Sucuri Technical Overview

Product and Service Description

TABLE OF CONTENTS

SUCURI OVERVIEW

PRODUCT/SERVICE DESCRIPTION

EXHIBITS

SUCURI OVERVIEW

COMPANY OVERVIEW

Sucuri is a globally-recognized security company, specializing in providing comprehensive security to website owners. A US-based company founded in 2010, Sucuri maintains a global presence with employees in over 23 countries distributed across the major continents to ensure support is accessible 24/7/365. It provides website security services to over 45,000 paying customers around the world, remediates over 500 infected websites a day, monitors over 400,000 websites and handles over 16 billion unique page views a month.

All of Sucuri's technology is proprietary, built by our team of security engineers and researchers. The technology is designed to address the growing online security threats as they emerge. Our team is dedicated to ensuring the confidentially, integrity, and availability of every website within the Sucuri network.

At Sucuri, we care and treat every website as if it's our own. The solution we offer is built on three core pillars – Protection | Detection | Response. We take a Defense-in-Depth approach to website security, in which we employ multiple layers of security to provide the most comprehensive solution available. Combining people, process, and technology ensures that websites are cared for and attacks are mitigated as quickly and efficiently as possible.

These pillars allow Sucuri to deploy a defensive solution to stop the attacks from ever abusing website components. This prevention solution is coupled with a continuous scanning engine designed to identify any rogue elements that might prove to be indicators of a potential compromise. Finally, Sucuri provides a professional Incident Response Team (IRT) in the event that an attack is successful, giving businesses peace of mind through our obsessive attention to current and emerging threats within the website security domain.

PEOPLE, PROCESSES, AND TECHNOLOGY

There are no turnkey solutions to security; instead it's a combination of people, processes, and technology that help create a manageable and scalable approach to security for any organization. Sucuri's products are designed to reduce a brand's risk of a breach through the deployment of both proactive and reactive mechanisms addressing each of the elements described above. Sucuri's solution is a complementary offering that bolts onto an organization's existing security controls, satisfying a number of governance requirements while alleviating and enabling security teams to continue to focus on their core responsibilities.

PRODUCT/SERVICE DESCRIPTION

Sucuri provides a comprehensive security solution for websites called the website security platform. It is comprised of four core functions designed to provide organizations a holistic end-to-end security solution for an organization's website properties.

MONITORING

The monitoring technology is a cloud-based Software as a Service (SaaS) Intrusion Detection System (IDS) built on the concept of a Network-Based Integrity Monitoring System (NBIMS). The monitoring system is a remote and local (server-side) continuous scanning engine, providing near real-time visibility into the security state of a website.

Our IRT is designed to detect multiple Indicators of Compromise (IoC), to include, but not limited to:

- Malware Distribution
- Blacklisting Incidents
- SEO Spam
- SSL Certificates
- Phishing Lure Pages
- Whois Changes
- DNS Changes

The monitoring feature includes an alerting engine in the event an IoC is detected. Then the appropriate Security Operations Group (SOG) is notified to take immediate action by the security IRT.

Activating monitoring requires no installation or application changes. All sites are added and configured via the Sucuri dashboard. To enable the server-side scanning, a PHP agent is required at the root of the main domain.

Note: Monitoring events can be outputted to an organization's System Information and Event Management (SIEM) upon request.

PROTECTION

The Sucuri Firewall is a cloud-based SaaS Website Application Firewall (WAF) and Intrusion Prevention System (IPS) for websites. It functions as a reverse proxy by intercepting and inspecting all incoming Hypertext Transfer Protocol/Secure (HTTP/HTTPS) requests to a website, stripping it of malicious requests at the Sucuri network edge before it arrives at your server. The Sucuri Firewall includes both Virtual Patching and Virtual Hardening engines that allow for real-time mitigation of threats with no impact to the website.

The Sucuri Firewall is built on a Content Distribution Network (CDN) that provides performance optimization features to a website. The CDN utilizes a proprietary approach to caching dynamic and static content across all nodes in the network to ensure optimal performance around the world.

Additionally, the Sucuri Firewall offers full Domain Name Server (DNS) services.

The Sucuri Firewall runs on a Globally Distributed Anycast Network (GDAN), built and managed by the Sucuri team. The GDAN configuration allows for high availability and redundancy in the event of any failures in the network. Sucuri currently manages six Points of Presence (PoP).

Points of Presence

San Jose, CA

Dallas, Texas

District of Columbia (DC)

London, United Kingdom

Frankfurt, Germany

Tokyo, Japan

The firewall is supported by the Sucuri Security Operations Center (SOC) which provides 24/7/365 monitoring and response to all attacks. Some of the features that the Sucuri Firewall offers a website owner include:

- Mitigation of Distributed Denial of Service (DDoS) Attacks
- Prevention of Vulnerability Exploit Attempts (i.e., SQLi, XSS, RFI / LFI, etc...)
- Protection Against the OWASP Top 10 (and more)
- Access Control Attacks (i.e., Brute Force attempts)
- Performance Optimization

The Sucuri Firewall requires no installation or application changes. It is done via DNS by adding an A record or switching to Sucuri nameservers.

RESPONSE

The response system offers a professional Security Incident Response Team (IRT). This team is available to respond to all website-related security incidents, including issues identified by Sucuri and even those that aren't. The team is highly trained and capable of mitigating all website infections and malware-related issues.

This solution exists because of the complex nature of website security. Intrusions occur for a variety of reasons. Although our various technologies are being employed to assist in the prevention of such compromises, there are things beyond Sucuri's control. Examples include, poor user/password management or creation, poor security configurations, and other similar environmental issues. Because of the expanded attack vector outside of Sucuri's control, the response feature was designed to provide organizations a complementary team to assist in the identification and eradication of any successful compromises. This would include analyzing the cause, assisting in the patching of the issue, and restoring the environment to operational order.

Response addresses all website infections, including but not limited to:

- Server Level Malware Infections
- Website Malware Infections
- SEO Spam Injections
- Malicious User Redirects
- Website Defacements
- Removal of all Backdoors
- Removal of Website Blacklist Annotations

Our response solution requires no installation, or application changes. It does require direct access to the web server / application via FTP/SFTP or SSH.

BACKUP

The backup system provides an organization continuous operations in the event of an emergency; it offers storage of all website files and databases in a remote location on Sucuri's network. In the event of an issue, the backups are available to an organization.

Backups requires no installation or application changes. All sites are added and configured via the Sucuri dashboard.

EXHIBIT A: HOLISTIC NETWORK DIAGRAM (SUCURI FIREWALL)

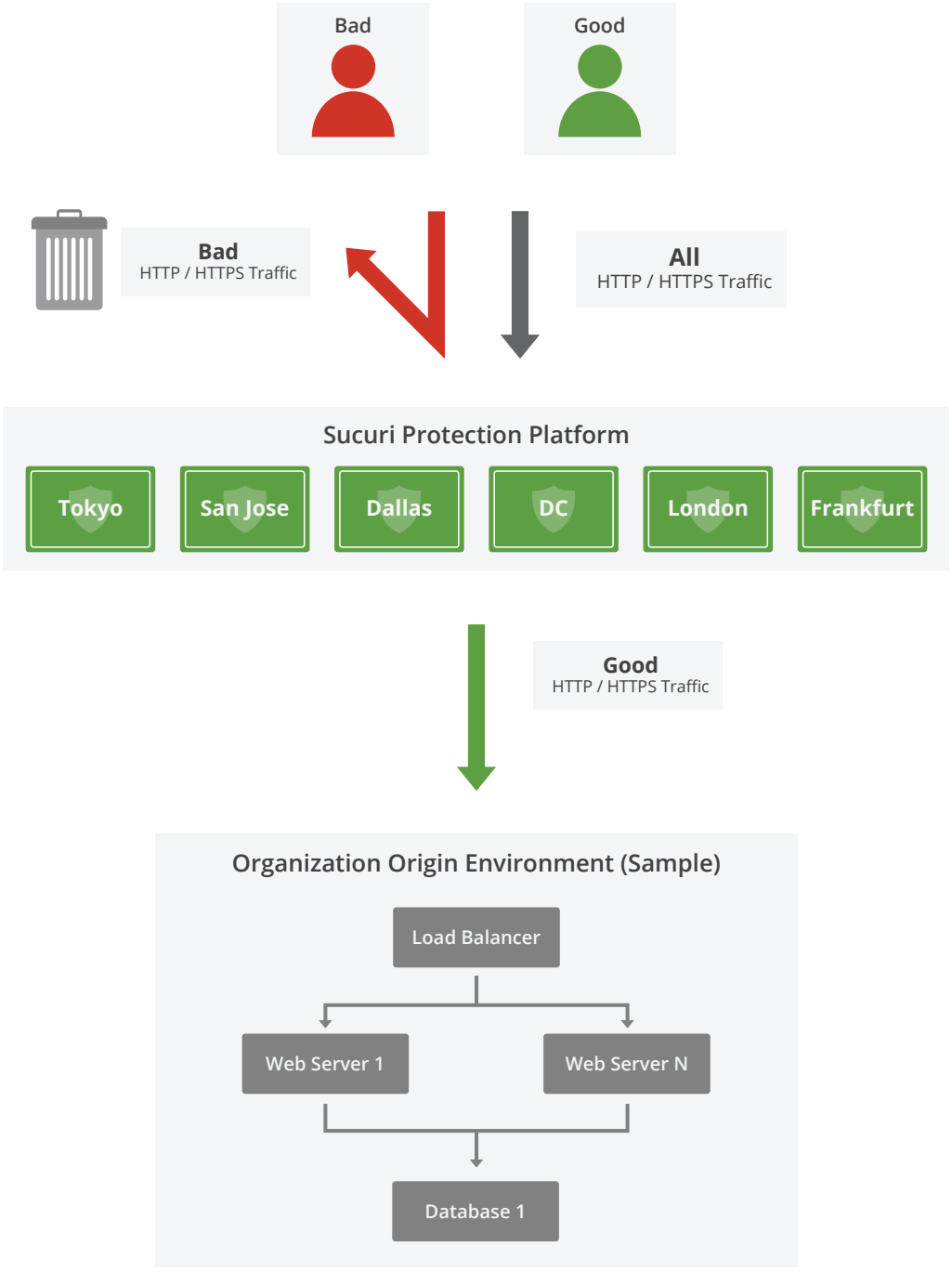

EXHIBIT B: DDoS MITIGATION

Mitigation of Distributed Denial of Service (DDoS) attacks is a key feature the Sucuri Firewall offers its customers.

NETWORK-BASED DDoS (N-DDoS) ATTACKS (A.K.A VOLUMETRIC ATTACKS)

Sucuri's approach to mitigating network-based attacks includes investing in resources across all PoP locations. It's built on an Anycast network that allows the distribution of all inbound traffic across the network, explicitly blocks all non-HTTP/HTTPS-based traffic. The current network capacity is in excess of 250 Gigabytes Per Second (GPS). Each PoP has multiple 10G and 40G ports from different providers, all designed to absorb and scale to very large inbound traffic requirements and attacks.

APPLICATION-BASED DDoS (A-DDoS) ATTACKS

These attacks are designed to disrupt a website's availability by attacking the server resources directly. Flooding a server with requests, an attacker is able to consume local server resources to the point where the server becomes incapable of responding to legitimate requests. In these cases, the website will become unresponsive. The order of magnitude is very different; these attacks are measured in Requests Per Second (RPS) and can begin at 100/200 requests per second for many web servers.

Sucuri's approach to mitigating these attacks is part technology, part human, and part machine intelligence. The firewall employs technology that allows the team and engine to profile and analyze requests across the entire network, allowing us to accurately strip malicious requests from benign requests. Additionally, within the Sucuri network websites can support 300k + RPS per website.

EXHIBIT C: EXPLOIT PREVENTION

Preventing remote exploit attempts that try to abuse software vulnerabilities, such as those identified by the Open Web Application Security Project (OWASP), is a critical feature of the firewall. These attacks may include exploit attempts against the website directly and target things like injection (e.g., SLQi, XSS, etc.), remote code execution (RCE), security misconfiguration, remote file inclusion (RFI), and many other vulnerabilities.

The Sucuri Firewall uses a proprietary multi-tiered approach to identifying and stripping malicious application requests.

Tier 1	Application Profiling	The first tier uses a deny-all approach and whitelist model, where all requests that don't fit an application's profile are blocked explicitly at the edge. This profile is built dynamically on the technology/CMS a website is using. No third-party services are used.
Tier 2	Blacklist Engine	The second tier uses a custom-built blacklist signature blocking model built by the Sucuri team to account for any potential outliers or evolving threats. No third-party services are used.
Tier 3	Correlation Engine	The third tier analyzes all requests across the Sucuri network to profile attacker behavior and apply it globally to all sites protected by Sucuri. This is a learning engine that proactively applies updates to the network as the threat landscape evolves.

Additionally, the Sucuri Firewall employs a Virtual Patching and Virtual Hardening approach to its mitigation strategy:

VIRTUAL PATCHING	With virtual patching, the Sucuri team is able to quickly respond to emerging threats with no impacts to a website. All patches are applied at the Sucuri edge. This is especially effective for larger organizations with strict security governance on when and how patches can be applied to a production environment. Additionally, custom rules can also be applied.
VIRTUAL HARDENING	With virtual hardening, the Sucuri team is able to apply vulnerability-agnostic patches to a website. Hardening can be specific to the CMS (i.e. WordPress, Joomla!, Drupal, etc) or more generic to a web server (i.e. Apache/IIS).

The effectiveness of the firewall is limited to its ability to see all incoming traffic. The most common evasion technique is for attackers to attack the origin server directly, which is why it's important that all direct traffic to the origin server is restricted to the Sucuri network.

EXHIBIT D: EXPLOIT PREVENTION

The Sucuri Firewall is able to mitigate attacks by intercepting all incoming traffic and performing real-time analysis of all requests over HTTP/HTTPS protocols (i.e., Layer 7 requests). Traffic that is encrypted (i.e., utilizes HTTPS) must be inspected as well.

To achieve this, end-point termination must occur at the Sucuri edge. The firewall, by design, must intercept and analyze all traffic to be effective. All analysis is done in memory, real-time - **there is no storage of the request packets**. The only data that is stored is the metadata of a request, in the form of web access logs.

Organizations have multiple options when dealing with SSL:

OPTION 1	Use Comodo DV certs that Sucuri will generate.
OPTION 2	Use a Free LetsEncrypt cert that Sucuri will generate.
OPTION 3	Use a custom cert provided by the organization.
OPTION 4	Sucuri provides a CSR for organizations to generate a cert via their CA.

EXHIBIT E: INSTALLATION AND CONFIGURATION

Each function has its own configuration and deployment requirements, but each are designed to be simple and require low overhead and engagement. Requirements are as follows:

PROTECTION	No installation required. A-record switch via DNS. Also support full DNS management via nameserver swap. Time to go live is dependent on Time to Live (TTL) value.
MONITORING	No installation required. Remote Scanning: Domains are loaded into the Sucuri Dashboard via API or Dashboard interface. Server Scanning: Domain PHP agents are loaded at the root of each website directory on the web server. **Requires SFTP/FTP/SSH access to load files. Organization can choose to load files on their own.
RESPONSE	No installation required. In the event of an incident, all Malware Removal Requests are handled and managed via the Sucuri ticketing system. Support engagement and SLA is dictated by your agreement. Does require access to the server via SFTP/FTP/SSH. Changes might be outlined in your agreement.
BACKUP	No installation required. Does require access to the server via SFTP/FTP/SSH. Changes might be outlined in your agreement.

Some agreements include custom support and integration services. Defer to your agreement and account manager for specifics pertaining to deployment for each function and associated responsibilities.

EXHIBIT F: PERFORMANCE OPTIMIZATION AND CACHING

All static content is cached when possible. This allows for faster responses to requests (500 ms vs 10 ms) and scales (50 concurrent users vs. 200k concurrent users). Standard known CMSs like Wordpress, Joomla!, Drupal and other similar CMS applications use cookies. We're aware of this and account for it in our caching logic.

The caching feature works by building a cache key. Every request that matches that key gets the same page. The cache key is comprised of the HTTP or HTTPS, domain, request URL, and normalized user agent (i.e. mobile, desktop, tablet, or RSS bot). This means that users of different devices (i.e. desktop vs mobile) won't see the same content.

CACHING OPTIONS

The CDN offers four means of caching:

OPTION	OPTION DESCRIPTION	TIME
Enabled (Recommended)	Caches entire site and only purges cache every few hours.	All - 3 hrs +
Minimal Caching	Caches entire site and purges cache every few minutes.	200 - 8 m 404 - 2 m 302 - 15 m 301 - 15 m
Site Caching (Site Headers)	Caches static content and respects site headers.	200 - 180 m 404 - 10 m 302 - 180 m 301 - 180 m
Disabled (Use w/caution)	Only caches static files such as images, .css, .js, .pdf, .txt, .mp3 and a few more extensions.	200 - 1 m 404 - 1 m 302 - 10m 301 - 10m

CLEARING CACHE

Clearing (purging) cache is a critical feature of the CDN. We allow cache to be cleared via the Sucuri Dashboard or the WAF API. Once initiated, the cache propagates through the network and clears all nodes within seconds.

EXHIBIT G: INFRASTRUCTURE SECURITY AND COMPLIANCE

Every data center we operate from meets or exceeds all standards and compliance regulations:

COMPLIANCE REGULATIONS

SSAE16 COMPLIANCE
OHSAS 18001:2007
PCIDSS PAYMENT CARD INDUSTRY STANDARD
ISO CERTIFICATION
ISO 9001:2008
ISO 14001:2004
ISO / IEC 27001:2005 AND 27001:2013
ISO 50001:2011

NETWORK INFRASTRUCTURE

Sucuri's network consists of multiple transit providers at each location that is utilized for primary traffic routing, internal traffic routing, and redundancy.

Utilizing a shared network with a primary and secondary termination for each connection prevents a single point of failure.

OPERATIONS

- Daily device vulnerability scan performed internally
- Daily vulnerability and compliance scan performed by third parties
- In-house penetration testing and third-party testing
- Documentation, practices, and continuous employee education
- Firewall change management procedures
- Data classification and ownership
- Incident management
- BCP (Business Continuity Plan) & DRP (Disaster Recovery Plan)
- Continuous network and log monitoring and review

MANAGEMENT AND HUMAN RESOURCES

- Mandatory security awareness training and review for each employee
- Strict least-privilege access practices throughout teams
- Required non-disclosure & confidentiality agreements
- Background checks and skills assessment
- Active management in all aspects of the security community
- Stay current in the ever changing cyber world

sucuri.net | 1.888.873.0817 | sales@sucuri.net