

Secure Hosting

Fast, protected and always available

- **Website protection:** Wildcard SSL certificates, malware scanning, a file permissions checker and WordPress checksum reports guard your site and its subdomains.
- **Data protection and compliance:** PCI-compliant servers for safe payments, ISO27001-certified data centres, and email security with antivirus, anti-spam and DKIM.
- **Defence against attacks:** DDoS protection, brute-force login defence, a web application firewall, two-factor authentication and visitor blocking.

Security at the foundation

Security and performance shaped the design of our platform. The way our servers are arranged keeps your site online and protected in difficult conditions.

Autoscaling keeps you online

Even failed attacks can use up hosting resources. Autoscaling absorbs surges automatically, so your site stays quick and available, and problems on neighbouring sites don't spill over to yours.

Redundancy throughout

No single failure can take the platform down. If hardware, software or a network component fails, automatic failover restores service quickly and protects your data.

Servers with separate jobs

Web servers serve websites, MySQL servers hold databases and email servers handle mail. Keeping these roles apart means that a breach of one doesn't give an attacker access to everything.

Tools that protect your business

These protections shield your data, your visitors and your reputation, from free SSL certificates to enterprise-level DDoS defence.

Wildcard SSL certificates

Any site that collects information, including through a simple contact form, needs SSL. It encrypts the connection between visitor and server, shown by https:// in the address. It also helps your search ranking, because Google treats SSL as a quality signal. Our wildcard certificates cover every subdomain.

Data centre security

Our data centres are certified to ISO27001:2013. They have redundant power, gated entry with photo ID and swipe cards, and 24/7 CCTV.

PCI compliance

Our servers meet Payment Card Industry (PCI) standards, which matter for any store taking card payments. Regular audits confirm we meet the requirements set by the major card brands, such as Visa and MasterCard.

Malware scanning

Malware can lead to stolen identities and lost data. We scan your site daily and alert you to threats, and you can run a scan on demand to confirm a problem is fixed.

WordPress checksum report

WordPress is a common target for attackers. The checksum test compares your installed WordPress files with the official version, so unauthorized changes are spotted before they can be exploited.

File permissions checker

Wrong file permissions can let the wrong people read or change your data. The checker reviews your settings and recommends fixes for anything risky.

DDoS protection

DDoS attacks flood a server with fake traffic so real visitors can't get in. Our protection absorbs these attacks, including very large ones, with capacity of more than 1 terabit per second.

Email security

Mail is scanned for viruses and malware before delivery, spam filters remove unwanted messages, and DKIM authentication helps stop email spoofing.

Web application firewall

The firewall inspects incoming traffic and blocks common attacks such as SQL injection and cross-site scripting, so attackers can't exploit weaknesses in your applications.

Two-factor authentication

Two-factor authentication protects StackCP, and password tools help you create strong passwords. You can also password-protect sensitive parts of your site and lock down FTP.

Brute-force login protection

Brute-force attacks use software to guess passwords. StackProtect watches login attempts on your site and flags suspicious automated requests.

Blocking visitors

Block traffic from particular countries or IP addresses when you need to control who can reach your site.

Questions, or ready to get started? Call **778-215-1504** or email **sales@10mb.com**. Pricing is quoted to fit your needs. Visit **10mb.com** for more.