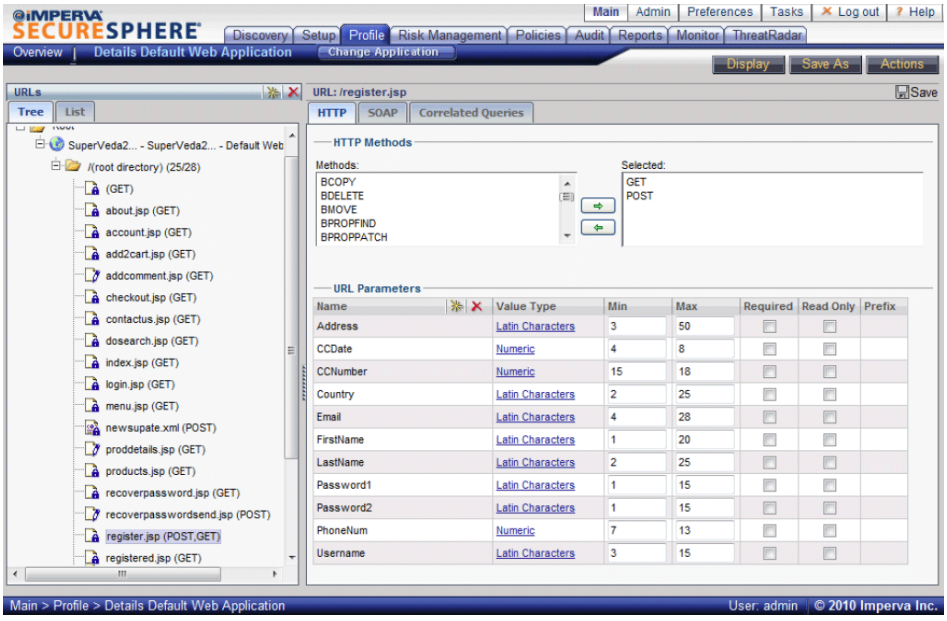
Dynamic Profiling

Because Web applications are unique, they have distinct structures and dynamics, and – unfortunately – different vulnerabilities. A web application security device, therefore, must understand the structure and usage of the protected applications. Depending on the complexity of the protected application, this task can entail managing thousands or even hundreds of thousands of constantly changing variables including users, URLs, directories, parameters, cookies, and HTIP methods. Imperva's patented Dynamic Profiling technology completely automates the management by learning application structure and usage with little to no manual tuning. This paper explains how Imperva's Dynamic Profiling streamlines configuration, provides up-to-date and accurate security, and substantially reduces administrative overhead.

Automated Application Learning

Dynamic Profiling is the cornerstone of Imperva's automated approach to Web application security. SecureSphere's Dynamic Profiling automatically models an application's structure and elements to learn legitimate user behavior such as acceptable form field values and protected cookies. Valid application changes are automatically detected and incorporated into the profile over time. By comparing profiled elements to actual traffic, SecureSphere can detect unacceptable behavior and prevent malicious activity with pinpoint precision.



Dynamic Profiling automatically builds a profile of application elements, structure and usage, including URLs, form fields, parameters, cookies and expected user input.

Dynamic Profiling overcomes the biggest drawback of other application firewall solutions- manual rule creation and maintenance. Unlike network firewall solutions where policy may be limited to a few dozen static rules, application firewall policy requires hundreds or thousands of rules governing thousands of constantly changing variables including URLs, parameters, cookies, XML elements and form fields.

Dynamic Profiling Over Time

Any application security architecture that relies upon manual rule creation by a security administrator requires constant rule-base tuning to account for changes to the applications. For example, many web application firewalls require manually created rules to define expected behaviors for client-side scripts. These manual rules specify detailed application variables such as allowed URLs, parameters, parameter types, and parameter constraints. Maintenance of these rules can be a major source of operational overhead as many sites rely on hundreds of scripts. Any script change requires a parallel rule change to avoid false positives.

Considering that many security managers are not kept abreast of all application changes, manually maintaining a white list security model is untenable.

In contrast, Dynamic Profiling automatically recognizes and incorporates changes into the profile over time. Because web applications often change, SecureSphere's automatic learning capability ensures that the application profile is always up-to-date. While customers can lock sensitive URLs or directories to prevent them from being updated automatically, almost all customers rely on SecureSphere's Dynamic Profiling capability to detect and adapt to application changes. Dynamic Profiling delivers completely automated security without requiring manual configuration or tuning.

Customizing the Application Profile

While Dynamic Profiling automatically builds the profile of protected web applications and detects application changes over time, it is also possible for organizations to manually adjust the application profile. All aspects of SecureSphere's application profile are customizable – meaning that customers can modify the application profiles to bridge any differences between actual usage and corporate security policies. If desired, customers can even manually define the complete web application profile through the SecureSphere management interface.

Dynamic Profiling in Depth: Technical Specifications

Dynamic Profiling relies on a statistical analysis model to accurately build the web application profile. By analyzing web requests and responses to the production web applications, SecureSphere dynamically models the application structure, elements and expected application usage. It takes approximately 2-5 days of analyzing live traffic to build the application profile.

SecureSphere automatically profiles the following elements:

- URLs
- Directories
- Cookies
- Form fields and URL parameters
- HTIP methods
- Referrers
- User authentication forms and fields for application user tracking
- XML elements
- SOAP actions

In addition, SecureSphere determines expected user behavior by analyzing many different web users and their usage patterns. Expected usage attributes include:

- Form field and parameter value length (approximate minimum and maximum length)
- If a parameter is required or if is optional
- If a parameter can be modified by the end user
- The parameter value type (for example, numeric, Latin characters, foreign characters)
- Allowed character groups (slash, white spaces, quotes, periods, commas, etc.)
- If a cookie is protected or if it can be modified by the user
- If a cookie must be set by the web server or if it can stored in the browser cache

Differentiating Between Legitimate and Illegitimate Activity

Because SecureSphere automatically learns application elements, structure and usage based on real web traffic, it must differentiate between acceptable user requests and application attacks. Otherwise, it might be possible for SecureSphere to add illegitimate requests to the application profile. SecureSphere uses the following techniques to differentiate between acceptable and malicious activity:

- SecureSphere ignores known malicious behavior (HTTP protocol violations, known attack signatures like SQL injection, double encoding, etc.) when building the profile
- SecureSphere analyzes server responses. If the web server replies with an error code such as "404: Not Found" or "500:Internal Server Error", then SecureSphere will ignore the request
- SecureSphere ignores web requests that have no referrer or have an external referrer unless the server generates a "200: OK" or a "304: Not Modified" response code. These types of requests may be generated by robots or scripts.
- SecureSphere analyzes many different attributes when developing the web application profile. It builds the profile based on the number of occurrences, length of time, and uniformity of requests.
- In addition, customers can restrict learning to trusted source IP addresses. Or customers can ignore non-trusted IP addresses.

SecureSphere automatically updates the profile over time.

- The administrator can be automatically alerted every time the profile changes.
- For profile updates, the behavior must be repeated by multiple sources. In addition, the behavior must be seen a certain amount of times per hour during a minimum number of hours. By default, most elements will be learned if the element is accessed by at least 50 different IP addresses or users and if the behavior is repeated at least 50 times for at least 12 different hours. All of these profile settings are configurable.

Note: Requested URLs that are not available (that generate a 404: Not Found error) will not be included in the standard application profile, but SecureSphere will track these URLs as broken links.

All of the aspects of the profile can be edited through the web management interface. However, Imperva's Dynamic Profiling capability is usually more accurate than manual configuration because it detects hidden form fields, optional form fields that are generated by scripts, and web pages that are not linked to other parts of the web site. That is why most SecureSphere customers rarely modify the dynamic profile.

SecureSphere administrators can determine how the dynamic profile is built. Learning can be limited to a pre defined set of known, trusted users. Profile update settings (for example, a parameter 'read-only' status will be removed if at least 50 unique web users change the parameter over a 12 hour period) can also be adjusted.

Application User Tracking

SecureSphere's innovative Dynamic Profiling technology automatically discovers web-based login pages. When users login to corporate web applications, SecureSphere will associate the user name with the session ID. So, SecureSphere can track and enforce security policies by user.

Dynamic Profiling: A Security Model that Is Positive In Every Way

Imperva's Dynamic Profiling addresses the manageability issues that plagued first generation web application firewalls. Now, organizations can protect their sensitive web applications and back end data without introducing excessive IT overhead and without blocking legitimate web users. Dynamic Profiling is the cornerstone of SecureSphere's positive security model. Combined with SecureSphere's other security measures, including HTTP protocol validation, application, web server software and operating system attack signatures, web services security, web worm defense, custom correlation rules, and ThreatRadar Reputation Services, SecureSphere protects both custom and packaged applications accurately without false positives. Organizations can deploy SecureSphere in minutes with no changes to existing applications or infrastructure to lockdown critical web applications and to meet security and compliance requirements.