WEBSCALE

DATASHEET

# Webscale M1 Support: Community and Enterprise

## Extend lifespan of Magento 1 Storefronts

In June 2020, all Magento 1.x versions will officially end-of-life (EOL). Thousands of merchants with online stores deployed on Magento 1 (M1) will lose all access to new features, functionality updates, bug fixes, and support from Adobe / Magento. Perhaps, most importantly, any future vulnerabilities exposed will no longer be addressed with new security patches from Magento.

Moving forward, all these updates and security measures, as well as some Magento extensions, will only be made available to, and supported on, Magento 2 (M2) storefronts.

However, moving from M1 to M2 is far from a simple upgrade. It's a re-platform that requires extensive development work, and it can be prohibitively expensive, for even the most basic sites. It also requires a comprehensive site redesign. Ecommerce site owners want the flexibility of staying on M1, without being forced to migrate to M2 per Adobe's timeline, and incurring huge development, license, and employee costs. The biggest need for such merchants lies in protecting their M1 applications against new vulnerabilities discovered after June 2020.

**Webscale M1 Support**

Webscale M1 Support is a security-focused SaaS platform that allows merchants to continue to use M1 beyond June 2020, securing their site against exploits, from the point of entry to the backend infrastructure. Webscale will also be working closely with the Magento Association, the community, and Magento experts world-wide to develop application security patches, and collaborating with its digital agency partners to apply these patches to merchants' applications.

# Product Benefits

### Flexible Schedule

The immediate “mandate” to move to M2 puts undue cost and timeline pressures on ecommerce site owners, who are having to adhere to seemingly arbitrary timelines imposed by a vendor. With Webscale M1 Support, merchants will have the flexibility of staying on M1 for the foreseeable future, and moving to M2 at any time, when it aligns with their own business demands.

### Reduced TCO

With Webscale M1 Support, ecommerce business owners are not forced to incur tens or hundreds of thousands of dollars in site redesign and re-platforming costs. Webscale M1 Support ensures it’s business as usual for merchants even after M1 EOL.

### Managed Security

Webscale’s robust SaaS-based security stack already protects thousands of Magento applications. With a programmable WAF, strong access control, Content Security Policy protection, and automated detection of cyberthreats, Webscale M1 Support will constantly monitor, identify, and proactively protect against potential exploits through malware insertion in the infrastructure, and/or bad traffic trying to access critical parts of the application. Merchants can also choose to obtain new M1 security patches from Webscale to keep their application code secure.

### Faster, Always-on Applications

Applications enabled by Webscale M1 Support have a multi-cloud elastic data plane, auto-scaling capabilities, and a highly available (HA) data tier architecture, ensuring zero application downtime. With caching at different layers, from the edge of the network to the application core, application resources are used only for real user traffic, such as checkouts. Everything else is handled outside the database and application tiers, significantly accelerating site performance.

# Key Features

## SaaS Security Stack

- **Programmable Web APP Firewall (WAF)**

  Webscale's application-aware WAF enables merchants to protect their online stores from known vulnerabilities, such as the OWASP Top 10, as well as easily add unlimited rules called "Web Controls" to protect against new threats.

- **Blocklisting / Allowlisting**

  These features allow merchants to block known bad actors permanently, or even entire geographical regions (geo-blocking) that merchants are not serving, while building a trusted model that only allows authorized personnel to access the most secure parts of the application (such as admin sites).

- **Content Security Policy Protection**

  Content Security Policy (CSP) is an HTTP security standard designed to protect client interaction with websites against cross-site scripting (XSS) attacks. It increases the trust between the browser and application by allowing the application to specify which domains can be trusted. The 'script-src' tag specifies which trusted domains the browser can execute scripts from. Webscale M1 Support enables real-time monitoring, reporting of trusted domains, and alerting of violations by non-trusted domains executing scripts or other suspect behavior.

- **Intrusion Detection**

  Sophisticated cyber-attacks involve placing malicious code in the application infrastructure, and executing it through browser calls. With automated intrusion detection, Webscale can immediately discover unauthorized file changes, quarantine the servers affected, and monitor and block any bad actors trying to access the scripts.

## SecOps and Support

- **Ongoing Security Patches**

  While Magento will stop providing security updates, Webscale is working with other experts to continue to provide patches, at a faster rate than what has been traditionally available from Magento themselves. In addition, Webscale will also be implementing its Web Controls to ensure the site is not vulnerable while these patches are being developed. Webscale M1 Support allows developers to update the M1 application itself, every time a new patch is available.

- **PCI Compliance Support**

  Webscale M1 Support enables ecommerce merchants to easily achieve and maintain PCI compliance during their annual security audits. Capabilities include longer retention (up to a year) of critical log data from different parts of the application infrastructure, access and integrated views of log data through the Webscale portal, and audit trails of all changes made to the application and its configurations.

- **Developer Support**

  Webscale is working with hundreds of digital agencies and developers worldwide to help manage M1 environments and ensure the rapid deployment of patches, as they are developed. This is a recommended add-on to Webscale M1 support.

- **M2 Re-platforming Service**

  When an ecommerce merchant is ready to re-platform to M2, Webscale helps streamline the process. Merchants can also access Webscale's qualified network of developers and agencies to assist with this transition.

# Platform Specifications

Available for both cloud-deployed storefronts and on-premise, datacenter hosted applications, Webscale M1 Support delivers the industry's most comprehensive security suite for Magento-based online businesses.

| | Cloud M1 Support | OnPrem M1 Support |
|---|---|---|
| **Infrastructure** | 1 application cluster with 1 backend | As-is datacenter hosted |
| **High Availability** | N+1 HA Architecture | As-is datacenter hosted |
| **Production Environment** | • Webscale Certified Production Architecture (Base configuration)<br>• Auto-scaling Webscale Elastic Data Plane<br>• Auto-scaling App Tier<br>• Scalable Database Tier | • Auto-scaling Webscale Elastic Data Plane<br>• Datacenter account access<br>• Log access and monitoring |
| **Security SaaS features** | • Blacklisting/Whitelisting<br>• Programmable WAF<br>• DDoS Shield<br>• Content Security Policy Protection<br>• App Shielding<br>• Intrusion Detection<br>• Malware scanners | • Blacklisting/Whitelisting<br>• Programmable WAF<br>• DDoS Shield<br>• Content Security Policy Protection |
| **Performance SaaS features** | • HTTP/2<br>• TLS Offload<br>• CDN Caching<br>• Cache Control<br>• Content Optimization<br>• Dynamic Site Cache | • HTTP/2<br>• TLS Offload<br>• CDN Caching<br>• Cache Control<br>• Content Optimization<br>• Dynamic Site Cache |
| **Availability SaaS features** | • Always-on Auto-scaling Web tier<br>• L7 Load Balancer<br>• Self-healing Infrastructure<br>• Predictive Application<br>• Auto-Scaling<br>• HA Data tier | • L7 Load Balancer<br>• Self healing and Scalable Web Tier |

| | Cloud M1 Support | OnPrem M1 Support |
|---|---|---|
| **Staging Environment** | Included | Optional add-on |
| **Dev Environment** | Included | Optional add-on |
| **Hosting** | Cloud Hosting included (GCP, AWS) | As-is datacenter hosted |
| **Logging** | 30-Day Log Access | 30-Day Log Access |
| **PCI Compliance support** | Optional add-on | Optional add-on |
| **Backup** | Daily Backup | Optional add-on |
| **Support** | 24x7x365 email support with 15-minute response time SLA for critical incidents | 24x7x365 email support with 1-hour response time SLA for critical incidents |
| **Add-ons available** | • Cloud Image Manager<br>• Cloud Bot Manager<br>• PCI Compliance Support | • Cloud Image Manager<br>• Cloud Bot Manager<br>• Staging Environment<br>• Development Environment<br>• PCI Compliance Support |