Sucuri Agency Service Level Agreement

What SLA metrics are important to your organization?

A **security-first approach** to enterprise-grade SLAs.

Redefined **availability** with rapid response and enterprise guarantees.

Professional response necessary for first-call resolutions.

Table of Contents

The Only Option is to Exceed Expectations

When it comes to protecting your web properties nothing is more important than reliable, fast and professional support. The need to plan for worst-case scenarios is critical, and this includes understanding how to address the ever-evolving landscape of cybersecurity threats.

A Service Level Agreement (SLA) should be written to **provide a clear and balanced understanding** to all parties involved of their rights and obligations when a triggering event happens. It should reflect your organization's priorities and provide accountability to all parties.

The performance parameters should be outlined, as well as the applicable metrics used to measure performance. The clearer the expectations are, the better the chances for a successful partnership between parties that rely on a SLA to address stressful circumstances.

Website security SLAs have the added pressure to be mission-critical and can potentially minimize financial losses to an organization under a cyber attack.

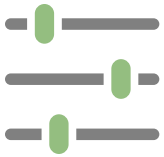
Defining Service Level Agreements

Defined as an agreement and not as a contract, **an SLA helps service providers set clear support guidelines to its customers,** minimizing the opportunity for disputes between parties when service level agreements need to be executed. Sucuri defines SLA response times based on priority levels.

In 2019, over **170 million** attack attempts were mitigated with the Sucuri Firewall.

Reliable Response

When your web properties are under attack, having well-trained analysts as first responders is key to a quick resolution during initial engagements with the technical team. At Sucuri, support is available 24/7/365 in different time zones, with direct access to our top analysts handling your tickets and requests through our support system.



Custom to Fit Your Needs

Our account executive team is agile and able to meet the requirements of the most demanding organizations - high availability, load balancing, DMZ, failover setups, and anything else your organization needs.

Dedicated Account Manager

Sucuri goes beyond the delivery of top-notch enterprise-grade SLA's by making sure a professional account manager is also assigned to your account and available as part of the support package. Consider us an extension of your team. They will be an incredible asset to ensure all products are properly configured.

Security Research

Sucuri is the most trusted brand in website security. Our approach to research keeps us on the forefront of emerging threats. Partner with dedicated security analysts and consultants who are passionate about creating a superior solution to safeguard your website availability.

Predictable Pricing

Most security companies have no support flexibility. Sucuri takes a different approach. Our pricing model is dependent on the response time and service level you require for incident response and customization. This enables many of our partners to save money and generate new revenue at the same time.

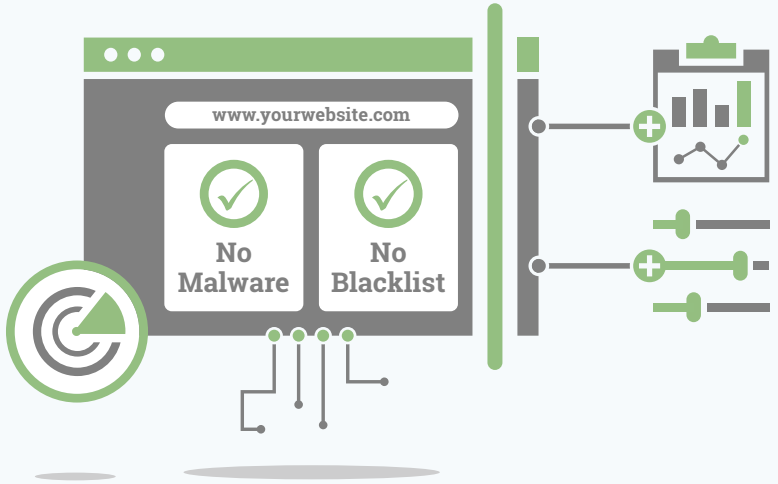
Defining Client Expectations

We can assist you with ensuring your clients **understand precisely what benefits they will receive by partnering with Sucuri.**

Our Agency plans offer robust protection and monitoring to keep your clients' websites safe.

Monitoring Platform

The Sucuri detection platform allows you to **identify various web security issues,** like malware, so you can respond quickly.



The Monitoring Platform includes:

- Known Website Hacks
- Security Issues and Anomalies
- Blacklist Warnings
- Downtime
- DNS Record Changes
- Blackhat SEO Spam Injections
- Malicious Redirects
- Hidden & Malicious iFrames
- Mobile Malware Infections
- Phishing Lures
- Hijacked Websites
- Obfuscated JavaScript Injections
- Redirects Targeting Mobile Devices
- Drive-by-Download Injections
- Pharma Hacks
- Infected Database / SQL Injections
- Website Defacements
- Cross-Site Scripting (XSS) Infections

Protection Platform

The Sucuri Firewall is scalable, reliable, and easy to integrate. Sucuri Firewall will **protect your web application** regardless of the type of application, code base or hosting environment.

The Protection Platform includes:

- Zero-Day Exploits
- Cross-Site Scripting (XSS)
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)
- SQL Injection Attack
- Cross-Site Request Forgery (CSRF)
- Login Form Bypassing
- Out-of-Date Software
- Insecure Plugins
- Vulnerable Themes
- Bad GET or POST Methods
- Drupalgeddon
- Heartbleed
- Malicious HTTP Requests
- Remote Code Execution
- TCP SYN & ACK Floods
- HTTP XML-RPC PingBack attacks
- Brute Force
- UDP Floods

A Simplified Tiered Approach

Sucuri offers a simplified tiered priority model that allows you to choose the pricing level based on your organization's SLA needs.

Does your organization have specific demands that won't fit the set models? No problem.

Sucuri will listen to your needs and work a customized plan that will meet your unique demands.

Feature	Ad-hoc Plan	Premium Plan
Monitoring	12 hours	6 hours
Malware Removal / Hack Cleanup	$100 ad-hoc charge	Included
Brand Reputation & Blacklist Monitoring	Included	Included
Stop Hacks & Virtual Patching	Included	Included
Advanced DDoS Mitigation	Included	Included
CDN Performance	Included	Included
SSL Certificate Support	Included	Included
Firewall HTTPS & PCI Compliant	Included	Included
Customer Support	Ticket & Account Manager	Ticket & Account Manager

Deploying Sucuri - What to Expect

Monitoring/Detection Platform

Activating Server-Side Monitoring

The front-end scanning will begin automatically once the domains are added to the Sucuri monitoring dashboard. In order to activate the Sucuri server-side monitoring, a .php agent must be added to the root code. Sucuri can complete this via (s)FTP or the agent can be supplied to the customer to add manually.

Types of Monitoring

Our remote scanner checks for conditional malware and security issues while our server-side agent detects indicators of compromise hidden on your server. We detect downtime and changes to your DNS settings, core file integrity issues, search engine blacklist status, antivirus security warnings, and SSL certificate records. We alert you if we detect anything suspicious.

Alerts and Notifications

When an indicator of compromise is detected on your websites, you will be notified immediately so you can take action or request a cleanup from our incident response team. The alerting mechanism notifies you via email, SMS, Slack, RSS, or custom post options. We also offer weekly or monthly email reports.

Firewall Preparation and Activation

Activating the WAF

To enable the protection of the Web Application Firewall, the DNS A record for each site can be set to its unique firewall IP. At this time, we will also confirm that we have the correct origin IP address set on the firewall.

Whitelisting Sucuri IP Addresses / Ranges

Sucuri will provide a range of IP addresses that the WAF will potentially use to connect to your origin server. These IPs need to be able to access the web ports your site runs on (port 80 and/or 443).

Ideally, our entire set of ranges would be whitelisted. If for any reason your sites come under attack and the remedy involves moving your configuration around our infrastructure, this will afford us the most latitude to help. At a minimum, there will be six IPs that need to have access.

Multiple Hosting IP / Backup IP

Sucuri can accommodate custom environments with multiple host IPs or backup/failover IPs. To enable this feature our team will need the appropriate IP addresses.

If Site is Behind External CDN

Sucuri is built on a CDN, however, if an external CDN is being used (and will continue to be used) it is supported by our system. To accomplish this, the external CDN will resolve to Sucuri's Firewall IP as the new Origin IP.

Preparing SSL (for HTTPS)

Both the certificate and key files are needed, including any intermediate bundles. They need to be in text format and either provided to our support team or added by the user under the SSL tab of the Sucuri dashboard.

Windows Environment: the proper export format is PKCS12 because that includes both the cert and key. A PKCS7 file will not contain the key.

Mixed Content Warnings

There are three configuration options to choose from. Please be mindful that leveraging our Let's Encrypt certificates can potentially cause delays. Read more about content mixed content warnings here.

Partial SSL

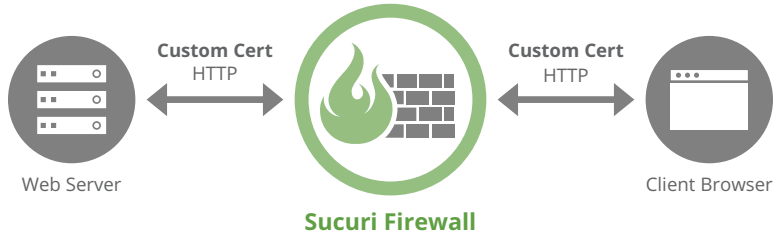
If your website backend does not provide HTTPS, we will proxy HTTPS->HTTP on your behalf. This is not ideal, but we are securing a very large piece of the communication chain between your customers and our network. This is the initial communication with your audience, and the most susceptible to Man in the Middle (MITM) attacks.

Full SSL

This is the most secure and ideal method. We proxy via HTTPS from our edge to the host server also running HTTPS, ensuring that communication is always encrypted in the wire.

Custom SSL

Under the Agency plan, you can use your own Extended Validation (EV), wildcard or any other certificate you have. Please be sure to **upload your cert prior to DNS change** to avoid disruption.



No HTTPS

You can disable HTTPS by forcing all HTTPS traffic to be redirected to HTTP. Just go to Settings->SSL and click on HTTP-only site support.

Onboarding / Environment Evaluation

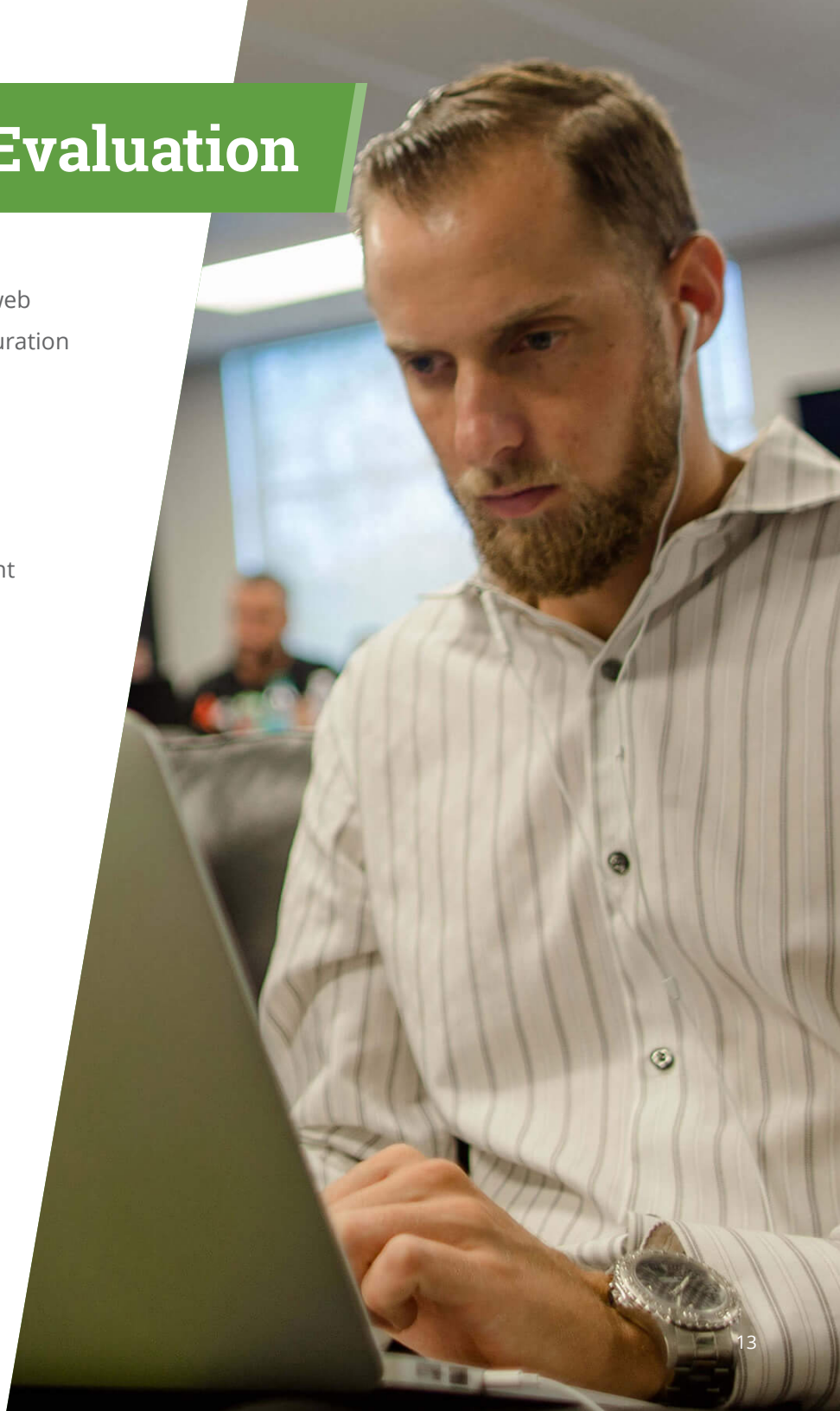
Sucuri realizes that every organization is unique in the deployment of their web properties. For this reason, we offer customized onboarding for each configuration – a tailored experience to match your organization's needs.

As an Agency, you may qualify for an onboarding process that includes a malware review of your server. This will be a critical service if you have any doubt about existing malware on your web properties. Please note: in order to prevent cross-site contamination, any malware review of your environment must be secured post-remediation.

If you've opted for this add-on service, our support team will **require** the following to ensure no onboarding delays:

- Accurate access credentials into your environment (FTP, WHM/cPANEL, SSH, etc.).
- A full list of domains, subdomains, and aliases are needed so Sucuri can add the sites to the monitoring and firewall dashboard.
- The number of sites/domains found in the server fit within the number of licenses available in your account.
- Access to DNS management of your websites. If not available, please let our team know during introductions.
- Please note any existing HTTPS/SSL setups so we can work together to upload any existing certificates in our systems.

If you have any questions about these requirements. or the service, please contact your Sucuri Account Executive.



Case Studies & Testimonials

Don’t take our word for it. See what Agency owners like you have to say.

Big Spring

Why Sucuri:

- Real People
- Industry Leaders
- Attentive Chat Team

Favorite Features

- Response Time
- Depth of Knowledge Base
- Level of Customer Service

"When you have so many clients and so many websites we can't look at everything all the time, so we need someone proactively checking that on our behalf and checking that when we need it. Another thing we like is that Sucuri knows about security issues before they become a problem – in advance."

READ FULL CASE STUDY >>>

Nicely Built

Why Sucuri:

- Affordable Pricing
- Customer Service

Favorite Features

- WordPress Plugin
- Firewall

"The Sucuri Plugin is a great solution. We were daisy-chaining other plugins together for a long time. But when we found Sucuri, we realized we just needed the one, which is awesome because we don't have to worry about code conflicts. It helps our sites stay strong, run close to the rails, and also have high performance."

READ FULL CASE STUDY >>>

Taylor Town

Why Sucuri:

- Highly Recommended
- Competitive Pricing
- Customer Reviews
- Committment to Timeline

Favorite Features

- Unlimited Remediation
- Firewall Protection
- Monitoring
- Ticketing System

"I've been doing WordPress design and optimization for about 3 years and I use Sucuri for malware removal. Recently, I removed malware from two websites for a new client using Sucuri."

READ FULL CASE STUDY >>>

Your Website Security Team

With Sucuri, you get a highly technical team of security professionals distributed around the world, each trained in identifying and fixing any issues you might be faced with. Consider us an extension of your existing team.

Contact us for a free consultation.

sales@sucuri.net

1–888-873-0817

sucuri.net/agency

Website Security Platform

Sucuri is a website security provider for demanding organizations that want to ensure the integrity and availability of their websites. Unlike other website security systems, Sucuri is a SaaS cloud-based solution built on state of the art technology, excellent customer service, and a deep passion for research.