ARISTA

Edge Threat Management

Data Sheet

Key Features

Advanced Security

- Protection, encryption, control & visibility
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

Intelligent Edge Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Optimal predictive routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

Cloud Management at Scale

- Zero touch deployment with auto-provisioning VPN
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

Network Security Simplified

The way we work is evolving. Businesses have adapted to new cloud-based technologies and applications that have increased employee efficiency and provided a scalable pathway to continued business growth. Work teams, now composed of employees working in headquarter offices, remotely, or branch offices, have become spread across increasingly large distances. While businesses realize a range of important benefits in this transformative era, managing these dispersed networks and their connected devices can bring new challenges of cost, complexity, and control.

NG Firewall and Micro Edge provide edge threat management and a comprehensive approach to network security orchestration. The suite of cloud-managed security and connectivity options work together to fit the needs of mid-sized businesses and distributed organizations. This integrated approach provides network administrators with the ability to ensure protection, monitoring and control across devices, applications, and events, enforcing a consistent security posture over the entire digital attack surface.

Centralized Cloud Based Management

One or many NG Firewall and Micro Edge appliances can be managed from any browser. Full visibility of all deployments in one single pane of glass view enables administrators to view appliance network status, important events, reporting data and push global configurations.

Simplified Device Management

Reduce management overhead by handling a range of tasks remotely. View appliance status at a glance, including uptime, bandwidth utilization, and network traffic summaries. Manage licensing, software updates, backups, alerts and more. Monitor connected endpoints on the network, get alerts when threats are detected, and initiate an endpoint protection scan. Real-time firewall, router and endpoint status alerts help with site management and maintaining regulatory compliance.

Zero Touch Deployment

Deploy and configure new NG Firewall or Micro Edge hardware appliances remotely. Zero touch deployment reduces the amount of time needed and complexity of deployment by eliminating the need to configure the appliance from the local network.

Network Orchestration

Group NG Firewall and Micro Edge appliances together via VPN creating a mesh network. Automatically connect appliances with auto-provisioning VPN, and view aggregated performance data for the entire network. Create shared WAN routing policies for Micro Edge appliances.

Security, Visibility & Control

NG Firewall simplifies network security with a single, modular software platform designed to fit the evolving needs of mid-sized and distributed organizations. NG Firewall provides a browser-based, responsive and intuitive interface enabling network administrators to quickly gain visibility into the traffic on the network. From content filtering to advanced threat protection, and VPN connectivity, NG Firewall delivers a bulletproof network security platform.

NG Firewall Features

NG Firewall is exceptionally easy to use with a simple app based graphical UI allowing administrators to tailor NG Firewall for specific network needs.

Comprehensive Security at the Gateway

Proactively stop malware, hacking attempts, phishing schemes and other threats before they reach users' devices.

Next-Generation Filtering

Get a handle on every rogue application, encrypted web request, malware distribution point, drive-by malvertising attempt, and rash of spam.

Deep Analysis and Insights

Gain valuable insights from database-driven reports without the need for a separate appliance. See the network status at a glance on the dashboard, ensure compliance with full event logs, and get notifications of threats, anomalies or unusual user behavior with alert rules.

Superior Connectivity & Performance

Meet the challenges of a remote workforce, branch offices and guest Wi-Fi. Keep users and data safe regardless of location or level of access. Balance competing priorities, ensure Quality of Service (QoS), and maximize uptime.

Protect

Proactively block malware, phishing, spam, hacking and other exploits from reaching users and devices on the network.

Firewall

Safeguard the network from Internet threats with control by IP address, protocol and port. Administrators can designate which systems and services (HTTP, FTP, etc.) are publicly available. Firewall can be run as a transparent bridge to complement a pre-existing firewall and allows administrators to control inbound and/or outbound access to specific IPs and ports.

Intrusion Prevention

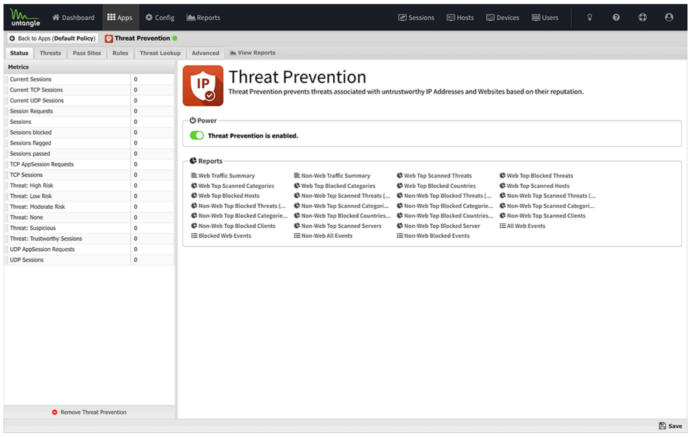
Stop exploits before they enter the network. Pre-configured signature-based IPS makes it easier for administrators to provide 24/7 network protection from hackers. It minimizes annoying false positives and ensures that signatures are always current with automatic updates. With an easy-to-use setup wizard allowing simple configuration of rules specific to each environment, Intrusion Prevention provides flexible control. Over 34,000 signature detections, including heuristic signatures for port scans, enable you to effectively monitor and block most suspicious requests.

Phish Blocker

Protect unsuspecting, click-happy users from identity theft attempts. Phish Blocker protects users from email phishing attacks and fraudulent pharming websites, and allows you to enable (or disable) the scanning of SMTP emails and take the appropriate action: Mark, Pass, Drop or Quarantine.

Threat Prevention

Block access to web and application content based on an analysis of the IP address's reputation. IP address reputation scoring is based on the Webroot BrightCloud® IP Reputation Service. This intelligent, real-time packet inspection categorizes IP addresses into five distinct categories – High Risk, Suspicious, Moderate Risk, Low Risk, and Trustworthy.



Metrics	
Current Sessions	0
Current TCP Sessions	0
Current UDP Sessions	0
Session Requests	0
Sessions	0
Sessions blocked	0
Sessions flagged	0
Sessions passed	0
TCP AppSession Requests	0
TCP Sessions	0
Threat: High Risk	0
Threat: Low Risk	0
Threat: Moderate Risk	0
Threat: None	0
Threat: Suspicious	0
Threat: Trustworthy Sessions	0
UDP AppSession Requests	0
UDP Sessions	0

Threat Prevention

Threat Prevention prevents threats associated with untrustworthy IP Addresses and Websites based on their reputation.

Power

Threat Prevention is enabled.

Reports

Web Traffic Summary
Web Top Scanned Categories
Web Top Blocked Hosts
Non-Web Top Blocked Threats (...
Non-Web Top Blocked Categorie...
Non-Web Top Blocked Clients
Blocked Web Events
Non-Web Traffic Summary
Web Top Blocked Categories
Non-Web Top Scanned Threats (...
Non-Web Top Scanned Categori...
Non-Web Top Blocked Countries...
Non-Web Top Scanned Servers
Non-Web All Events
Web Top Scanned Threats
Web Top Blocked Countries
Non-Web Top Blocked Threats (...
Non-Web Top Blocked Categorie...
Non-Web Top Blocked Countries...
Non-Web Top Blocked Server
Non-Web Blocked Events
Web Top Blocked Threats
Web Top Scanned Hosts
Non-Web Top Scanned Threats (...
Non-Web Top Scanned Categori...
Non-Web Top Scanned Clients
All Web Events

Figure 1: NG Firewall Threat Prevention

Virus Blocker

Virus Blocker stops viruses at the gateway by leveraging signatures from Bitdefender™, the leader in speed and efficacy in identifying emerging threats. Heuristic models provide an additional layer of protection against zero-day threats, and real-time updates with no system downtime ensure that your network is always protected. Virus Blocker identifies and blocks zero-day threats, viruses, worms, Trojan horses, botnets, unknown malware, and new infections.

Filter

Get a handle on every rogue application, encrypted web request, malware distribution point and rash of spam.

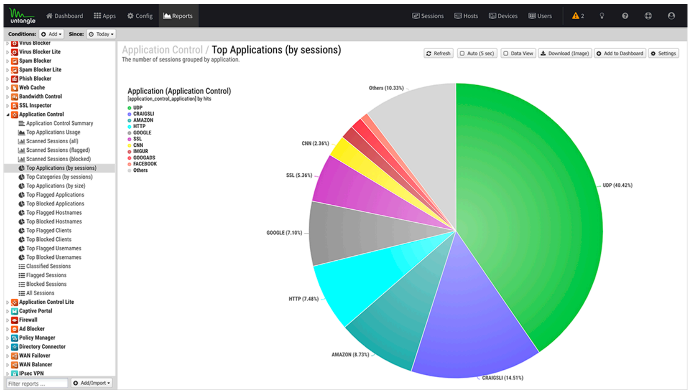
Ad Blocker

Eliminate ad and cookie tracking, while improving webpage load times. Based on the open source project AdBlock Plus, Ad Blocker lets you easily block ads at the gateway without installing browser plugins. Ad Blocker prevents malware and scams through banner ads while reducing traffic on the network.

Application Control

Control access to applications, which can be productivity drains and bandwidth hogs. Application Control performs deep packet (DPI) and deep flow (DFI) inspection of network traffic, enabling it to accurately identify thousands of common applications such as social networking, P2P, instant messaging, video streaming, file sharing, enterprise applications and much more.

Make sure that your users can access mission-critical and cloud-based apps while keeping recreational or inappropriate apps off the network. Application Control works in concert with Web Filter, SSL Inspector, Bandwidth Control and Policy Manager to give you the tools you need to enforce your user policies.



Application Control / Top Applications (by sessions)

The number of sessions grouped by application.

Figure 2: NG Firewall Application Control Report

Spam Blocker

Filters and quarantines fraudulent email—spam, phishing and email fraud—preventing it from reaching your users. Its smart analysis delivers a catch rate of 99.5% while minimizing false positives. Spammers constantly adjust their content and tactics to evade spam blockers. Spam Blocker is updated in real-time to keep you one step ahead of spammers. Quarantine is automatic and maintenance-free.

SSL Inspector

Decrypt, scan and re-encrypt HTTPS and SMTP traffic on the fly. SSL Inspector creates a specialized certificate on each client. This certificate communicates directly with the gateway which is then able to decrypt HTTPS and SMTP traffic, process, and re-encrypt it without ever exposing the decrypted traffic to the network. This enables HTTPS traffic to be inspected in the same way as regular HTTP traffic, meaning that all NG Firewall apps and their rules can be applied.

Web Filter

Block inappropriate content at the gateway before it reaches users. Allow, block, flag or alert by category to easily set up rules that meet your criteria. Web Filter allows you to monitor and control searches across popular search engines including Google, YouTube, Ask, Bing, and Yahoo. You can also enforce safe search on YouTube, as well as log searches, giving you an unprecedented degree of visibility and control, ideal for content-sensitive environments like schools, public libraries, and social services organizations.

Perform

Ensure network performance, maximum uptime and QoS to increase productivity.

Bandwidth Control

Manage the priority of business-critical, recreational and inappropriate traffic. Ensure Quality of Service (QoS), utilize bandwidth resources efficiently, and prioritize bandwidth toward business-critical apps like VOIP, cloud-based business applications, or video conferences. Combine Bandwidth Control with Policy Manager to define different actions based on policies (user, group, time of day, etc.).

WAN Balancer

Distribute Internet traffic to optimize QoS over two or more connections. WAN Balancer helps you maximize your cumulative network performance and throughput by distributing the traffic based on simple rules. It also enables you to combine multiple commodity Internet connections into a cost-effective alternative to pricey high-bandwidth connections.

WAN Failover

Reroute traffic automatically when one Internet connection fails. WAN Failover continually tests your Internet connections, and when one slows or fails, it can reroute network traffic over the remaining connections, maximizing your uptime. WAN Failover also logs all downtime for each connection, arming you with the evidence you need to hold your ISPs accountable.

Web Cache

Streamline and accelerate users' Internet browsing experience. Web Cache enables cached elements to be shared by all Internet users on your network increasing the responsiveness of web applications and reducing the bandwidth load.

Connect

Maintain visibility and control over remote workers, branch offices and guest Wi-Fi to keep users connected and data safe.

Captive Portal

Easily manage Wi-Fi and guest access to the Internet. With Captive Portal you can require users to view or accept an Acceptable Use Policy before accessing the Internet (e.g. public WiFi), authenticate users against Local Directory, RADIUS or Microsoft Active Directory (requires Directory Connector), and separate mobile devices to a different rack with different policies for BYOD (bring your own device) environments.

IPsec VPN

Provide seamless, secure network access for branch offices and remote employees. Uses cutting-edge security technology, supporting full tunnel or split tunnel, integrated with L2TP and Xauth. NG Firewall will detect VPN tunnel states immediately and automatically restart a tunnel in the event of downed connection.

OpenVPN

Enables SSL-based VPN that supports both site-to-site and client-to-site tunnels. OpenVPN can run as a server allowing for remote clients to connect to the Untangle server, and the OpenVPN application can connect to other remote servers as a client.

Tunnel VPN

Provide connectivity through encrypted tunnels to remote VPN servers and services. Tunnel VPN features a configuration wizard to enable connections to many privacy VPN providers like ExpressVPN or NordVPN. Tunnel VPN is for connecting NG Firewall as a client to a remote server or service.

WireGuard VPN

Build secure, fast, and cutting-edge connections between sites and to remote users. For networks with one or more branch offices or locations, WireGuard VPN creates an encrypted tunnel, enabling them to function as a single virtual network. Site-to-site tunnels with WireGuard VPN have very little overhead which ensures network bandwidth is maintained.

Manage

Create policies by user, group, device, and time to control access. Get complete visibility into network activity and traffic.

Directory Connector

Use Microsoft Active Directory or RADIUS to power policy management. Users can quickly and easily authenticate to the network, providing smooth, secure, and seamless access to the network. Network administrators gain visibility to each user as they authenticate, and can assign them to groups in the directory, simplifying and augmenting policy management.

Policy Manager

Define and manage network privileges based on usernames, groups, time, day or protocol. Policies provide a way to segment network traffic to provide completely separate configurations for traffic processing. For example, in a school network you could allow teachers to access Facebook but not students.

Additionally, administrators can configure multiple applications in separate policies simultaneously using the Parent Policy system. Parent Policies provide a tiered organization of policies providing global policies at the Parent Policy level that apply to all traffic, and additional more customized policies for "child" tiers or levels below the Parent Policy.

Reports

Drill down into any feature or across all features by user, group, time and more. Comprehensive, or summary reports can also be distributed automatically via email to key stakeholders.

Configuration Backup

Enables recovery from hardware failures and disasters, and configuration profiles to be shared across multiple deployments of NG Firewall.

Branding Manager

Personalize user-facing screens to add company logo, name and contact information.

Zero-Touch Provisioning

Network administrators can remotely set up and configure NG Firewall without having to be on site. Automatic upgrades ensure all appliances are kept up to date with the latest security updates and enhancements.

Centralized Management

One or many NG Firewall appliances can be managed from any browser. Full visibility of all deployments enables administrators to view appliance network status, important events, reporting data and push global configurations.

Deploying NG Firewall

NG Firewall can be deployed in various ways allowing you to choose the best deployment method for your network. Use a dedicated NG Firewall hardware appliance and drop it into your network with zero touch deployment, or use your own hardware that meets the hardware requirements. NG Firewall can also be deployed on a virtual machine, or in the cloud with AWS or Azure.

Model Number	CCA-ETM-Q8	CCA-ETM-Q8W	CCA-ETM-Q12	CCA-ETM-Q20
Recommended Devices	Up to 250	Up to 250	Up to 1500	Up to 5000
Processor	Quad core Intel Atom C3558 with AES Max Frequency: 2.2 GHz	Quad core Intel Atom C3558 with AES Max Frequency: 2.2 GHz	Quad core Intel Xeon E3-1225 v5 Max Frequency: 3.7 Ghz	Six core Intel Xeon E-2176G Max Frequency: 4.7 Ghz
RAM	8GB DDR4 2400Mhz	8GB DDR4 2400Mhz	16GB DDR4 @2133Mhz	32GB DDR4 @2666Mhz
Storage	128 GB SATA DOM	128 GB SATA DOM	512 GB NVMe SSD	512 GB NVMe SSD
Interfaces	4x GbE / 2x SFP+ / 2x PoE+	4x GbE / 2x SFP+ / 2x PoE+	8x GbE / 4x SFP	17x GbE / 4x SFP+
USB ports	2	2	2	2
Video	Mini USB and RJ45	Mini USB and RJ45	HDMI	HDMI
Wireless	-	802.11 b/g/n/ac MU-MIMO w/ Beam Forming	-	-
External Antennas	-	2	-	-
Form Factor	Desktop (Rack Mount Option)	Desktop (Rack Mount Option)	1U Rackmount	1U Rackmount
Firewall Throughput	9.4 Gbps	9.4 Gbps	950 Mbps	8.5 Gbps
NGFW Throughput*	870 Mbps	870 Mbps	950 Mbps	2 Gbps
Dimensions (HxWxD)	9.8″ x 9.9″ x 1.7″ (250 x 252 x 44mm)	9.8″ x 9.9″ x 1.7″ (250 x 252 x 44mm)	17.2″ x 16.9″ x 1.7″ (438 x 430 x 44mm)	17.2″ x 21.8″ x 1.7″ (438 x 553 x 44mm)
Unit Weight	4 lbs (1.8 kg)	4 lbs (1.8 kg)	14 lbs (6.4 kg)	21 lbs (9.5 kg)
Shipping Weight	8 lbs (3.6 kg)	8 lbs (3.6 kg)	23 lbs (10.4 kg)	32 lbs (14.5 kg)
Operating Temperature	32° – 104°F (0° – 40°C)	32° – 104°F (0° – 40°C)	32° – 104°F (0° – 40°C)	32° – 104°F (0° – 40°C)
Power Supply	12V5A Adapter / 54V1.2A Adapter (PoE+)	12V5A Adapter / 54V1.2A Adapter (PoE+)	250 Watt	Dual 300W (Redundant PSU)
Certifications	CE/FCC/UL	CE/FCC/UL	CE/FCC/UL	CE/FCC/UL

*NGFW throughput is measured with Application Control, IPS, Web Filter, Virus Blocker and Reports.

Warranty

Appliances come with a one-year limited hardware warranty, which covers parts, repair, or replacement. A 3-year hardware warranty is also available for purchase.

Optimize Your Network from Edge to Edge

Micro Edge is a lightweight device with advanced connectivity and security capabilities enabling businesses to have a secure network edge. Micro Edge provides secure branch connectivity, optimizes existing internet infrastructure, and prioritizes business critical applications to maximize employee productivity. As the network expands, Micro Edge seamlessly scales to ensure the network edge remains connected and protected.

Seamless Connectivity to Branch-offices and Business Continuity

Micro Edge appliances have multiple WAN ports that balance network traffic in real-time over multiple Internet paths. Link monitoring and automatic failover eliminate network downtime. Zero Touch Deployment and centrally managed configuration profiles enable branch offices to be connected and protected in minutes.

Edge Optimization

Untangle's optimal predictive routing technology identifies application traffic at the first packet. This advanced technology prioritizes business critical traffic to ensure the network runs smoothly. Boost Internet connectivity with traffic shaping and QoS, and leverage real-time performance monitoring with WAN balancing to make the most of the available bandwidth.

Secure Network Edge

Micro Edge has a stateful firewall, Threat Prevention and Web Filter which block traffic that can cause harm to your network ensuring the network, data and users are protected from the ever increasing volume of cyberthreats. Encrypted traffic is a hotspot for hackers to hide malware or other malicious code. However, Threat Prevention and Web Filter can make assessments even if the traffic is encrypted and block harmful files or transmissions before they get onto the network. Web Filter blocks access to dangerous, inappropriate or distracting website content to protect the network and increase employee productivity. Threat Prevention ensures any web address accessed is not associated with any malware, hacking or malicious attacks.

Micro Edge Features

Application-based Optimization

Optimal predictive path selection technology incorporates a sophisticated cloud component to identify applications at the first packet. This advanced technology enables Micro Edge to choose the best path for specific applications or categories of network traffic.

Edge Optimization

Traffic shaping and Quality of Service prioritizes business critical traffic across WAN links.

Real-time Link Performance Monitoring

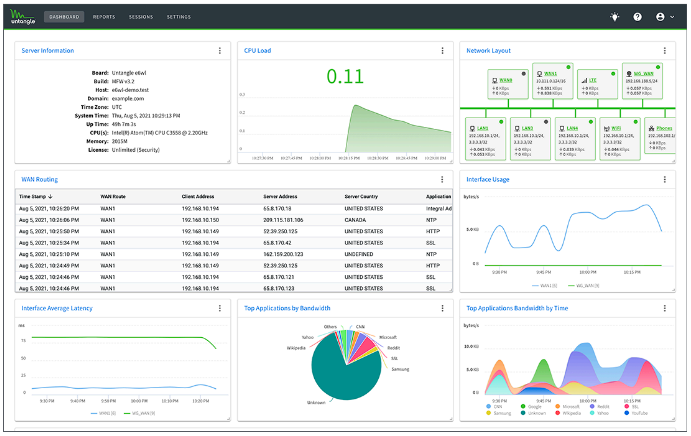
Jitter, packet loss, latency and throughput of each link are continually measured to ensure applications can be sent over the best performing links for their needs.

Dynamic Path Selection

Decisions on which links to use are made in real-time based on actual current link performance of packet loss, latency and jitter conditions, as well as available bandwidth.

Multiple Internet Pathways

Multiple WANs as well as LTE connectivity can be used as primary or failover links. Application based path selection can optimize performance over LTE and hard-wired links.



Server Information

Board: Untangle e6wl
Build: MFW v3.2
Host: e6wl-demo.test
Domain: example.com
Time Zone: UTC
System Time: Thu, Aug 5, 2021 10:29:13 PM
Up Time: 49h 7m 3s
CPU(s): Intel(R) Atom(TM) CPU C3558 @ 2.20GHz
Memory: 2015M
License: Unlimited (Security)

WAN Routing

Time Stamp ↓	WAN Route	Client Address	Server Address	Server Country	Application
Aug 5, 2021, 10:26:20 PM	WAN1	192.168.10.194	65.8.170.18	UNITED STATES	Integral Ad
Aug 5, 2021, 10:26:06 PM	WAN1	192.168.10.150	209.115.181.106	CANADA	NTP
Aug 5, 2021, 10:25:50 PM	WAN1	192.168.10.149	52.39.250.125	UNITED STATES	HTTP
Aug 5, 2021, 10:25:34 PM	WAN1	192.168.10.194	65.8.170.42	UNITED STATES	SSL
Aug 5, 2021, 10:25:10 PM	WAN1	192.168.10.149	162.159.200.123	UNDEFINED	NTP
Aug 5, 2021, 10:24:49 PM	WAN1	192.168.10.149	52.39.250.125	UNITED STATES	HTTP
Aug 5, 2021, 10:24:46 PM	WAN1	192.168.10.194	65.8.170.121	UNITED STATES	SSL
Aug 5, 2021, 10:24:46 PM	WAN1	192.168.10.194	65.8.170.123	UNITED STATES	SSL

Figure 3: Micro Edge Dashboard

Configurable Performance Thresholds

Network optimization can be configured at the application level with failover conditions specified using limits for desired maximum packet loss, or latency thresholds.

Automated Link Failover

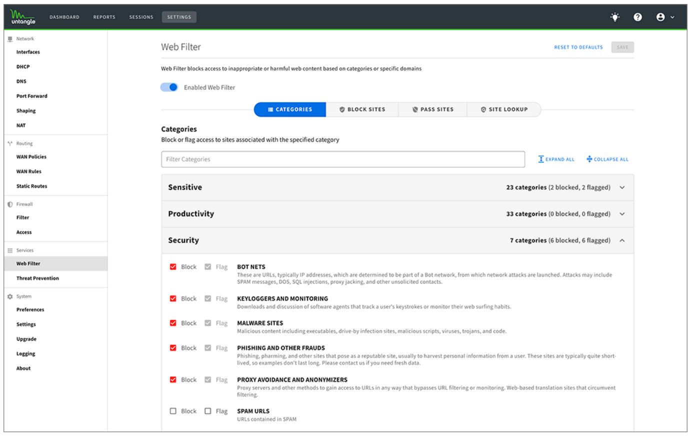
Network traffic will be sent over the next best performing link when a link fails, or fails to meet performance requirements.

Threat Prevention

Advanced security capability that blocks high risk Internet traffic using the Webroot BrightCloud® reputation score associated with the server hosting the service.

Web Filter

Protects the network and increases employee productivity powered by performing a real-time assessment, utilizing the Webroot BrightCloud®web classification and reputation database, and blocks access to dangerous, inappropriate or distracting website content.



Web Filter

Web Filter blocks access to inappropriate or harmful web content based on categories or specific domains

Enabled Web Filter

Categories

Block or flag access to sites associated with the specified category

Sensitive	**23 categories** (2 blocked, 2 flagged)
Productivity	**33 categories** (0 blocked, 0 flagged)
Security	**7 categories** (6 blocked, 6 flagged)

☑ Block ☑ Flag **BOT NETS**
These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.

☑ Block ☑ Flag **KEYLOGGERS AND MONITORING**
Downloads and discussion of software agents that track a user's keystrokes or monitor their web surfing habits.

☑ Block ☑ Flag **MALWARE SITES**
Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.

☑ Block ☑ Flag **PHISHING AND OTHER FRAUDS**
Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples don't last long. Please contact us if you need fresh data.

☑ Block ☑ Flag **PROXY AVOIDANCE AND ANONYMIZERS**
Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.

☐ Block ☐ Flag **SPAM URLS**
URLs contained in SPAM

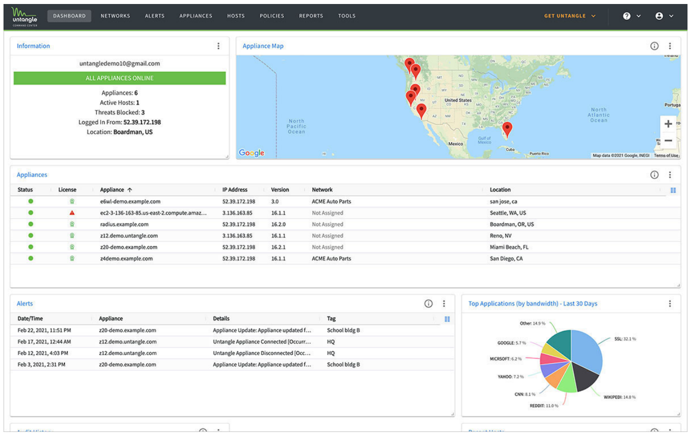
Figure 4: Micro Edge Web Filter

Zero-Touch Provisioning

Network administrators can remotely set up and configure Micro Edge without having to be on site. Automatic upgrades ensure all appliances are kept up to date with the latest security updates and enhancements.

Centralized Management

One or many Micro Edge appliances can be managed from any browser. Full visibility of all deployments enables administrators to view appliance network status, important events, reporting data and push global configurations.



Information

untangledemo10@gmail.com
ALL APPLIANCES ONLINE
Appliances: **6**
Active Hosts: **1**
Threats Blocked: **3**
Logged In From: **52.39.172.198**
Location: **Boardman, US**

Appliances

Status	License	Appliance ↑	IP Address	Version	Network	Location
●	✓	e6wl-demo.example.com	52.39.172.198	3.0	ACME Auto Parts	san jose, ca
●	▲	ec2-3-136-163-85.us-east-2.compute.amaz...	3.136.163.85	16.1.1	Not Assigned	Seattle, WA, US
●	✓	radius.example.com	52.39.172.198	16.2.0	Not Assigned	Boardman, OR, US
●	✓	z12.demo.untangle.com	3.136.163.85	16.1.1	Not Assigned	Reno, NV
●	✓	z20-demo.example.com	52.39.172.198	16.2.1	Not Assigned	Miami Beach, FL
●	✓	z4demo.example.com	52.39.172.198	16.1.1	ACME Auto Parts	San Diego, CA

Alerts

Date/Time	Appliance	Details	Tag
Feb 22, 2021, 11:51 PM	z20-demo.example.com	Appliance Update: Appliance updated f...	School bldg B
Feb 17, 2021, 12:44 AM	z12.demo.untangle.com	Untangle Appliance Connected [Occurr...	HQ
Feb 12, 2021, 4:03 PM	z12.demo.untangle.com	Untangle Appliance Disconnected [Occ...	HQ
Feb 3, 2021, 2:31 PM	z20-demo.example.com	Appliance Update: Appliance updated f...	School bldg B

Figure 5: Centralized management dashboard

Deploying Micro Edge

Micro Edge has multiple deployment options to fit into your existing IT environment. Choose one of our performance-optimized appliances, or use your existing infrastructure with a virtual appliance running on a hypervisor.

Model Number	CCA-ETM-Q6E	CCA-ETM-Q6EWL
Recommended devices	Up to 300	Up to 300
Processor	Intel C3558 Quad Core at 2.2 GHz	Intel C3558 Quad Core at 2.2 GHz
RAM	2 GB	2 GB
Storage	8 GB mSATA SSD	8 GB mSATA SSD
Interfaces	2x GbE SFP Combo / 4x GbE	2x GbE SFP Combo / 4x GbE
USB Ports	2	2
Video	Mini USB and RJ45	Mini USB and RJ45
Wireless	802.11 2X2 MU-MIMO ac/a/b/g/n	802.11 2X2 MU-MIMO ac/a/b/g/n
LTE	-	4G LTE Cat-6 AT&T, T-Mobile, or Verizon
External Antennas	-	2 WiFi / 2 LTE
Form Factor	Fanless Desktop	Fanless Desktop
Max Throughput	950 Mbps	950 Mbps
Dimensions (HxWxD)	9.1" x 6.9" x 1.7" (231 x 175 x 43mm)	9.1" x 6.9" x 1.7" (231 x 175 x 43mm)
Unit Weight	3.1 lbs (1.4 kg)	3.3 lbs (1.5 kg)
Shipping Weight	5.5 lbs (2.5 kg)	5.7 lbs (2.6 kg)
Operating Temperature	32° – 104°F (0° – 40°C)	32° – 104°F (0° – 40°C)
Power Supply	40W Power Adapter	40W Power Adapter
Certifications	CE/FCC/UL	CE/FCC/UL

Warranty

Appliances come with a one-year limited hardware warranty, which covers parts, repair, or replacement. A 3-year hardware warranty is also available for purchase.

Headquarters

5453 Great America Parkway
Santa Clara, California 95054
408-547-5500

Support

support@arista.com
408-547-5502
866-476-0000

Sales

sales@arista.com
408-547-5501
866-497-0000

www.arista.com

ARISTA

March 1, 2022