SD-Edge Services Overview

Firewall & Security

Secure Access Service Edge (SASE)

BENU NETWORKS

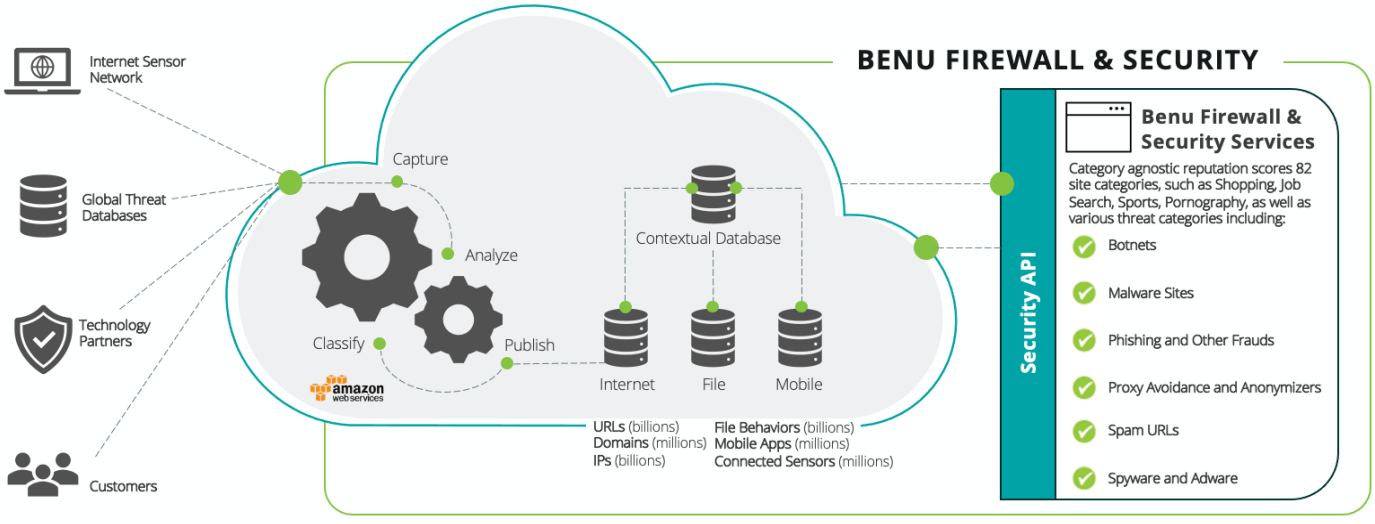
Upgrading From Traditional Firewalls

Traditional perimeter-only firewalls are no longer effective due to the high reliance on cloud-based applications and the limited budgets to provide deep-threat protection at every single business site and remote worker site. Furthermore, many sites have a large guest user base, such as in retail, education, healthcare, venues, MDUs, hospitality, and public WiFi networks. In all of these scenarios, there is a mix of trusted users (employees and staff), trust devices (Internet-of-Things), partially trusted users (vendors or suppliers), and untrusted users (guests).

For all these different types of users, even trusted users, Benu supports a zero-trust approach. Zero-trust security restricts users to only the parts of the network and applications that they need, thereby reducing the attack surface and minimizing access to sensitive parts of the network. Microsegmentation creates separate zones within the network to maintain separate layers of access to applications and network resources. In addition, unlike typical firewalls, Benu's SD-Edge platform supports per-user policy enforcement which is essential in environments with a high number of untrusted or partially trusted guests. These per-user policies include network access controls, QoS and rate limiting, content filtering, and data volume limits.

What Sets Benu Apart

Benu's carrier-class firewall is protecting over 24 million WLAN APs and the users behind them. Carrying over 7 Petabytes of traffic a day, Benu's firewall software is field proven for nearly a decade of broad commercial deployment. Trusted by the largest Tier-1 carriers in the world, Benu's SD-Edge software and firewall capabilities are currently used in a wide range of applications, from public WIFi networks to major venues, carrier broadband access networks, multi-dwelling units (MDUs), retail establishments, and hospitality.



For web security services, Benu provides unmatched visibility and knowledge across URLs, IP addresses, files, and mobile threats. Leveraging real-time deep packet inspection processing and machine learning, threat intelligence is always up-to-date and highly accurate.

Full URLs Not Just DNS

Benu conducts full URL path inspection by looking at web traffic, not just DNS (which is simply the domain). There is no DNS traffic if a person uses an IP address for the domain portion of the URL. This method allows us to detect and quarantine individual pages that have malware but are located on a generally benign domain. For example, if someone visits a domain that is considered safe, but then clicks on links that have been compromised on that same domain, these will be detected and blocked. In addition, if someone tries to force a different DNS (they change the DNS settings on their computer or router), we can still detect the malicious sites.

Web Security and Malware Protection

This service will inspect for any URL component against a database of pre-classified data containing billions of URLs, millions of domains, and billions of IP addresses. The URL component may be a fully qualified domain name, a full URL with path or an IP address that would be the host portion of the URL.

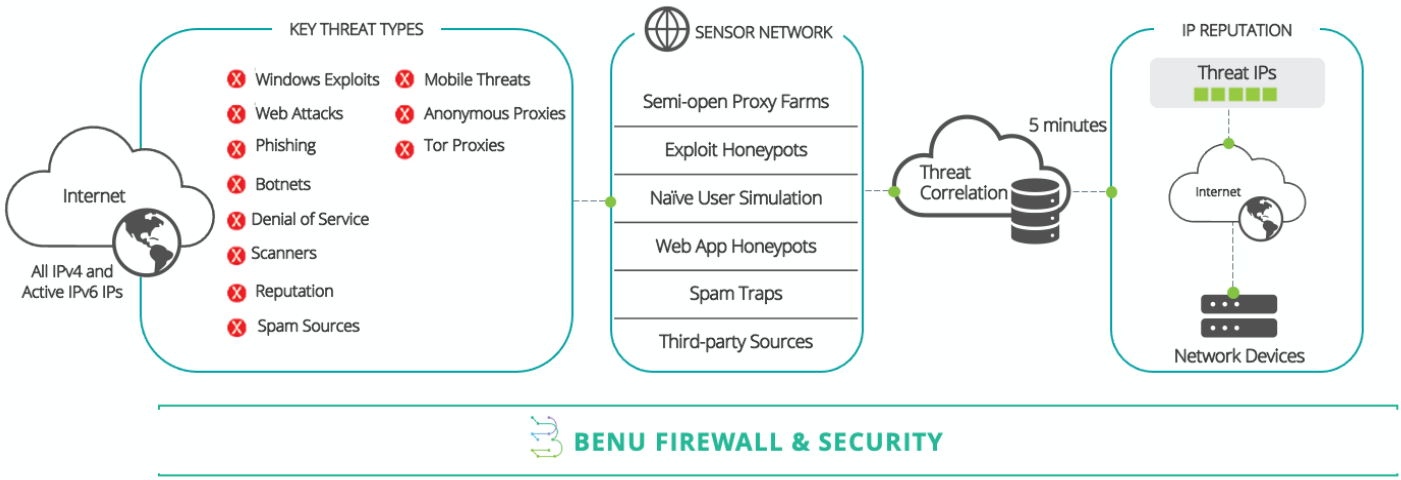
The web classification service benefits from real-time data processing in the cloud, and newly classified URLs are updated in the database every 5 minutes. This data processing includes each of the multi-layered defenses built into the security service, including DNS filtering, web filtering, real-time phishing detection and behavior-based intent determination. With this direct experience of new threats, we can determine the malware distribution URL, malware family, malicious behaviors and command-and-control (C2) URLs and IPs.

Content Filtering

Content Filtering checks for the membership of any URL against 82 categories and provides a calculated reputation score for the URL, along with other metadata. This service provides content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites. With 82 website categories, the Benu SD-Edge can accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with sensitive content, such as adult, drugs, and gambling. Using these categories and reputation scores, organizations can achieve a more secure network, adhere to HR and compliance policies, and implement and enforce effective web policies that protect users against web threats and prohibited content.

Phising Protection

Phishing sites are some of the most dynamic and short-lived attack platforms on the web, so intelligence sources must be capable of detecting and tracking them in real-time. Most phishing intelligence sources depend on manual submissions of phishing sites by end users. This is far from ideal. Users are prone to error, and for every 10,000 users who click on a phishing site only one will report it to an authority or tracking service, leading to massive underreporting of this threat vector. Today, 95% of all attack campaigns begin with a phishing email. Many of these lead the user a lure page in order to capture their credentials or deliver an exploit or malware payload.



Feature Overview

Benu Firewall

The Benu SD-Edge web security solution leverages phishing detection machine learning models built over the past decade. The latest phishing URLs that have been classified by machine learning models, which are generated on a daily basis, so they are able to adapt to new phishing techniques as these evolve. Our phishing classification category also benefits greatly from the real-time phishing detection that is built into partner endpoint security agents, which protect millions of PCs worldwide, and the service has great visibility into new threat URLs thanks to calls to cloud APIs from 120+ partners who are powering their products and services with this data. With this direct experience of new threats, we can determine the malware distribution URL, malware family, malicious behaviors and command-and-control (C2) URLs and IPs.

Cloud-based Approach for Volume, Scale, Accuracy, and Speed

Most modern malware is created with a specific purpose and, once its mission is complete, the threat disappears. Traditional, reactive, list-based security that works by recognizing known threats is ineffective against sophisticated attacks. Benu's SD-Edge security services use a proactive approach. Via Benu's partners, data is fed into the cloud from over 95 million global sensors and real-world endpoints, where it is analyzed and correlated with other data points, to provide a comprehensive view of the online threat. The solution features limitless scale, lightning-fast data processing, and a globally distributed database cluster for high performance and resilience.

Data Correlation for Contextual, Predictive Threat Intelligence

Benu leverages a powerful contextual analysis engine that takes disparate data from a variety of feeds and correlates it for deep insight into the landscape of interconnected URLs, IPs, files and mobile apps. Mapping the relationships between these different data points enables Benu to provide partners with highly accurate and actionable intelligence that is always up-to-date.

This also allows the Benu SD-Edge solution to accurately predict how likely an internet object is to be malicious in the future by its associations with other URLs, IPs, files, and mobile apps. For example, a seemingly benign IP, which other services may classify as safe, may be tied to other URLs, IPs, files, or mobile apps with histories of dangerous behavior.

Our advanced analysis provides a predictive reputation score which enables users to proactively protect themselves through self-defined policies based on their risk tolerance. Each of the above threat intelligence services benefits from this correlation engine to proactively protect users against threats that traditional technologies can't detect.

Product Scaling

All Benu SD-Edge products - from uCPE to WAG to BNG or 5G AGF - can support SASE services. They can be deployed as a virtual machine, containers , or bare metal on Benu xMEG appliances. Capacity scaling varies based on the platform and the configuration.

WAG Stateful Firewall Capacity	xMEG-1	xMEG-10	xMEG-100	xMEG-200
Throughput	14 Gbps	40 Gbps	100 Gbps	200 Gbps
Tunnels (GRE, GRE/UDP, L2TPv3)	1000	100K	1M	1M
CADs	20K	100K	1M	1M
CGNAT	10M	50M	512M	512M
ACLs (port or subscriber)	512	16K	16K	16K
Rate Limiting	21K	200K	2M	2M
DHCP transactions/sec	160	800	4K	4K
RADIUS transactions/sec	320	1600	24K	24K
Device counters	80K	400K	4M	4M

Features

Stateful Firewall	• No external connections initated from the Internet permitted
Carrier-Grade Network Address Translation (CGNAT)	• Static IP, dynamic IP, dynamic IP and port (port address translation) • Tunable dynamic IP reservation

Protection from Un-Authenticated Guest Users	• Un-authenticated guests have either access only to captive portal or "walled garden" access to specific sites
	• Guest user access can be limited based on time duration, data volume
	• Un-authenticated guests use:
	  · Separate IP pool and routing policies
	  · Separate port block sizes, to prevent port scanning
	• SD-Edge platform resources segmented so that un-authenticated users cannot impact authenticated users
	• Blacklisting of malicious devices / users
	• Policy-based packet drops can be mirrored for further reconnaissance

Protection from Authenticated Users	• Per-user identification and policy enforcement: QoS, rate limit, access control list (ACL), content filtering, total data volume • Per WiFi AP throttling
Traffic Segmentation	• Traffic policies keep network traffic from different zones or WiFi APs separate • ACLs for different zones or WiFi APs
DNS Attack Prevention	• DNS proxy support, enabling ultimate visibility and control over DNS • Wildcard DNS support for easier whitelisting or blacklisting
Control Plane Security	• SSH, SNMP (v2, v3), RADIUS and other control plane protocols are protected by ACLs that only allow certain hosts • Routing protocols only communicate with authenticated peers, using IETF standards-based authentication

Features

DoS Attack Prevention	• Intelligent control plane rate limiting of each protocol, preventing excessive traffic of any given protocol • Control plane queuing prioritization to ensure most critical control plane packets are prioritized over others
Malformed Packet and Fragmentation Protection	• Drop malformed packets • Packet fragmentation policies to prevent attacks from fragmentation
Content Filtering (Separately Licensed)	• 37+ billion URLs classified, 842+ million domains • 6 million dangerous IPs correlated with URLs • 80+ predefined categories, including porn, terrorism, hate speech, violence, weapons, alcohol, drugs, etc. to choose for filtering • URL classifier can make determinations on over 5,000 URLs per minute • 45+ languages
Malware and Phishing Protection (Separately Licensed)	• Network-wide, per VLAN, per WiFi AP, or per user protection from: · Bot Nets · Malware Sites · Phishing and Other Frauds · Proxy Avoidance and Anonymizers · Spam URLs · Spyware and Adware • Zero-day attack protection • Full-path URL path detection, going way beyond DNS-based approaches • Classification based on · Global threat sensors · Machine learning algorithms · Human classification · Inter-URL and IP contextualization