Key Steps to Secure your Customer Facing Web Application

WHITEPAPER

INTRODUCTION

The standard features of web applications define the success of your business. Web applications such as websites, online services, mobile apps make it possible with greater efficiency. Many SMBs are now using web apps to interact with customers, track workflows, automate tasks, and other requirements. But the persistently evolving web threats and attacks can put entire enterprises at risk.

Businesses need to secure their website from hackers, but the challenge here starts with the website vulnerabilities. Few common challenges because of hackers are DOS and DDOS attacks, SQL injections, Cross-Site Scripting, Phishing, Path Traversal, Local File, and Inclusion. Overcoming these challenges requires complex concepts and convoluted solutions. Yet, there are standard best practices to follow to enhance your website's security.

Security has unlimited boundaries that are curbed by cost. While there are no limits to secure a web application, there are some basic considerations for security. Working backward, thinking from the shoes of hackers is the best approach to solve security challenges. Sun Technologies utilizes the expertise of seasoned and certified ethical hackers and security analysts to advise security for a web application based on the requirement, budget, timeline.

What and what not to compromise is the most crucial factor in securing the web application. Following are the three essential steps to enhance web application security to protect your customers, business, and network.

01. Securing the Infrastructure & Network

The exponential increase of threats to your sensitive data and network infrastructure can make your employees unhappy and your company inoperable in some ways. But, the encouraging fact is that you can tighten your network infrastructure and security parallelly.

The process of tightening the infrastructure is mandatory to secure networks. Tightening includes steps to block all ports by default and open if required and to pause and discard unused services. Enterprises should develop tightening policies for each device based on its function in the network.

Outlined below are few essential network components that enhance your infrastructure security and ensure your network remains an asset rather than a liability.

1.1 VPC & Load Balancers

Setting up a Virtual Private Cloud(VPC) helps enterprises improve privacy, security and prevent proprietary data loss.

1.2 Reverse Proxy

A reverse proxy provides load balancing services for seamless web experiences and imposes web application security at the necessary insertion points in a network through firewalls.

1.3 Web Application Firewall (WAF)

WAF helps secure your web applications or APIs against general web threats that affect security, availability and utilize extreme resources. takes two approaches to analyze and filter the IPs in the HTTP requests.

Whitelisting: WAF denies all requests by default and allows only trusted requests.

Blacklisting: WAF allows the packets with the user's preset signatures to block malicious web traffic and protect web applications.

1.4 App Shielding Tools

Using a shield to perform heuristic analysis of logs periodically makes the network remains protected. For example, AWS Shield protects the web applications from the most common, frequently occurring network and DDoS attacks.

Also, operational methodologies are necessary to keep the standards and configurations updated. Choosing the right strategies can help you stay on top of emerging security threats without ignoring your network infrastructure. The perfect device configurations alone are not enough to protect your network infrastructure from threats. You need to restrict the unauthorized users and allow access only for authorized users. Sun Technologies' experts have enormous expertise in creating standards and will work with your team to develop all essential norms and methods. The created standards produce tightened configurations and enhance your network security.

02 Securing the Application

Web Applications are the most convenient channel for cyber attackers who steal data or breach user's security defenses. Your web applications may face cyber threats from both outside and within. Enterprises nowadays use vulnerable components in the development phase to mitigate the risks. The awareness about web application security has increased, and therefore they adopt best security practices to ensure web applications with robust security. Continuous security testing is one of the ideal solutions for regularly running web applications to reduce potential vulnerabilities by fixing and enhancing security.

In addition to adopting continuous security testing, there are few other areas your enterprise can focus on to protect web applications better.

2.1 Encryption at Rest, Transit

Protecting sensitive data in transit and at rest is mandatory for modern businesses as hackers find more innovative ways to understand systems and steal data. For protecting data in transit, organizations prefer to encrypt sensitive data before moving and use encrypted connections to secure data content in transit. Companies can encrypt sensitive files before storing them and encrypt the storage drive to protect data at rest.

2.2 Rate Limiting

Implementing rate limits allow better flow of data and improve security by reducing attacks such as DDoS.

2.3 Authorization and Authentication

Authentication and Authorization help capture the malicious/unauthorized activities and maintain the internal accounts systemized. Ensure every account has only the required permissions so that your team can identify any unusual behavior early and take the necessary actions.

The right architecture makes your development phase easy and secures your application. Our web application architecture covers all the required performances and acknowledgment to a customer, generally on a web browser. A web application will have multiple distinct layers that include servers, business, and data in the backend. There are different architectures comprised of multiple layering approaches depends upon the requirement. In addition to that, creating web application security is also essential. Our dedicated web application development team ensures that all web applications' business requirements and production goals are accomplished without any security threat when deployed within the production environment. We perform architecture and code review against our standardized checklist to ensure there are no security loopholes.

2.4 API Gateways

One of the prominent roles of API gateway authentication is API gateway. It executes the complete functions of APIs that are running behind and manages authentication and authorization. Thus, it protects your applications and data against unnecessary access, exploits, threats, and data breaches. It also enables you to reduce the amount of data transmitted to prevent attacks and one API user from overloading the web application.

2.5 Authorization in Service Layer

The business service layer is the first layer you have to consider implementing your authorization checks seriously. Suppose all your external-facing access points depend on the business service layer to perform the functions that they need. In such a case, your authorization checks will be efficient. Here, you usually have all the conditions you require to make better security decisions.

When deploying authentication in your serverless application, follow the below two steps:

- Store user sessions
- Retrieve users identity in your serverless functions

2.6 Cookie-Based Authentication

In cookie-based authentication, the client and server will have to maintain the token to manage a session between the pages for a user. Since cookies are small in size, it is stored on both the client and server. The server stores the cookie in the database to keep track of every user session and allows the client to hold the session identifier. Cookie-based authentication makes your application stateful and is efficient in tracking and customizing the state of a user.

2.7 Storage-Based Authorization

The metastore server security is configured to use Storage-Based Authorization; it uses the file system permissions for folders. Roles are determined at the system level, so they are valid for all databases in the system. For Example, MongoDB allows Role-Based Access Control (RBAC) to give access to a MongoDB system. A user is assigned one or more roles that define the user's access to database resources and functions. Outside of role assignments, the user has zero access to the system.

03. Practicing & Governing Security throughout SDLC

Secure SDLC is vital because application security is essential. Gone were the days where the bugs are addressed once the product is released.

Developers now need to be aware of potential security problems at each phase of the projects' process. Integrating security into your SDLC is the right solution as anyone can get access to your source code. Therefore, opting for a reliable and secure SDLC process is crucial to ensure your application is free from security threats. Build a security layer during SDLC for a protected cyber environment. It is vital to maintain the developed security policies at different phases of the software development life cycle, ensuring secure software development.

Following are some of the best practices enterprises can consider to tighten the security in SDLC:

3.1 Static Code Analysis

Performing static code analysis in SDLC does not need a working application and can occur without code execution. The enterprise may face the challenge of finding the right resource to perform code reviews on applications. Static Application Security Testing tools(SAST) (e.g., Sonar Qube, Veracode) can analyze 100% of the codebase and find critical vulnerabilities that include SQL Injection, buffer overflows, and much more.

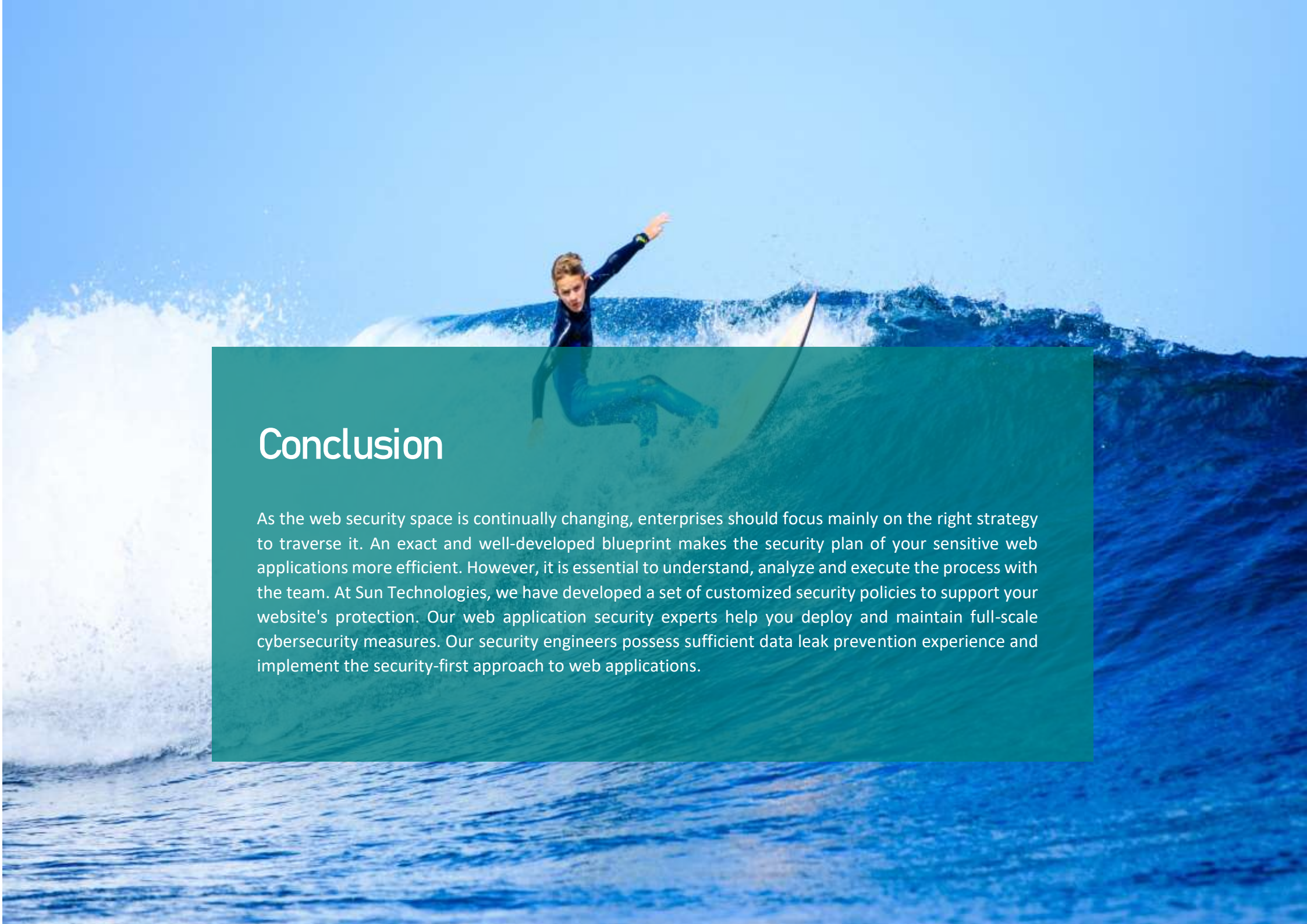
3.2 Vulnerability and Penetration Testing

Executing a web penetration test needs not only expertise but also a considerable amount of time. Ethical hackers reduce assessment duration and correct exposures before attackers identify them. A right-thinking penetration tester can automate multiple tasks with the proper tools, especially during early stages such as observation and scanning. Tools such as Sonar, Checkmark, Burp Suit are some of the best tools for penetration testing. These tools help you identify exploitable vulnerabilities and map your targets.

3.3 DevSecOps

DevSecOps delivers security in the earlier stage of SDLC, thus reducing vulnerabilities and unite application development, IT operations, Quality Assurance teams, and security teams under a common DevSecOps space.

Sun Technologies offer the right skills, performance, and experience to you based on your requirement. Our best-of-breed pentesters possess the expertise to match your security needs and business requirements. Our efficient requirement analysis and completion of the project on time and within the budget enable our customers to achieve greater business visibility, innovation, and return on investments.



Conclusion

As the web security space is continually changing, enterprises should focus mainly on the right strategy to traverse it. An exact and well-developed blueprint makes the security plan of your sensitive web applications more efficient. However, it is essential to understand, analyze and execute the process with the team. At Sun Technologies, we have developed a set of customized security policies to support your website's protection. Our web application security experts help you deploy and maintain full-scale cybersecurity measures. Our security engineers possess sufficient data leak prevention experience and implement the security-first approach to web applications.

Vaidyanathan Ganesa Sankaran
Head – Solution Architect, Sun Technologies

Vaidy is Lead Solutions Architect, heading sales and project delivery for Cloud (AWS, Azure), DevOps, and legacy modernization projects at Sun Technologies. With over 15+ years of experience, he has a demonstrated history of working in the information technology and services industry. He also holds a Master of Science (MS) in Computer Software Engineering from BITS Pilani.

ABOUT SUN TECHNOLOGIES

Established in 1996, Sun Technologies Inc. is recognized as an award-winning and innovative IT solutions company, specializing in IT Infrastructure Modernization, Digital Transformation, Test Automation, Mobile Applications, Cloud/DevOps, and Game Testing Services with expertise in many technologies in the areas such as Databases, Servers, Operating Systems, Cloud, Storage, Virtualization, Middleware, and Security. Learn how Sun helps clients lead with digital at www.suntechnologies.com.

Corporate Headquarters: Alpharetta, USA

Global Offices: India | UK | UAE | Switzerland | Denmark | Australia

For more information please contact: marketing@suntechnologies.com | www.suntechnologies.com