

secureli



SAME-DAY HACKED WEBSITE REPAIR
WEBSITE MALWARE REMOVAL
BANK-GRADE SECURITY

24/7/365 MONITORING & RESPONSE

24/7/365 PHONE SUPPORT

100% UPTIME GUARANTEE

100% MONEY-BACK GUARANTEE

15-MINUTE RESPONSE SERVICE AGREEMENT

ZERO HACKED CLIENTS



Our **24/7/365, U.S.-based team** is here to help repair & protect your digital assets with next-generation monitoring & response.

secureli

Clients **feel peace of mind**, knowing that we have a **100% success rate of cleaning all hacked websites within 24 hours**, as well as a **100% success rate keeping our clients hacker-free since 2013**.

To understand our entire system, think of security in terms of “end to end” - we repair and secure your website, but digital security incidents go beyond just “fixing a website”. It is **important to follow a series of steps after being compromised by a hacker**, including: **working with Google’s security team, freezing your credit, running anti-virus** on your computer, resetting your passwords, and much more that our company will do for you.

Our goal is to provide **emergency repair services** for hacked websites and companies, then **ensure long-term security** using **next-generation, machine-learning antivirus and intrusion prevention systems** with **24/7/365 HUMAN monitoring**.

That’s what separates us from the rest: **two 24/7/365 dedicated account managers, next-generation monitoring systems, and world-class digital security analysts constantly monitoring** our clients’ security for any suspicious or malicious activity.



secureli

24/7/365 PHONE SUPPORT **“POWER OF SPEECH”**

Sure, we offer 24/7 e-mail and chat support.

“Personally, I’ve always found it to be easier to SPEAK to another human who can understand my needs and address my issues over the phone.”

-John Martinelli, Founder

However, our account managers have found more can get done in one phone call than in multiple e-mails!

So, feel free to reach out to either your day-time, or night-time dedicated account managers at ANY time.

If you’re a new client, call us 24/7/365 at

(833) SITE-FIX

Our on-call security specialists are all certified security professionals to help your immediate needs, as well as implement long-term security strategy plans.



100% MONEY- BACK GUARANTEE

WE ONLY WANT YOUR
HONEST BUSINESS.

Our success speaks for itself. Since our grand opening in 2013 (originally, SECURITI.com), we have had **ZERO clients hacked.**

We have a **100% money-back guarantee** if you don't:

- 1) Stay hacker-free while we manage you
- 2) Experience faster page load times
- 3) Improve your company's digital presence with search engine result benefits

Simply **call, e-mail, or text your account manager** and your refund will be processed within 24 hours.

secureli



Threat Intelligence At-Scale

Accurately identify bots by applying behavioral analysis, machine learning and fingerprinting to a diverse and vast volume of globally distributed data.



Integrated Security and Performance

Cloudflare's Bot Management solution seamlessly integrates with its WAF, DDoS and CDN products, enhancing security, user experience, and performance.



Complete Without Complexity

Instant deployment and protection against a full range of bot attacks without Javascript injection and mobile SDK.



Behavioral Analysis

Cloudflare analyzes behavior and detects anomalies in your internet property's specific traffic, scoring every request by how different it is from the baseline.



Automatic Whitelists

Allows good bots, such as those belonging to search engines, to keep reaching your site while preventing malicious traffic.



Mobile App and API Protection

Protects your mobile applications from impersonation and emulation attacks without using mobile SDK. The solution also protects APIs that are accessed via web browsers.



Configuration Flexibility

Granular rules, user-defined mitigations and unique actions beyond the industry standard like render a mock-login or alternative pricing page to thwart bots



Machine Learning

Cloudflare's Machine Learning trains on a curated subset of hundreds of billions of requests per day to create a reliable bot score for every request.

Why do enterprises choose SECURELI?



Massive network scale

A global cloud network that spans 200 cities in more than 90 countries



Ease of use

No code changes required; the SECURELI dashboard enables quick configuration



Integrated security & performance

Deeply integrated products that form a unified control plane



24/7/365 enterprise support

Award winning global customer support with dedicated technical resources and a comprehensive knowledge base



No Surprises Pricing

Transparent pricing structure - flat rate, with unlimited bandwidth and space. 100% uptime guarantee with a 30-minute SLA time..



Developer friendly

Augment existing applications or create entirely new ones without configuring or maintaining infrastructure



Fingerprinting

Cloudflare uses fingerprinting from over 20 million internet properties to accurately classify bots. It does not generate or store device fingerprints, eliminating the risk of user privacy being compromised.



Why do hackers break into websites?

WordPress powers 40% of the websites on the internet today. This makes it a very popular target to research vulnerabilities. And exploit these security holes for a number of reasons.

The most common reasons motivating a hack are:

- Stealing payment information from e-commerce stores, both from the customers, as well as the businesses' bank account / point-of-sale system
- Installing viruses on website visitors, to steal personal information for committing identify theft
- Installing ransomware, forcing you to pay hackers money up-front to fix your website issues
- Stealing company secrets, our internal-use-only documents with sensitive information
- Mining cryptocurrency using your servers/hosts resource
- Using your website to host phishing pages, where visitors are pushed to enter in sensitive information like their bank account username and password, social security number, etc.

MACHINE-LEARNING FIREWALL & ANTIVIRUS

In 2013, we developed a piece of machine-learning software that studied the behavior of malware and various viruses we observed acting “in the wild”...

...that is, genuine hacker intrusions and virus infections of servers on the internet.

We studied the results of these findings and found an interesting result - they always have a “Command and Control” center that provides instructions to these hacked servers, through one channel or another.

Sometimes this is encrypted, sometimes it’s not.

Our network-level security actively improves with the more data we feed it. With 7 years of data, examining over 1 trillion internet requests, our systems have a very low rate of false positives, giving our Security Operation Center (SOC) time to focus on the important aspects of protecting our clients.



secureli

200

Cities covered by our worldwide network, including 17 in mainland China

20M+

Internet properties experiencing increased performance and security

99%

Internet users in the developed world within 100ms

8K+

Interconnected networks bringing you and your customers together

CONTENT DISTRIBUTION NETWORK

< 1 SECOND PAGE LOAD



secureli

When it comes to user experience, search engines are your biggest critics.

Page load time is the #1 factor, besides SSL (which, by the way, is included at no cost for all of our clients), in determining the ranking factor of your website in Google search engine result pages.

Page load time is also very important for mobile optimization. 73% of users have “exited out” of websites that were slow to respond on their phone.

Without our global network of servers, we deliver your website’s content to the closest server in physical proximity, resulting in less than 300 milliseconds of time on our end of the network.



Performance

Cloudflare Performance Services improve conversions, reduce churn, and improve visitor experiences by accelerating web and mobile performance, while keeping applications available.



Content Delivery Network (CDN)

Spanning 200 cities across 90 countries, Cloudflare's Anycast CDN caches static content at the edge, reducing latency by delivering assets as close as geographically possible to visitors.

[Learn More >](#)



Workers

Cloudflare Workers let developers run JavaScript Service Workers in Cloudflare's global cloud network across 200 cities.



Mobile SDK

Cloudflare's Mobile SDK provides visibility into application performance and load times across any global carrier network.



Railgun™

Railgun compresses previously unreachable web objects by leveraging techniques similar to those used in the compression of high-quality video. This can result in additional performance increase.

Security

Cloudflare Security Services reduce the risk of lost customers, declining revenues, and degraded brand by protecting against DDoS attacks, abusive bots, and data breach.



Anycast Network

With 200 cities across 90 countries and 30 Tbps of capacity, Cloudflare's Anycast network absorbs distributed attack traffic by dispersing it geographically, while keeping Internet properties available and performant.



Argo Tunnel

Cloudflare creates an encrypted tunnel between its nearest data center and an application's origin server without opening a public inbound port.



Access

Secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare.



Secure Registrar

Cloudflare is an ICANN accredited registrar, protecting organizations from domain hijacking with high-touch, online and offline verification for any changes to a registrar account.



Stream

Cloudflare Stream makes streaming high quality video at scale, easy and affordable.



Orbit

Cloudflare Orbit solves security-related issues for Internet of Things devices at the network level.



Website Optimizations

Cloudflare includes a suite of web optimizations to improve the performance of Internet assets. Optimizations include the latest web standards, such as HTTP/2 and TLS 1.3, as well as proprietary enhancements for images and mobile device visitors.



DNSSEC

DNSSEC is the Internet's non-spoofable caller ID. It guarantees a web application's traffic is safely routed to the correct servers so that a site's visitors are not intercepted by a hidden "man-in-the-middle" attacker.



Load Balancing

Cloudflare Load Balancing provides load balancing, geo-steering, monitoring and failover for single, hybrid-cloud, and multi-cloud environments, enhancing performance and availability.



Rate Limiting

Rate Limiting protects critical resources by providing fine-grained control to block or qualify visitors with suspicious request rates.



Argo Smart Routing

Argo Smart Routing improves Internet asset performance on average of 30% by routing visitors through the least congested and most reliable paths on Cloudflare's private network.

[Learn More >](#)



SSL / TLS

Transport Layer Security (TLS) encryption enables HTTPS connections between visitors and origin server(s), preventing man-in-the-middle attacks, packet sniffing, the display of web browser trust warnings, and more.

[Learn More >](#)

WHITE-GLOVE WEBSITE SECURITY MANAGEMENT

If you decide to host your website on our platform, you will receive a huge amount of value.

That being said, we are NOT the lowest cost, but we can we ARE the highest quality WordPress website security management and hosting platform.

Never worry about updates, conflicts, downtime, or hosting again.

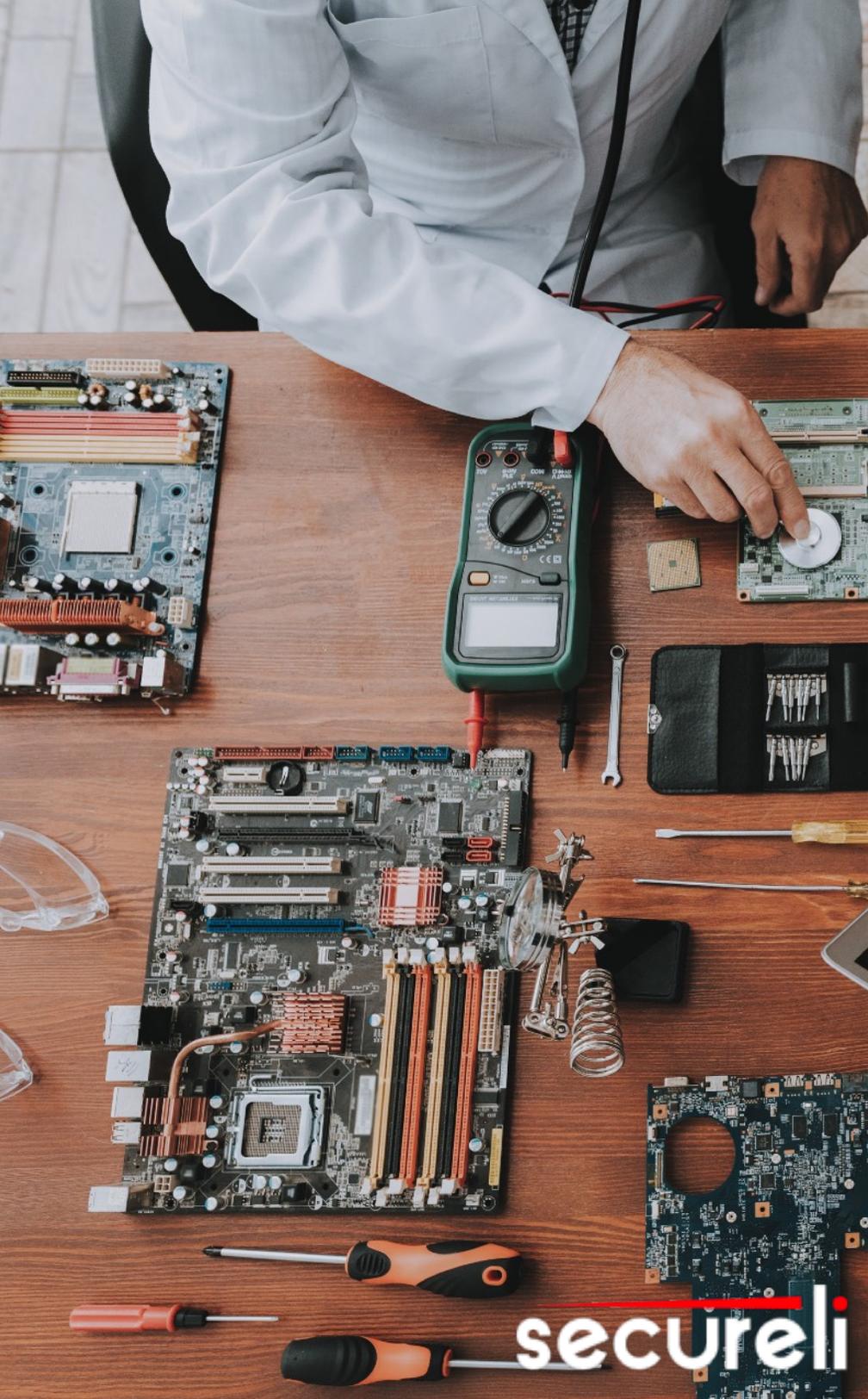
We guarantee a 100% uptime, due to our partnerships with CloudFlare and WPEngine.com

When your website is being protected by SECURELI, don't worry about uptime, backups, updates, upgrades, plugins, spam, or anything.

We've got you covered.

secureli





24/7/365 BACKUPS WITH 1-CLICK RESTORE

The most important defense against hackers attacking your website are clean, **DAILY** backups of your website.

Since we have a clean backup of your website, if there's ever an issue with security, a change to your website, or an SEO problem, we can simply roll back to your last clean backup in 1 click.

That's what WE manage - disaster recovery plans.

Although we have had zero clients successfully hacked since 2013, we truly believe this is because we have the best "Disaster Recovery Policies" in the business.

With a single click, our analysts can freeze a website, analyze the traffic in real-time, and determine if malicious activity is occurring.

If this is the case, your website is "frozen", restored to it's last known clean state, and our team will analyze the log files to identify what went wrong, while your site stays online just fine!

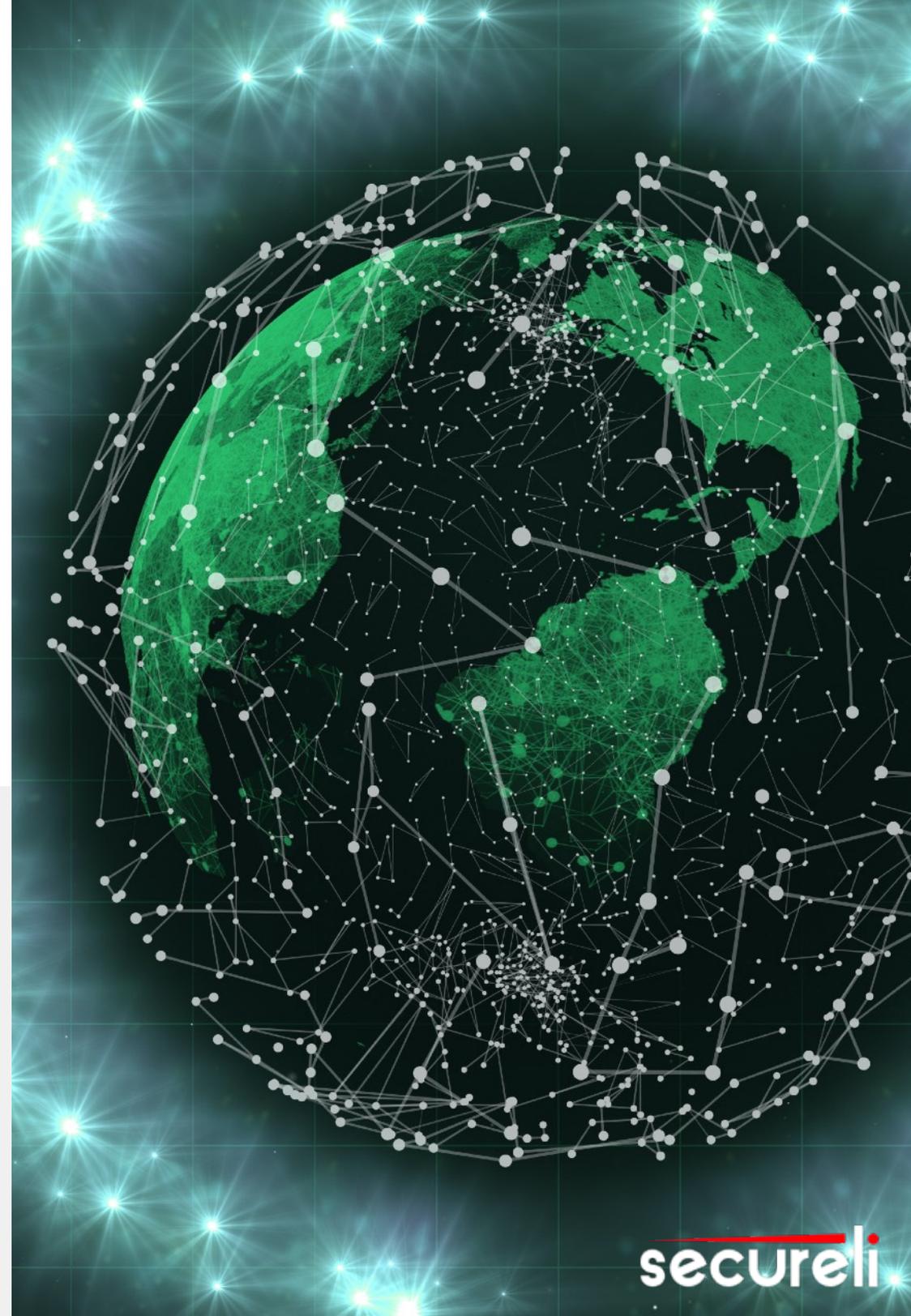
secureli

CONSTANT "MAN & MACHINE" MONITORING

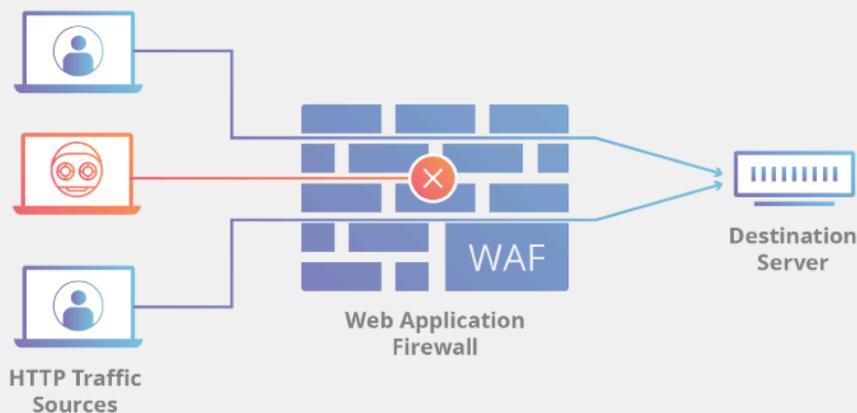
When we first started in the business, the digital security landscape was very different.

Today, there are more automated, sophisticated attacks that we encounter on a daily basis.

Our business thrives off off the 1 trillion pieces of data we have fed into our machine-learning web application firewall, with 24/7 human monitoring and constant improvements to our defense platform by our security software development team.



A [web application firewall](#) or WAF helps protect a web application against malicious [HTTP](#) traffic. By placing a filtration barrier between the targeted server and the attacker, the WAF is able to protect against attacks like cross site forgery, cross site scripting and SQL injection. [Learn more about Cloudflare's WAF.](#)





MONTHLY REPORTS FOR MARKETING & SECURITY

Due to the nature of our hosting platform, you will see an immediate improvement of your search engine results.

We take great pride in providing the best security platform, which Google rewards due to the various benefits (page load time, complimentary HTTPS, mobile optimization, etc.)

Every month, your account manager will attempt to schedule a call with you to go over:

- 1) What has been going well this month
- 2) What has room for improvement
- 3) What actions can we take to improve your website's conversion rate - that is, maximizing the percentage of your website visitors that turn into customers.

If you already have a website marketing company that does your SEO, we would love to bring them into the meetings with you so we can provide the highest level of value possible.

MARKETING BENEFITS

HTTPS-“ALWAYS”

All of our clients get https:// in front of their website address! Not only does this ensure users trust your site, it's a MAJOR benefit for Google and other search engines to rank you highly. It's very important to encrypt your website traffic using HTTPS.

PAGE-LOAD TIME

80% of our sites load in under 500 milliseconds. 99% load in under 1 second.

The other 1% are extremely advertising heavy in digital and high-resolution banner ads.

By loading in <1 second, your website gets an INSTANT search engine improvement.



secureli

WHO IS
ATTACKING
YOUR WORDPRESS WEBSITE





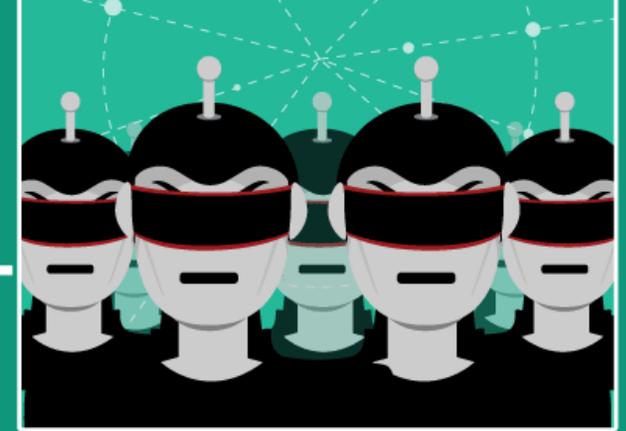
SINGLE BOT

An automated computer that can attack one site at a time or a small number of sites simultaneously. Usually unsophisticated attacks.



PERSON

Operates a computer manually, attacks one site at a time, slow in attacking but thorough.



BOTNET

A group of computers, can be thousands, attacking multiple sites simultaneously and rapidly. Attacks are unsophisticated but can originate from multiple IP's which add complexity.

How do they get information?



**THROUGH
RECONNAISSANCE
USING THESE
INFORMATION
SOURCES:**

Using tools to
automate scans

OS Recon with port scans
and OS fingerprinting

(OSINT) **Open Source
Intelligence Sites**

Enumerating
themes and plugins

Examining server
response headers

WordPress version
publicly displayed

(SSRF) **Server Side
Request Forgery**

Author scans

What is being attacked on WordPress sites?

VULNERABILITIES IN PHP CODE INCLUDING WORDPRESS CORE, THEMES, PLUGINS AND OTHER PHP APPLICATIONS:

RCE - Remote Code Execution

SQLi - SQL Injection

XSS - Cross Site Scripting attacks

CSRF - Cross Site Request Forgery

PHP Object Injection

RFI - Remote file inclusion

Authentication Bypass

XXE - External Entity Expansion
(an XML based attack)



PRIVILEGE ESCALATION

• A ordinary user with non-admin access can find a way to escalate their privileges to 'admin' level access



OLDER AND UNMAINTAINED WEB APPLICATIONS HOSTED ON THE SAME HOSTING ACCOUNT

- A WordPress install in a subdirectory that is not maintained
- An application like phpmyadmin that is forgotten about and unmaintained
- Backups of your WordPress directory in a subdirectory that are executable PHP and forgotten about



XMLRPC SERVICE

- Brute force logins
- DDoS attacks launched via XMLRPC e.g. Trackback



THE LOGIN PAGE VIA:

- Brute force attacks
- Recon to check if usernames exist



ON SHARED HOSTING:

- World writable directories. An attacker on the same machine can install a shell on your website.
- Wp-config.php world-readable can give an attacker on the same machine access to your database.
- World-writable files can allow an attacker to execute code as your website.



SOURCE CODE REPOSITORY CONFIG FILES

- .git subdirectory can contain source that is intended to be private
- .svn subdirectory can contain sensitive info



TEMPORARY FILES CREATED BY OTHER APPLICATIONS NOT INTENDED FOR PUBLIC ACCESS

- When the 'vim' editor is used, the temporary file it creates can be web accessible and allow access to sensitive files like wp-config.php containing login credentials for MySQL



ATTACKS THAT TARGET THE OPERATING SYSTEM AND WEB SERVER

- Attacks that target the web server. E.g. Heartbleed
- Attacks that target the operating system services e.g. Shellshock, SSH vulnerabilities, vulnerabilities in other services.

Benefits / Services for Clients



1. Secured website hosting with a 100% uptime guarantee
2. Hacked website repair in under 24 hours
3. 24/7/365 U.S.-based phone support
4. 100% money-back guarantee
5. Fully managed WordPress hosting
6. Daily backups of your website with one-click restore
7. Next-generation web application firewall to protect against new threats
8. Hosting on Google Cloud & Amazon Web Services cloud infrastructure
9. Unlimited bandwidth and file space at no cost
10. Guaranteed significant website performance improvement
11. Complimentary HTTPS (SSL/TLS) certificate and installation
12. Monthly status reports (always) and meetings (at your request) to discuss your website's security, performance, and marketing
13. Access to our full stack website & software development team
14. Access to our Mobile Optimization, Organic Marketing, and Paid Marketing team
15. SFTP, SSH, and WP-Admin access
16. Free 30-day trial of our cloud hosting environment

Total Cost:

~~**\$747/year per website**~~
\$497/year per website
or \$47/mo per website

Comparison Chart





Uptime	100% guaranteed	99.99% guaranteed	99.99% guaranteed
Support	24/7/365 Phone, E-mail, and Chat	Ticket System	Live Chat + Ticket System
Money-Back Guarantee	90 Days	30 Days	30 Days
Complimentary SSL	✓	✗	✗
Backups	Constant	Daily	Daily
Dedicated Account Manager	✓	✗	✗
Malware Removal	Free (<24 hours)	Free (no guaranteed timeline)	Free (no guaranteed timeline)
Private Cloud WordPress Hosting	✓	✗	✗
Fully Managed Patching & Updates	Same-Day	✓	✓
Fully Managed Firewall & Security	Constantly	Constantly	Once Daily
Malicious Activity Monitor	Constantly	Constantly	Once Daily
Automated Threat Detection & Removal	Constantly	Constantly	Once Daily
Blacklist Removal	✓	✓	✓
Website Response Time	<1s	Varies	Varies

100% PCI Compliant



Security Scans

Every 30 Minutes

Every 6 Hours

Daily

Malware Detection

Every 30 Minutes

Every 6 Hours

Daily

Security Anomaly Detection

Every 30 Minutes

Every 6 Hours

Daily

Blacklist Monitoring

Every 30 Minutes

Every 6 Hours

Daily

File Change Detection

Every 30 Minutes

Every 6 Hours

Daily

DNS Monitoring

Every 30 Minutes

Every 24 Hours

Daily

SSL Monitoring

Every 30 Minutes

Every 24 Hours

Daily

Web Application Firewall (WAF)



Intrusion Detection System (IDS)



DDoS Attack Mitigation



Brute Force Protection



Block Hack Attempts



For Agencies

Most of our clients are agencies that use our services for their clients.

Some of our clients up-sell our security service to their clients, while others prefer we work silently in the background with the agency. Every engagement is custom.

There are a few ways we can provide bank-grade security services for your clients:

Monitoring

- Hourly Security Scans
- SMS & E-mail Alerts
- **24/7/365 Phone, E-mail, & Ticket Support**
- Weekly White-label Security Reports
- Actionable alerts with all information needed to resolve the security vulnerability

Monitoring and Management

- Includes all Monitoring features.
- Daily backups with **one-click restore**
- Unlimited malware removal at no cost
- Full security - automatic plugin, theme, and WordPress updates

Monitoring, Management, and Hosting

- Includes all Monitoring & Management features.
- Bullet-proof hosting with **100% uptime**
- Guaranteed hack-free due to **24/7/365 Security Operation Center** and **Website Application Firewall**

READY TO GET STARTED?

If you are a website owner, give us a call @ **(833) SITE-FIX** or fill out the form on <https://secureli.com/go> to get your website repaired today.

If you are an agency, please call us @ **(833) SITE-FIX** or your **SECURELI** account manager to discuss any questions you may have to get started.

"We look forward to providing you complete peace-of-mind, by providing 24/7/365 security defenses by combining next-generation automated defense tools, in addition to manual, human-powered security analysis.

We look forward to providing world-class digital security services to your company."

-The Team @ SECURELI

secureli



SAME-DAY HACKED WEBSITE REPAIR
WEBSITE MALWARE REMOVAL
BANK-GRADE SECURITY

24/7/365 MONITORING & RESPONSE

24/7/365 PHONE SUPPORT

100% UPTIME GUARANTEE

100% MONEY-BACK GUARANTEE

15-MINUTE RESPONSE SERVICE AGREEMENT

ZERO HACKED CLIENTS