Markmonitor™

Secure Forwarding & Parking

Secure Every Click, Every Time

For Additional Information, Contact Your Account Manager or Visit markmonitor.com

Your domain names are more than just online addresses, they're brand assets, security touchpoints, and they serve as digital trust indicators. Yet many organizations overlook a hidden vulnerability: parked or redirected domains that aren't secured with HTTPS.

Ensure every parked or redirected domain is protected and easy to manage with Markmonitor's Secure Forwarding & Parking (SF&P). Whether you're rerouting traffic or simply holding domains for future use, SF&P provides seamless, secure, and scalable protection for your entire domain portfolio.

The Hidden Threat of Insecure Domains

You may have parked domains for brand protection, future campaigns, or simply to prevent misuse by third parties. But **if those parked or redirected domains don't support HTTPS, they become low-hanging fruit for cybercriminals and red flags for security auditors.**

Here's Why That Matters:

- **88% of websites now default to HTTPS,** especially those like .app, .page, and .dev that enforce HSTS (HTTP Strict Transport Security) by design【1】
- **Domains without valid SSL/TLS certificates often trigger browser warnings** like "This site can't provide a secure connection", driving users away instantly
- Services like **BitSight and SecurityScorecard routinely downgrade organizations for not secure or non-functional domains**—even if they're parked or redirected【2】【3】

1. *W3Techs, "Usage statistics of Default protocol https for websites"*
2. *BitSight, "How Does Bitsight Work? A Look at Security Ratings & How They're Used"*
3. *SecurityScorecard, "SecurityScorecard Unveils the Industry's Most Predictive Cybersecurity Risk Ratings with Refined Scoring Algorithm"*

Why Markmonitor Secure Forwarding & Parking?

Strengthen Your Security Posture

- Avoid browser errors like "This site can't provide a secure connection"
- Markmonitor manages and automatically provisions SSL/TLS certificates for SF&P
- SSL/TLS certificates are dedicated per account and are not shared with other customers
- Eliminate risks from HTTP-only redirects and non-secure parked pages

Universal Accessibility

- Works across all major browsers and network environments
- Conforms to browser and firewall rules requiring HTTPS
- Compatible with HTTPS-only top-level domains like .app, .dev, and .page

Set-and-Forget Simplicity

- Automatic enablement across all compliant domains
- **Certificates are refreshed every 30 days** - well ahead of the 2029 SSL/TLS maximum validity requirement of 47 days
- Integrated DNS, WAF, and Email Security Records (SPF, DKIM, DMARC)

Trusted Brand Experience

- Visitors land on a secure, professional page every time
- Mitigates "not secure site" warnings that damage brand trust
- Makes full use of your domain portfolio - including defensive names

SF&P Managed Migration Service

For domains that cannot tolerate any disruption to HTTPS-to-HTTPS connections, Markmonitor provides a managed Secure Forwarding & Parking (SF&P) migration service designed to ensure continuous availability and a consistent user experience throughout the transition.

Available as an additional managed service for critical domain migrations, this offering delivers a seamless transition process that minimizes the risk of unexpected interruptions, putting our expertise to work for your most valuable assets.

- Supports uninterrupted HTTPS connectivity with 100% uptime during migration
- Validates domain ownership through TXT records and pre-authoritative certificates
- Seamlessly transitions domains to standard SF&P once DNS and registrar authority are transferred to Markmonitor

Connect With Your Markmonitor Account Representative Today About Early Adopter Programs, Portfolio Reviews, and Competitive Bundles!

Key Features at a Glance

FEATURE	BENEFIT
Dedicated Infrastructure	Each customer has unique SSL certs and load-balancers, no cross-traffic
Auto-Renewing Certs Every 30 Days	Future-proof against SSL/TLS policy changes; always secure
Automatic HTTPS for All Zones	Ensures compliance, security, and better user experience
Web Application Firewall (WAF)	Blocks malicious traffic before it reaches destination URLs
DNS-Based & Email Security	Built-in best practices enhance security scores and prevent phishing attacks
Global DNS Performance	Delivers reliable speed and uptime across all domains