BANYAN SECURITY

Security Service Edge (SSE) Evaluation Checklist

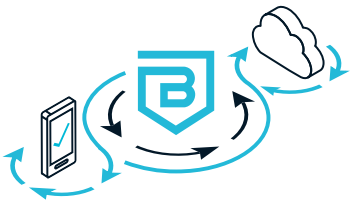
Problem

Providing secure zero trust access to applications and infrastructure at scale while protecting the modern workforce from advanced internet threats is challenging. Risk and security must be continuously evaluated, incorporating telemetry from adjacent security tools. With infrastructures growing ever more complex, and applications spread across on-premises, hybrid, and multi-cloud environments, network-centric solutions like legacy VPNs and firewalls have been put to the test and revealed significant performance, usability, and systemic security issues that band-aids cannot fix.

Post-COVID, a significant percentage of workers remain remote, and hiring is now best-in-class, not best-in-geographic-region. Increasing reliance on contractors, partners, and other contingent workers makes onboarding, offboarding, and BYOD support critical.

The access and protection strategies that most companies have in place can't keep up with these realities. A scalable and comprehensive approach is required. A robust Security Service Edge (SSE) solution with ZTNA (Zero Trust Network Access), VPNaaS (VPN as a Service), CASB (Cloud Access Security Broker), and SWG (Secure Web Gateway) components should be evaluated as part of this new strategy.

Use Cases

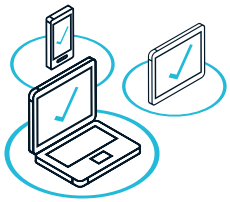


Modernize Legacy VPN & Firewall

Protect company resources by enabling least-privilege access to specific applications and servers based on the combined real-time contextual factors of user and device trust and resource sensitivity. Deploy incrementally – alongside existing infrastructure, if desired.

Device Trust and Internet Threat Protection

Complement user trust by uniquely identifying each device and quantifying its security posture. Protect workers from being phished, straying onto malicious web sites, or being exposed to ransomware. Optionally block domain categories for compliance.



Support Third-Party Access / BYOD / M&A

Provide third-parties easy, secure access to only specifically needed resources, optionally incorporating device trust. Enable BYOD and protect corporate assets without needing Mobile Device Management (MDM) or Unified Endpoint Management (UEM).

Operational Changes

Before	After	Security Benefit
Standalone ZTNA, SWG, and CASB products have varying configurations and no integrated visibility.	A single, unified platform with a lightweight app is easier to deploy, maintain, and manage. Gain insights into user behavior and corporate security in one place.	A platform view and unified policy for your security and access edge allows administrative insight and response for all resources.
Network focus, access is granted based on the network where the desired resource resides.	Focus is on access to distributed assets spanning all environments and protocols, regardless of network or location.	Every network, resource, and asset can be configured for least-privilege access using the internet as transport with micro-tunnels securing the data.
Users can access all network resources once they authenticate to a network, unless there is network micro-segmentation.	Use of micro-segmentation for granular access control at the application, protocol, URL, or resource level without needing network segmentation.	Prevents lateral movement for a threat actor because access control is refined and granular, leaving little room to wander across a network and its resources.
Distributed security access control based on who owns the network, different approaches for on-premises, hybrid, and multi-cloud environments. Different approaches for employees, developers, and contractors.	Centralized access control and policy enforcement supporting any type of work by any person at any location.	Reduces attack surface risk, every resource and access session is managed with the same process and controls regardless of what type of environment or business use.
Access policies are referenced a single time to initially authenticate users. Updates to policy may require end-user reboot or update to take effect.	Continuous re-authorization of users and devices against access policies. Policy updates are immediate and user access is dropped if privilege and device security requirements are not met.	Policy adherence is constant rather than a snapshot in time.
Some support for device security context with a mix of additional security tools and integrations.	Full device support, continuously verifying critical security elements and device certification, against access policies.	Minimize risk from device compromise with continuous re-validation of a device's security posture. This is especially important for access to sensitive and classified information.

Before	After	Security Benefit
Legacy VPNs create silos of hard-to-manage infrastructure that suffer from scale, performance, and usability issues. Users are granted ungoverned, overly-broad access to entire networks.	Situations needing tunnels use modern technology employing continuous authorization with device trust against consistent trust-based policy.	Access is continuously authorized, severing connections should user or device fail to meet policy requirements.
Legacy web gateways require all traffic to be backhauled to corporate to be inspected and policy to be enforced on the way out.	The agent on the device acts as the “new edge” and provides web gateway capabilities including DNS and URL filtering.	All devices, connected or not, will have internet threat protection enforced.
Cloud-based web gateways require all traffic to be sent to a 3rd party for decryption, inspection, and encryption.	Traffic filtering decisions are made on the device based on DNS and URL filtering. The small minority of traffic that requires additional inspection will be done based on metadata for source and destination and not the data itself.	Data privacy and sovereignty is maintained, and traffic can be accounted for end-to-end fulfilling compliance needs.

Security Service Edge (SSE) Evaluation Checklist

	Feature/Capability	BANYAN SECURITY	Vendor 1	Vendor 2
Installation	Immediate value – simple 15 min deployment	✔		
	100% software platform, no hardware or virtual appliance required	✔		
	Single client app for all SSE functionality	✔		
	Supports public and private cloud or on-premises installation	✔		
	Supports both tarball and Docker installations	✔		
	Supports AWS CloudFormation templates for ease of deployment	✔		
	Purpose-built device-centric Security Service Edge (SSE) platform	✔		
	Lightweight installation on Linux distributions including Raspberry Pi and Windows Subsystem for Linux (WSL)	✔		
	Requires minimal or no changes to corporate network infrastructure	✔		
	Terraform support for automated deployment of zero trust security policies	✔		
Integration	Integrates easily with existing security tools	✔		
	IdP for authentication (e.g., Azure AD, Okta, Ping)	✔		
	SAML and OIDC support for IdP integrations	✔		
	MDM / EMM / UEM tools for device trust (e.g., AirWatch, Intune, Jamf)	✔		
	EDR for real-time device health signals (e.g., Carbon Black, CrowdStrike, Sophos)	✔		
	Managed application configs for zero touch enrollment	✔		
	Export events/audit logs to SIEMs (Splunk Phantom, Demisto, etc.)	✔		
	Documented APIs for general automation	✔		
Connectivity	Private network access	✔		
	Proxied access	✔		
	Split Tunneling	✔		
	Full Tunneling	✔		
	Publish applications using your organization's corporate domains	✔		
	Enables MFA for cloud SaaS applications	✔		
	Enforces device trust policies for cloud SaaS applications	✔		
	Define zero trust policies for individual, or groups of, SaaS applications	✔		
	Enables Source IP restrictions for cloud SaaS applications	✔		
	Restricts Cloud IdP access to registered devices to prevent password-stuffing and MFA-compromise attacks	✔		
	Support unregistered/unmanaged devices	✔		

Feature/Capability		BANYAN SECURITY	Vendor 1	Vendor 2
Internet Threat Protection	DNS Layer Security	✔		
	Enables security based on category of site	✔		
	Enables security based on type of threat	✔		
	Provides always-on security	✔		
	Real-time updates to categories and threats	✔		
Access Controls	Includes easy-to-use, human-readable policy engine for least privilege access controls	✔		
	Provides trust scoring framework that incorporates signals from existing tools as part of access and enforcement decisions	✔		
	Provides continuous device trust validation (context includes EDR running/ OS version/firewall/encryption)	✔		
	Policy engine supports both managed devices and BYOD environments with ease	✔		
	Includes real-time event monitoring and alerting	✔		
	Provides continuous authorization via short-lived certificates and tokens	✔		
	Provides granular, API-level controls	✔		
	Provides user-to-application segmentation without providing access to the network	✔		
	Least privilege access restricts lateral movement	✔		
	Provides APIs for policy and config automation	✔		
	Provides categorical controls for internet traffic	✔		
	Provides threat protection controls based on threat type	✔		
Architecture	Cloaks applications from exposure to the public internet	✔		
	Provides an identity-aware proxy architecture designed for multi-cloud environments	✔		
	Provides a lightweight app installed on devices to continuously verify posture and establish device trust	✔		
	Flexibly supports cloud IaaS while also offering the option for enterprises to self-host their edge	✔		
	Integrates easily with existing IAMs through leading IAM marketplaces	✔		
	Incorporates native PKI for certs and integrates with existing PKI	✔		
Network	Requires minimal or no changes to existing networking infrastructure	✔		
	Incrementally deploy one service or application at a time	✔		
	No overlapping IP addresses or subnets to manage	✔		
	Uses cryptographic identity instead of IP address for network access	✔		
	No NGFW/VPN appliance required	✔		
	No web gateway appliance required	✔		

	Feature/Capability	BANYAN SECURITY	Vendor 1	Vendor 2
Use Cases	Supports on-premises, hybrid- and multi-cloud, and SaaS use cases	✔		
	Hosted web applications – HTTP	✔		
	SaaS application access and security – SAML/OIDC	✔		
	Servers – SSH, RDP, and Kubernetes	✔		
	Services – Database and other TCP	✔		
	Enables Acceptable Use Policy (AUP) enforcement	✔		
	Always-on DNS filtering	✔		
	Always-on deep URL filtering	✔		
	Protects against phishing/malware/ransomware attempts	✔		
	Add MFA and device posture assessment to legacy web applications without modification	✔		
User Experience	Provides a unified service catalog for users' services and web apps	✔		
	Provides one-click access and autorun capabilities to infrastructure services	✔		
	Replaces user/password authentication to SSH with short-lived certificates	✔		
	Provides zero trust access that is transparent to end users	✔		
	Services can be grouped into bundles and users can add favorites for fast, easy access	✔		
	Frictionless access to use any SSH client and commands	✔		
	Supports passwordless zero trust access	✔		
	Communicates trust factors to end users thereby decreasing support calls	✔		
	Trust level shown to end users to help improve their device security posture	✔		
	Server and application discovery to quickly publish services	✔		
	Provides easily customizable remediation descriptions and URLs enabling users to self-remediate	✔		
	Protect against internet threats without requiring user login	✔		
	Single app installation supports multiple organizations	✔		
	Supports Windows/macOS/Linux/Android/iOS/iPadOS	✔		

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.