BANYAN SECURITY

SOLUTION BRIEF

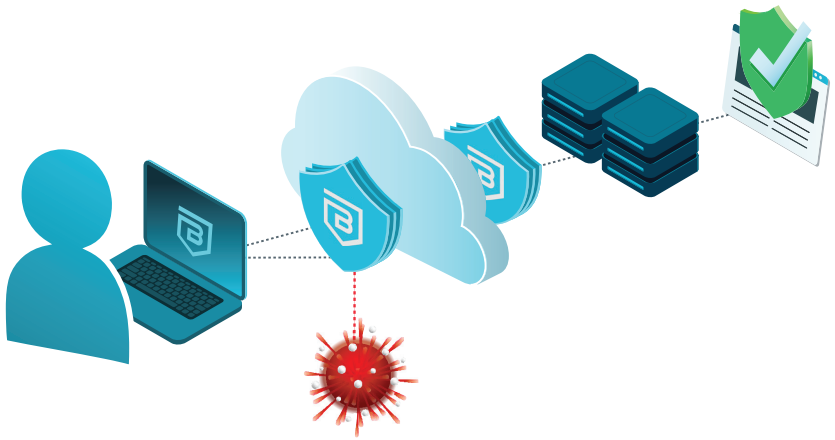
Internet Threat Protection

The Banyan Security Platform

Banyan's Secure Web Gateway (SWG) technology protects users from being phished, straying onto malicious web sites, and being exposed to malware attacks

Now more than ever, people are using the internet as their network of choice to connect to the applications and resources they need to do their jobs. Unfortunately, the internet can be a dangerous place, where an innocent click on a link can infect a machine with malware, leading to credential theft or even an organizational ransomware incident.

Rapid adoption of "work from anywhere" has provided global hiring options, organizational flexibility and resilience, but creates challenges due to employees, contractors, and third-parties on non-managed devices (think BYOD) using unknown networks. This often results in networking, IT, and security teams managing by exception and special case, arranging one-off mechanisms for providing secure access.



Protecting this modern workforce from damage caused by an errant click is of paramount importance. Doing so in an easily deployed and managed way while ensuring end user productivity is doubly important.

"The human element continues to drive breaches. This year, 82% of breaches involved the human element."

"Ransomware has continued its upward trend with an almost 13% increase (for a total of 25% of breaches) – a rise as big as the past five years combined."

- Verizon
2022 Data Breach Investigations Report (DBIR)

Enabling Safe, Secure Access

Banyan Security's Secure Web Gateway (SWG) capabilities provide robust internet threat protection. Protect users from being phished, straying onto malicious web sites, credential theft, or being exposed to ransomware. Optional controls enable organizations to enforce acceptable use policy (AUP), for example blocking specific categories of web sites like gambling and pornography.

Rest assured your workforce is protected, regardless of worker type or location, supporting use of both managed or unmanaged BYOD devices.

SWG Use Cases

Common use cases include:

- Protecting users from internet threats like phishing, malware, and ransomware
- Controlling access at an appropriate level of detail using granular policies
- Enforcing an organization's acceptable use policies (control internet access)
- Gaining visibility into user activity

Banyan Security Platform SWG Capabilities

Banyan provides an easy-to-configure combination of DNS and web security as well as app discovery and blocking, enabling you to filter and block harmful or unauthorized content in real-time. Protection users against traditional threats as well as high-risk domains, including new domains and cryptomining. Newly seen domains are continuously categorized using an artificial intelligence scanning engine, taking less than 15 seconds on average. Users are kept safe while seamlessly being afforded the freedom of modern internet use.

DNS – All DNS requests are analyzed, ensuring known-bad and risky domains are not accessed

Web – Deeper URL inspection allows more granular handling of specific sites

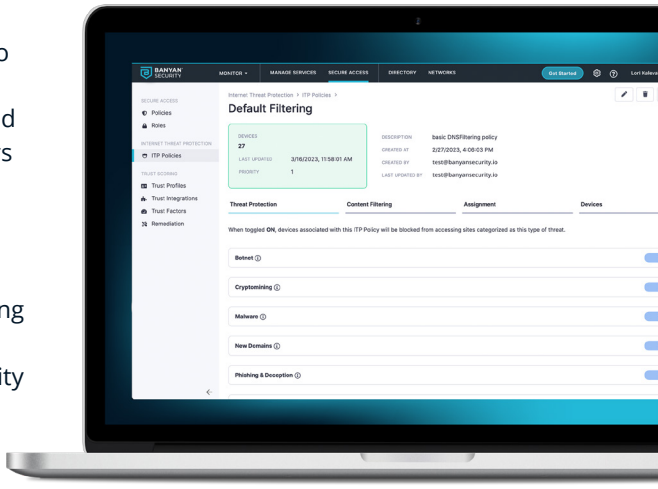
App – Knowing what cloud apps your organization uses helps identify risk areas, blocking as appropriate

All needed functionality is built right into the lightweight Banyan app. Protection is afforded even if the user hasn't logged in!

Other vendors force all traffic across a full tunnel, causing end users to suffer poor performance, especially with high-bandwidth applications like collaboration tools and video. Banyan's device-centric solution locally chooses the appropriate method for each type of access, providing full protection without degrading performance, infringing on privacy, or harming the user experience.

Banyan administrators create flexible, granular policies using dozens of available threat types and domain categories. Protection is further refined to include (block) or exclude (allow) specific top-level domains or subdomains. Policies are then assigned to users based on role, device ownership type, and device posture. Of course, admins have full control over the messaging users see when experiencing a block. These powerful, human-readable policies help to meet regulatory and compliance needs, as well as ensure your organization's acceptable use polices are enforced.

Since issues are prevented from happening in the first place rather than being discovered after the fact, reported malware and alerts are greatly reduced. This "de-cluttering" increases the value of the visibility gained into user activity including key items like top blocked domains, top domains searched, times when domains were searched, and domains searched per client.



About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access to applications and resources for employees and third parties while protecting them from being phished, straying onto malicious web sites, or being exposed to ransomware. A Flexible Edge architecture enables rapid, incremental deployment on-premises or in the cloud without compromising privacy or data sovereignty. A unique device-centric approach intelligently routes traffic for optimal performance and security delivering a great end user experience. Banyan Security protects workers across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit www.banyansecurity.io or follow us on Twitter at @BanyanSecurity.

BANYAN SECURITY

Banyan Security, Inc. | +1 415-289-9414 | www.banyansecurity.io