent. Trend Micro was able to detect 100 percent of backdoor, botnet, polymorphic zero-day and ransomware samples. Trend Micro also showed excellent detection of 90 percent or higher for advanced evasive techniques, advanced persistent threats, legacy files, malicious documents and RATs. We saw evidence of Trend Micro's cloud control and antivirus signature management infrastructure as we received very similar results across different classes of devices that all connect to the Trend Micro management cloud.



Percentage Malware Blocked (%) over FTP
Competitive Unified Threat Management

	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FG60E	SonicWALL TZ350
■ Active Threat	86.1	86.1	86.1	63.6	24.1
■ AET	88.1	92.7	89.9	89.9	22
■ APT	87.5	86.3	86.3	60.6	56.3
■ Backdoor	75	100	75	50	50
■ Botnet	79.6	81.6	83.7	87.8	20.4
■ Legacy	54.3	95	90	42.5	53.2
■ Malicious Document	86.2	86.2	86.2	92.6	23.4
■ Polymorphic	78.6	78.6	78.6	92.9	53.6
■ Ransomware	100	100	100	87.5	87.5
■ RAT	88.9	88.9	88.9	86.1	47.2
■ Average	82.4	89.5	86.5	75.4	43.8

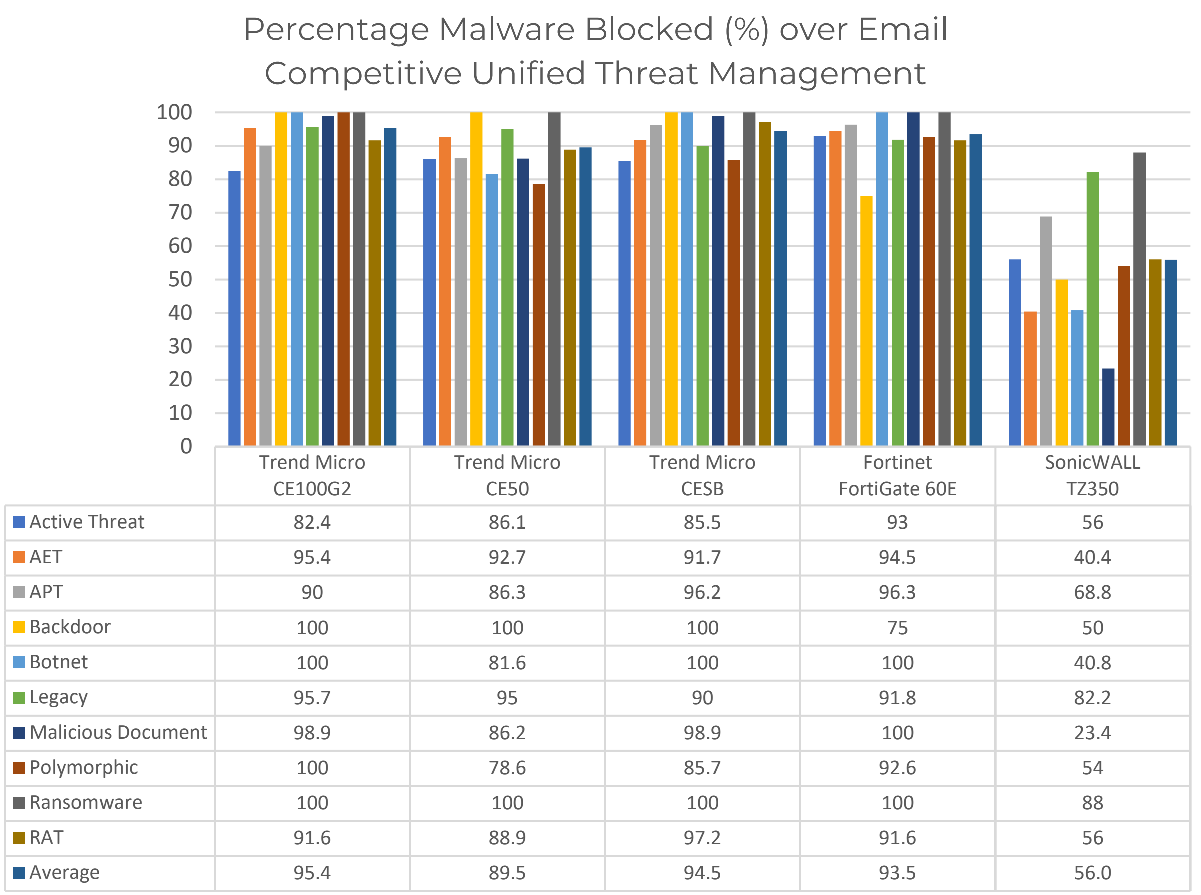
Source: Miercom 2019

All malware samples were delivered to target hosts using an FTP server. We expected similar, if not identical, results to the HTTP/HTTPS analysis since the devices' antivirus engines were the same across protocols. In general, detection efficacy observed for all vendors over FTP was less than over HTTP/S. Trend Micro was the only vendor to see increased detection of active threats, by as much as 4 percent. The Cloud Edge 50 was only UTM product whose security efficacy remained the same on FTP as it was on HTTP/S. Most vendors saw an overall average degradation of about 10 percent.

5.2 Email Security

Attackers know billions of emails are sent and received each day – making it the perfect medium for convenient access and manipulation of business networks. UTM devices should inspect emails for malicious payloads via standard protocols such as SMTP/S, IMAP/S and POP/S. Malicious content should be blocked and removed, and the email marked accordingly before forwarded to the recipient.

To test the email security feature of each UTM, email accounts were simulated and used to deliver malware samples to an unprotected victim behind the protection of the device under test.



	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FortiGate 60E	SonicWALL TZ350
■ Active Threat	82.4	86.1	85.5	93	56
■ AET	95.4	92.7	91.7	94.5	40.4
■ APT	90	86.3	96.2	96.3	68.8
■ Backdoor	100	100	100	75	50
■ Botnet	100	81.6	100	100	40.8
■ Legacy	95.7	95	90	91.8	82.2
■ Malicious Document	98.9	86.2	98.9	100	23.4
■ Polymorphic	100	78.6	85.7	92.6	54
■ Ransomware	100	100	100	100	88
■ RAT	91.6	88.9	97.2	91.6	56
■ Average	95.4	89.5	94.5	93.5	56.0

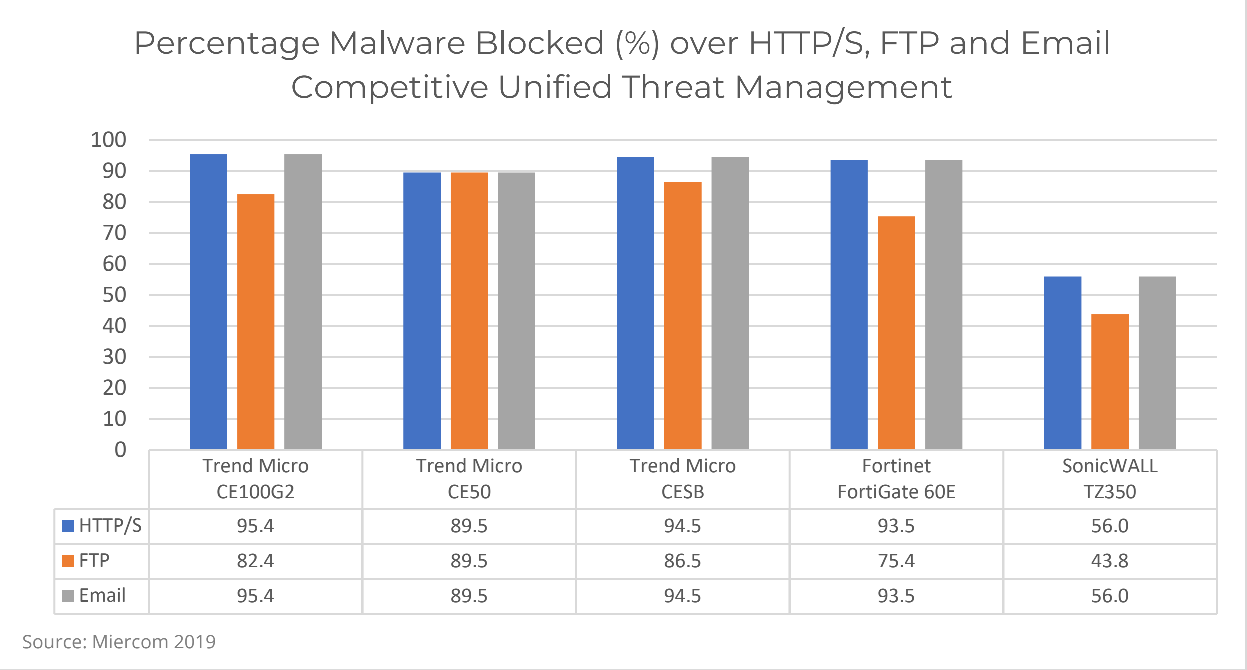
Source: Miercom 2019

All vendors were able to detect 100 percent of the malware samples over email protocols as those tested in Section 5.1 – resulting in the same efficacy rates as the HTTP/S test. Trend Micro detected as much as 95.4 percent of all threats – the highest efficacy score of all competing vendors.

5.3 Summary of Malware Detection

Malware sets were delivered through different protocols, averaged and compared for each UTM device. Detection was analyzed using the same set across three major Internet protocol suites: HTTP/S, FTP, and unencrypted and encrypted mail.

Malware was initially downloaded from our proprietary malware server over HTTP and FTP through the UTM device to a victim endpoint. We expected samples to be detected by each device for unencrypted protocols; failure to do so implied the inability to detect malware. Results were expected to be the same or lower for HTTPS and email – more complicated protocols to inspect for malware.



Percentage Malware Blocked (%) over HTTP/S, FTP and Email
Competitive Unified Threat Management

	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FortiGate 60E	SonicWALL TZ350
🟦 HTTP/S	95.4	89.5	94.5	93.5	56.0
🟧 FTP	82.4	89.5	86.5	75.4	43.8
■ Email	95.4	89.5	94.5	93.5	56.0

Source: Miercom 2019

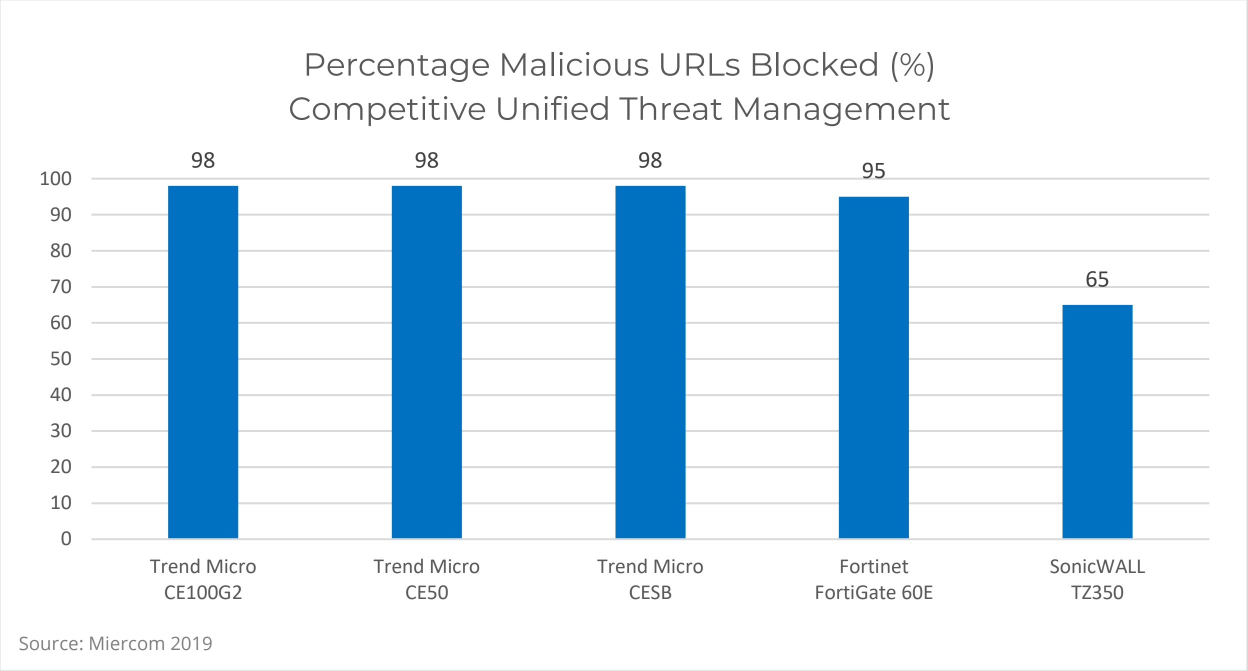
Malware detection efficacy for HTTP/S and email protocols were the same for each UTM product. Detection across FTP was an average of 10 percent lower, except for the Trend Micro CE50 which had the same security efficacy regardless of protocol type.

5.4 URL Filtering

A UTM device is the first line of defense during Internet access. It can prevent users from reaching malicious locations which put the endpoint and network at risk for infection. The UTM device should block known, harmful locations regardless of an attacker's antivirus bypassing technique.

Malicious locations change quickly, so our proprietary malware suite used a new set of malicious URLs. All UTM devices were assessed simultaneously to ensure comparable URL filtering results.

Automated scripts simulated an endpoint attempting to access each website through the UTM device. If the site was reached, it received a failing mark. If the UTM product makes the site inaccessible, or a block page is displayed, the sample was reported as blocked. Results were recorded as a percentage of blocked URL samples out of the total samples attempted.



Source: Miercom 2019

The Trend Micro Cloud Edge series blocked 98 percent of malicious URL samples access by the victim end user, 3 percent higher than Fortinet and 33 percent higher than SonicWALL.

5.5 Intrusion Prevention System

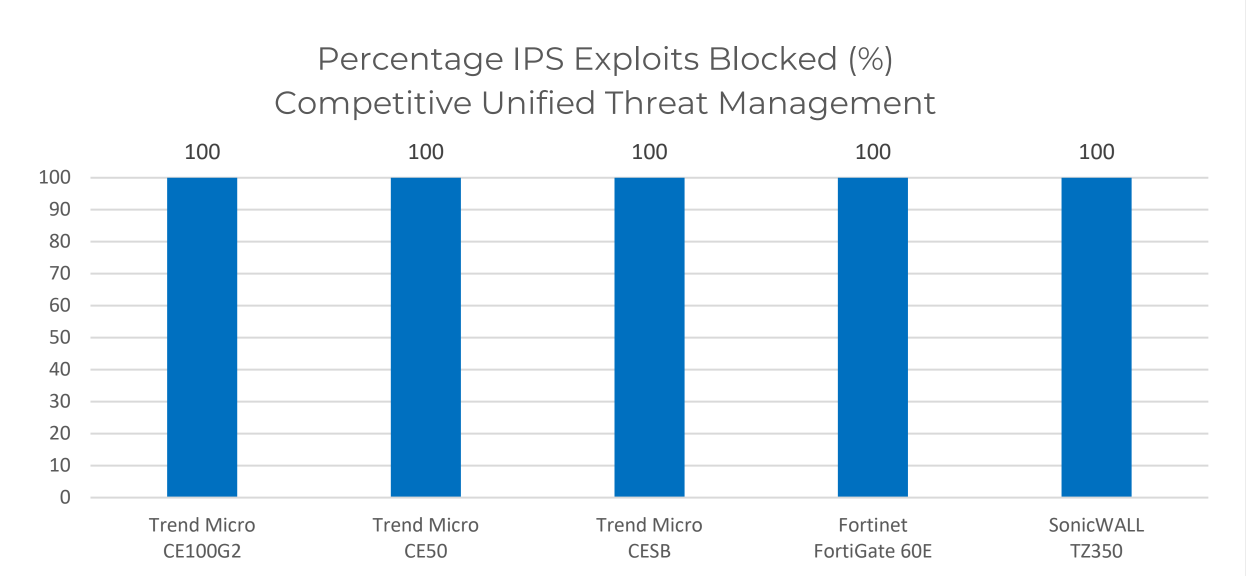
An Intrusion Prevention System (IPS) is a refined security feature that continuously monitors a network for malicious activity to immediately alert an administrator for remediation. Preventative actions may include adjustments to configurations, policies or access control.

The Ixia BreakingPoint tool uses a Critical Strike Pack – a dynamic collection of evolving attacks updated with hundreds of current, dangerous exploits and vulnerabilities – to reflect a real-world threat scenario. Using the IPS Strike List, we assessed each UTM device for its threat detection efficacy.

BreakingPoint Strike is an attack suite containing:

- Over 6,000 strikes (SQL injections, cross-site scripting, buffer overflow)
- Natively implemented exploits, as opposed to capture replayed events
- Over 100 evasion techniques to hide attacks from security
- Over 35,000 malware
- Distributed Denial-of-Service (DDoS) attacks in parallel with application traffic (L2 through L4)
- Fragmentation, flood and DNS reflection attacks

Blocking of exploitive traffic is logged by the Ixia BreakingPoint. The amount blocked out of the total samples of the IPS Strike List are recorded below.



Source: Miercom 2019

Trend Micro Cloud Edge blocked 100 percent of exploits designed to challenge the IPS feature of the tested UTM devices.

5.6 Application Control

Application control enables UTM devices to allow or restrict specific traffic types to promote user productivity and reduce downtime. This cornerstone technology keeps networks secure and users focused on workloads.

Based on rule-matching and scanning engines built into the UTM firewall, administrators use application control to selectively disable specific applications such as instant messaging (IM) platforms, peer-to-peer (P2P) networks, file transfers, social media tools, online gaming and more behaviors unrelated to work tasks.

Many of these applications carry a large potential for attacks; high-encryption IM platforms like Telegram or Signal can exfiltrate data or infiltrate malware through the firewall. File transfer and P2P networks are an additional legal liability and security risk.

To test for meaningful application control offered by the UTM devices, we attempted to perform the following test cases:

- **Online Messaging**: We attempted a Skype call without and with application control enabled
- **File Transfer**: We attempted a Bit-torrent transfer using a known server and well-known port 6881
- **Games**: We attempted to run Steam client and download some games
- **Encrypted Traffic**: We attempted to use Tor to navigate the dark web
- **Video Streaming**: We attempted to view videos on Netflix, Hulu and HBOGO
- **Mobile Applications and Downloads**: We used Google Play on devices connected to UTM

We began by testing each scenario with the Application Control feature disabled, or set application-specific policies to *allow* access in devices that cannot disable Application Control (such as the Trend Micro Cloud Edge Series).

Next, we enabled Application Control, or disable application-specific policies which allowed such behavior and found each UTM devices quickly blocked traffic from each scenario. All attempts to engage unauthorized behavior were successfully prevented.

6.0 Performance

Network performance is dependent on the amount of processing required. Security requires many high-quality services that typically require a sacrifice in performance. While UTM devices aim to provide enhanced network security, another goal is minimizing processing loads to maintain competitive performance. UTM devices capable of optimally balancing security and performance with superior engineering design are the first to be considered for organizational security.

Throughput tests were performed with the UTM device deployed inline using a single 1-Gigagbit Ethernet (GbE) port pair, with egress to WAN and ingress to LAN. Some products offer more than a single port pair, but most UTM deployments use a single 1-GbE port configuration. Any discrepancy between observed and published datasheet values reflect this implementation.

Before running performance tests, normal traffic flow through the UTM device is verified. We observed throughput rates using two scenarios: Stateless and Stateful Traffic.

Both Intrusion Prevention System (IPS) and Antivirus (AV) functionality were verified prior to testing using Ixia BreakingPoint Strike exploit packs. Throughput was recorded as the maximum rate before packet loss occurs.

For both scenarios, we recorded throughput rates for:

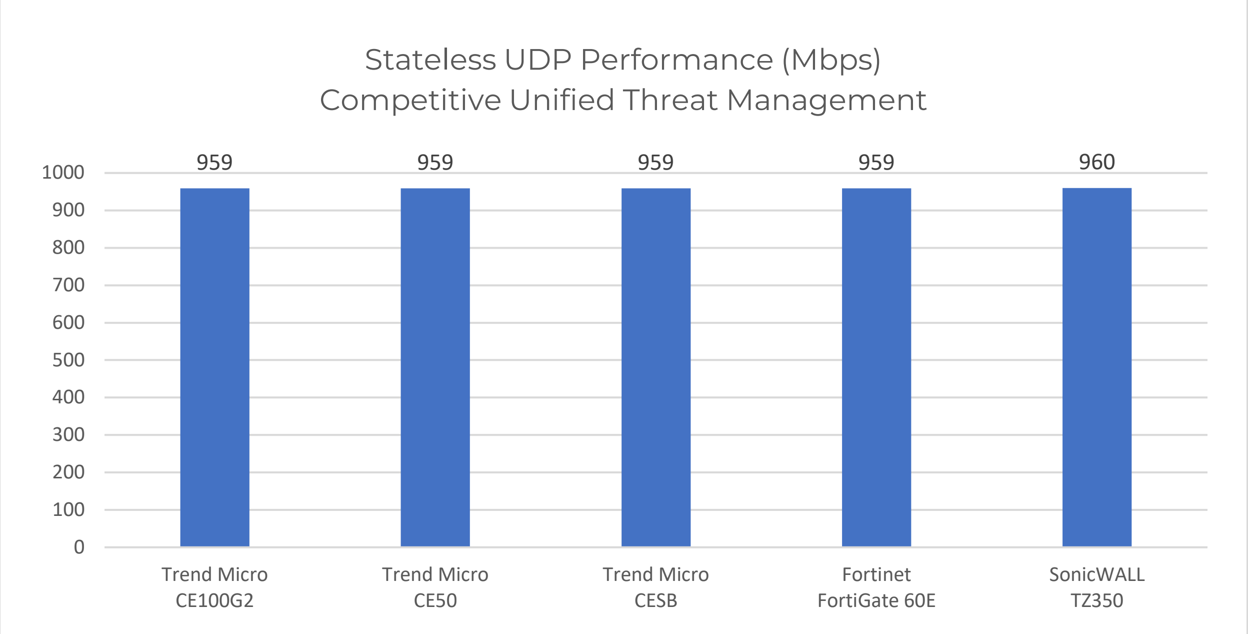
- Firewall (FW)
- Firewall and Application Control (FW+AppCtrl)
- Firewall, Application Control and Intrusion Prevention System (FW+AppCtrl+IPS)
- Firewall, Application Control and Antivirus (FW+AppCtrl+AV)
- Full Unified Threat Management (UTM)

The impact of deploying the additional features is quantified as observed performance degradation associated with each security configuration. Our testing intended to validate how Trend Micro Cloud Edge 100G2/50/SB have minimal performance degradation as a result of enabled features in comparison to similar UTM products.

6.1 Stateless Traffic Performance

Before looking at realistic performance, we first observed the ideal routing maximum rate by routing as many datagrams or packets per second through the WAN interface to the LAN side. Layer 3 UDP/TCP packets were generated and routed through the UTM device under test. Throughput in megabits per second (Mbps) for each frame size was measured for firewall enabled only and recorded as the maximum throughput capacity before packet loss occurs.

Results



Source: Miercom 2019

Trend Micro Cloud Edge 100G2/50/SB products showed comparable stateless throughput at 959 Mbps.

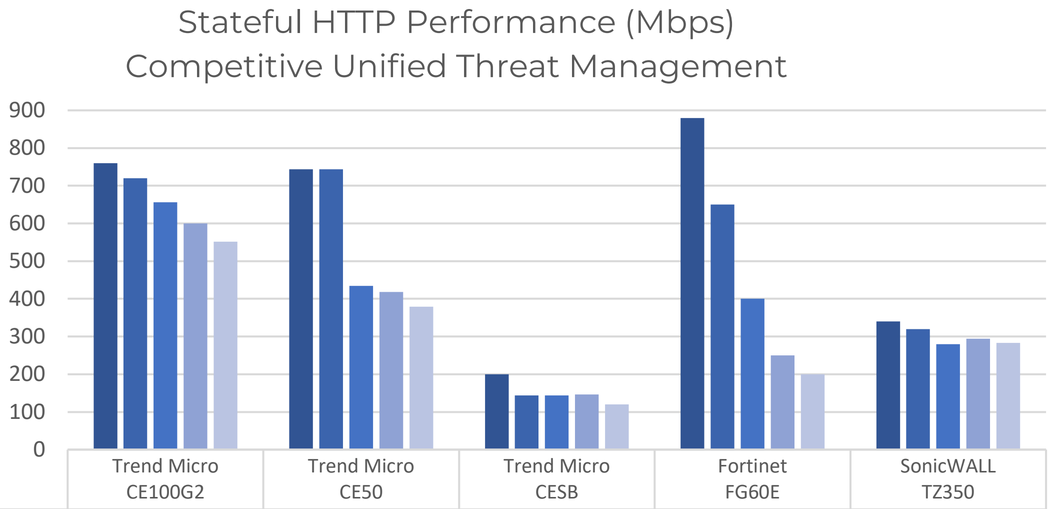
6.2 Stateful Traffic Performance

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. Firewall throughput was expected to yield the highest performance. UTM 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.

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 over HTTP and HTTPS, where the number of client streams varied randomly from 1 to 500. Traffic was increased until transactions began to fail. 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.

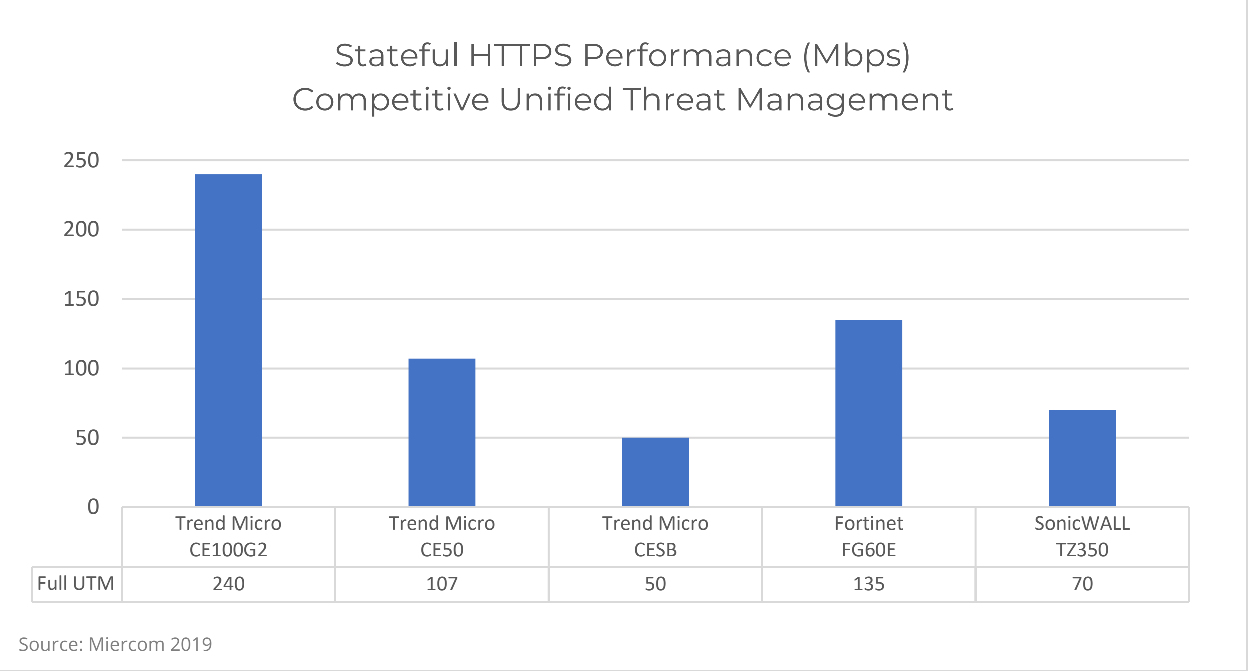
Results



	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FG60E	SonicWALL TZ350
■ FW	760	744	200	880	340
■ FW + AppCtrl	720	744	144	650	320
■ FW + AppCtrl + IPS	656	434	144	400	280
■ FW + AppCtrl + AV	600	418	146	250	294
■ Full UTM	552	379	120	200	283

Source: Miercom 2019

Trend Micro Cloud Edge CE100G2 had the highest UTM throughput of all competing devices at 552 Mbps – outperforming its competitions by as much as 64 percent. The Trend Micro CE100G2 and CE50 had the highest throughput for all configurations except basic firewall routing.



	Trend Micro CE100G2	Trend Micro CE50	Trend Micro CESB	Fortinet FG60E	SonicWALL TZ350
Full UTM	240	107	50	135	70

Source: Miercom 2019

Trend Micro Cloud Edge CE100G2 had the highest encrypted UTM throughput of all competing devices at 240 Mbps, outperforming its competitors by as much as 71 percent.

7.0 Quality of Experience

A UTM product may be excellent in terms of security and speed, but quality of experience 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 reporting.

7.1 Management and Deployment

The devices tested are intended for small business deployments which typically have limited IT resources or expertise in the deployment of security devices. Therefore, the best solutions require a comprehensive and simplistic user interface.

The commands and controls differ by vendor. We found Trend Micro had the easiest security settings and AV logs to configure. This differentiated the Trend Micro Cloud Series UTM as an excellent choice for reducing deployment and management complexity to avoid misconfiguration errors.

Miercom Tip: Miercom recommends the use of a test file for assessing a UTM security configuration (e.g. EICAR file as an email attachment to the internal mail server). An undetected test file reveals a misconfiguration that allows inbound mail to become an attack vector.

Below is an overview of important features and capabilities for manageability and ease of use. Any differentiators impact based on 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 remotely.

	Trend Micro CE Series	Fortinet FortiGate 60E	SonicWALL TZ350
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	●	●	

Out-of-box deployment and management are expected to be simple and intuitive. While products may provide organized information, some have overwhelming consoles. End users can be more productive and accurate when using a management-friendly interface. We observed product setup, organization, visibility and aesthetic and found the following positive features:

Trend Micro CE Series

- Cloud management simplifies policies and central management of multiple devices
- Configurable dashboard using pre-defined widgets
- Easy event analysis with filters to view specific devices or end points
- Customizable log can be switched to a graphical overview with 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 60E

- Smooth user interface with conventional monitoring and configuration layout in left panel
- Configurable user dashboard widgets provide end user customization
- Simple log and report view with specific event details in a collapsible display on the right side; events are assigned threat scores to help the end user understand the severity
- Useful security audit feature for identifying configuration shortcomings
- Built-in help links and highlighting is very useful for trying to solve configuration shortcomings

SonicWALL TZ350

- Quick configuration choices make deployment very easy
- Helpful advanced settings in the web-based ‘diag’ page
- Internal Packet Capture helps with troubleshooting
- Ability to switch between new and old GUI is helpful for older guides and tech support
- Viewable and downloadable actions for sandboxed files when analyzing problems
- 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	Fortinet FortiGate 60E	SonicWALL TZ350
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 unique features: email tagging, cloud console, machine learning and business email malware detection. 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 a tag to inform the sender and receiver of detected, and removed, malware. The console gives a real-time update of found malware, showing an increase in the Email Anti-Malware count.

If a non-malicious email is identified as malicious and blocked, this feature alerts the end user of malicious content origins and allows rule applications for versality and visibility of specific end users or groups. The email is cleaned of the malicious attachment, the subject is tagged, and the body of text includes a statement regarding content removal. Tagging avoids deleting the entire message and quarantines the emails instead for end user awareness and control.

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 cloud technology. It is used to analyze and detect security risks that were not seen before or have no signatures 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 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.