TRINITY CYBER

BUYERS GUIDE

Seven Must Haves for a Modern Secure Web Gateway

What to demand when refreshing your SWG

01 Stops threats at the gateway

Why it matters:

Web attacks that pass the SWG create downstream work and raise risk. Buyers must ask if the control protects the user and network from modern, AI-era threats.

Buyers ignoring this need often add cost, complexity, and user frustration to their security stack by layering in nearline sandboxing and Remote Browser Isolation (RBI), which are unnecessary with Trinity Cyber.

How Trinity Cyber does it better:

Trinity Cyber inspects traffic inline and edits malicious content out of live sessions, before it reaches your users. Inspecting over 2 Trillion protocols, scripts, and files per day, Trinity Cyber performs at scale, invisibly to your end-users with <1ms of inspection latency.

You create your acceptable use policies, Trinity Cyber's private-cloud Point of Presence (PoP) network fully manages your threat defense, with an action log for review.

02 Sees the whole session

Why it matters:

Modern attacks hide inside encrypted traffic, trusted clouds, scripts, and content assembled in the browser. Threats sits below the URL or file level.

How Trinity Cyber does it better:

Patented Trinity Cyber Full Content Inspection™ (FCI) parses files, scripts, protocols, and session context across Layers 3 through 7. Trinity Cyber protects over 3 million users every day.

03 Recognizes attacker behavior

Why it matters:

Fresh domains and payloads make reputation scores and signatures stale. Buyers need detections that follow the techniques attackers reuse.

How Trinity Cyber does it better:

We build detections around first-order adversary TTPs. One detection efficiently covers a class of variants for superior protection vs. alternatives with shallow heuristics and high false positives.

04 Acts with precision in live traffic

Why it matters:

Attackers place harmful scripts or objects inside useful sessions. Precise action removes the malicious element and keeps the business flow intact.

How Trinity Cyber does it better:

Threats are edited out of in-flight traffic in real time; the remaining clean session passes to the user. It's security at business speed for uptime of critical operations, transactions, and supply chains.

05 Keeps TLS inspection fast and simple

Why it matters:

Most web traffic is encrypted. Slow decryption and certificate overhead limits coverage frustrates users and admins.

How Trinity Cyber does it better:

TLS inspection is managed as part of the Trinity Cyber service. Trinity Cyber delivers sub-millisecond inspection latency and excludes traffic as you require.

06 Fits your stack and keeps policy control

Why it matters:

Modern SWGs must support acceptable-use policy and connect cleanly to the environment already in place. A broad redesign slows adoption and adds cost.

How Trinity Cyber does it better:

We enable the latest acceptable-use policy controls, and work alongside existing firewalls and EDRs, and enable you to simplify your stack. Trinity Cyber ZTNA and IPsec connections feed the SWG service.

07 Lightens your load

Why it matters:

Missed threats and noisy alerts consume security time. The SWG should take work out of your queue.

How Trinity Cyber does it better:

Trinity Cyber's managed service features an industry-low false-positive rate below 0.01%, while stopping more threats.