Virtis Intelligence™

Web Application Shielding Vulnerability Intelligence

10-100x faster & cheaper than fixing code or replacing software

Make 100% vulnerability mitigation a reality!

EXPOSURE IS NOT AN OPTION.

IN A COMMODITIZING WAF MARKET

WHY VIRTIS Vi?

We pick up where WAFs leave off

There are some great tools out there. But if you don't know how to use them properly or have the resources to manage them, what good are they?

The Market

The internet is a huge business enabler; it provides:

1) Lots of apps and services that your employees can leverage for productivity.
2) A promotional and distribution mechanism to get your applications or services to the global market.

It is also a dangerous place; Cybercrime is now 3x bigger than the drug trade and growing:

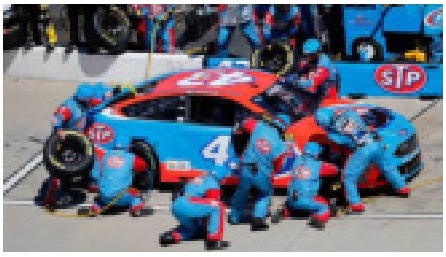
1) Behind the useful apps are malicious scripts and applications,
2) Highly skilled criminal gangs and even adversarial government funded actors

Where you publish your applications to customers, partners and employees, can be at risk. Skilled hackers and robots continually scan the internet from the shadows. They build inventories of your component technologies and then exploit either opportunistically or in targeted attacks. Awareness doesn’t help here; they can attack anytime without warning. Given the poor state of application code and hosting infrastructure we are seeing more and more exploits occurring through this channel.

Whitehat Security reveals that for the 40% of companies that do get regular application security audits, on average 11 vulnerabilities are discovered and on average these remain open for 300 days.

99% remediated is still 100% exploitable.

Would you trust your car to win the Daytona 500 by giving your driver just a torque wrench? You need a pit crew.



The Role of a Web Application Firewall

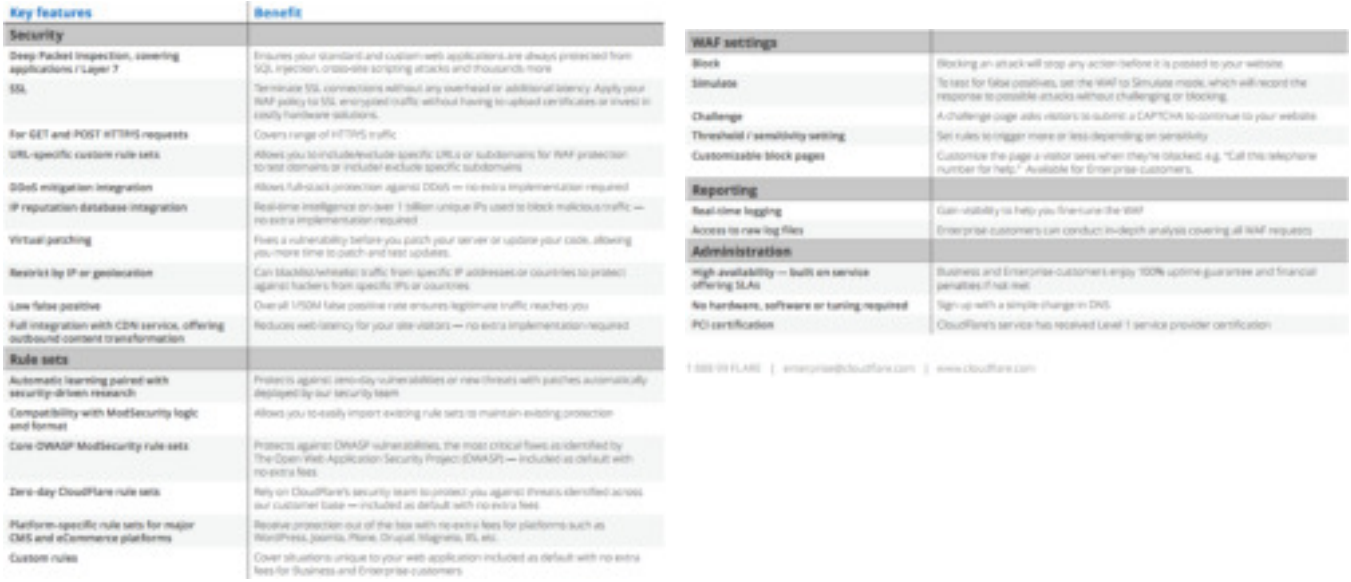
The Web Application Firewall (WAF) is a technology that has emerged to assist with this problem. A WAF can be configured to blacklist traffic (use signatures to block malicious requests), and/or to whitelist traffic (only allow defined pages, parameters, file types etc).

When configured correctly, a WAF can block a large number of generic technical exploitable flaws in a web application without requiring developers to remediate a single line of code.

As WAFs operate at the HTTP layer they do not maintain application state, hence do not address application logic flaws, that is a task for the Software Development community.

Given a WAF is typically deployed for externally facing applications, where DDoS protection and CDN capabilities are also required, Cloud WAFs that combine these three capabilities have grown in popularity.

With Cloud WAF services your security team is able to configure the WAF for your application through templates, machine learning, dashboards and APIs. They are typically promoted as a range of security controls that can scrub your traffic. They still require you to develop the skills to optimise the tool yourself.



Key features	Benefit
Security	
Deep Packet Inspection, covering applications / Layer 7	Ensures your standard and custom web applications are always protected from SQL injection, cross-site scripting attacks and thousands more
SSL	Terminate SSL connections without any overhead or additional latency. Apply your WAF policy to SSL encrypted traffic without having to upload certificates or invest in costly hardware solutions.
For GET and POST HTTPS requests	Covers range of HTTPS traffic
URL-specific custom rule sets	Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/ exclude specific subdomains
DDoS mitigation integration	Allows full-stack protection against DDoS — no extra implementation required
IP reputation database integration	Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required
Virtual patching	Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates.
Restrict by IP or geolocation	Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries
Low false positive	Overall 1/50M false positive rate ensures legitimate traffic reaches you
Full integration with CDN service, offering outbound content transformation	Reduces web latency for your site visitors — no extra implementation required
Rule sets	
Automatic learning paired with security-driven research	Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team
Compatibility with ModSecurity logic and format	Allows you to easily import existing rule sets to maintain existing protection
Core OWASP ModSecurity rule sets	Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees
Zero-day CloudFlare rule sets	Rely on CloudFlare's security team to protect you against threats identified across our customer base — included as default with no extra fees
Platform-specific rule sets for major CMS and eCommerce platforms	Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc.
Custom rules	Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers
WAF settings	
Block	Blocking an attack will stop any action before it is posted to your website
Simulate	To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking.
Challenge	A challenge page asks visitors to submit a CAPTCHA to continue to your website
Threshold / sensitivity setting	Set rules to trigger more or less depending on sensitivity
Customizable block pages	Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers.
Reporting	
Real-time logging	Gain visibility to help you fine-tune the WAF
Access to raw log files	Enterprise customers can conduct in-depth analysis covering all WAF requests
Administration	
High availability — built on service offering SLAs	Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met
No hardware, software or tuning required	Sign up with a simple change in DNS
PCI certification	CloudFlare's service has received Level 1 service provider certification

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Figure 1 Cloudflare's security control options

The VIRTIS Vi Difference

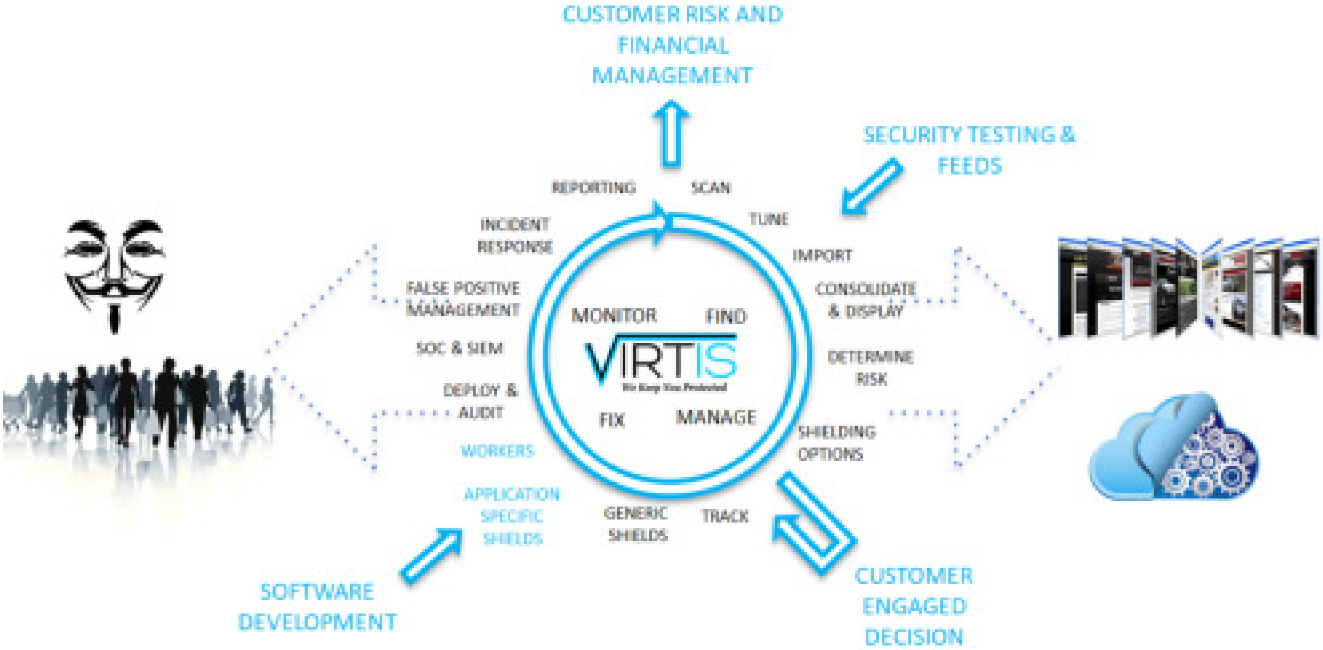
VIRTIS Vi has taken a different approach to the same under-lying problem. VIRTIS Vi's premise is that you should prioritise mitigation of discovered exploitable security flaws in your application. Blocking all conceivable threats is an infinite problem, however an exploit only materializes when threat traffic matches a finite set of application specific vulnerabilities.

To deliver business outcomes, you have to address EVERY discovered exploitable vulnerability. It is not enough to address only some of the issues. **99% remediated is still 100% exploitable.**

To achieve this result, VIRTIS Vi claims that:

1. WAFs are useful, but more advanced tools are also required to address application stateful business logic flaws.
2. If a flaw is still exploitable, whether by design or misconfiguration, it is not resolved, hence continuous testing is required
3. Automation and Machine-Learning assistance is necessary, but highly skilled and focused staff are also required to supervise, train and augment those systems. In this specialist area, experience & muscle memory for both deployment and incident response is required.
4. Mature processes are needed to ensure consistent and high-quality results 24/7.

To this end, VIRTIS Vi has built a "Do It For Me" advanced managed security service that uses CMMI 3.0 processes with highly skilled operators using a range of tools, including but not limited to WAF, to find, manage, fix, monitor and report on the status of Web Application security risk.



Powered by RedShield

Figure 2 The VIRTIS Vi Service provides all the skills and processes to produce a risk management outcome from a range of tools

Security controls are tailored to YOUR specific vulnerabilities and risks

Reported Application Exploit	Application Exploit Specific Shield
SQL Injection (SQLi)	Parsing, Input validation then either WAF REGEX signatures or Rewrite REQs to escape user input
Obsolete Apache Web Server	Server response header removed, analysis of relevant CVEs and specific exploit defenses enabled. Still recommend upgrade, but risk greatly reduced
Out of Date OpenSSL Library	VIRTIS Vi's hardened SSL stack used towards the client
Server Side Cross Site Scripting (XSS)	Parsing, Input validation then either WAF REGEX signatures or Rewrite REQs to escape user input
Fragment DOM Based Cross Site Scripting (XSS)	Rewrite the exploitable JavaScript files and replace it when requested
Multiple Direct Object Reference Issues	Protect hidden fields from manipulation by signing accepted values during server responses
Cross Site Request Forgery	CSRF tokens inserted into links, forms and JavaScript
Session Token Sent in the URL	Session token removed from the URL between VIRTIS Vi and client, stored in a cookie then reinserted into requests when
LDAP Injection	Parsing, Input validation then either WAF REGEX signatures or Rewrite REQs to escape user input
Unencrypted Communication to Report Server	Out of Scope – VIRTIS Vi cannot address some server to server issues To solve VIRTIS Vi would need to be in path for both servers
Insufficient Idle Timeout	Maintain and enforce an idle timeout session on the VIRTIS Vi proxy. Mitigation includes JavaScript redirects as required by iFrames
Insecure File Upload	Redirection of files to a AV/Sandbox device for media classification, size and virus detection. Then security policy enforcement based on information returned
User Enumeration	Rewrite login errors with a generic message
Security headers/flags unset	Insertion of HSTS and X-Frame-Options, X-XSS-Protection, X-Content-Type plus removal of Server, X-powered-by and Version server response headers. Setting of Secure and HTTPOnly cookie flags. Note insertion or even creation of Content-Security-Policy maybe possible however requires further discussion
Weak HTTPS cryptographic protocol SSLv3	Use a strong SSL between VIRTIS Vi and the Client
Form Field Autocomplete	Enumerate all forms with username and password, transform responses to disable autocomplete in line with recommended practise. Note that some browsers may override this.
Verbose Error Messages	Determine error codes and replace body with customized content
TRACE method enabled	Only allow whitelisted HTTP methods
Cacheable HTTPS responses	Modify caching headers
Content Spoofing (injecting messages)	Whitelist allowed message values
Session Cookie is short/predictable	Add random data, encrypt, maintain session state on proxy, dynamically substitute cookies
Session logout not preventing reuse	Track session state on proxy, disallow logged out session reuse
Session Information in URI	Substitute in Responses, maintain state and reconstruct Requests
Insufficient Authorization	Can be simple blacklist URI; or per-user response data redaction
Insecure redirects	Whitelist redirects, or sign trusted redirect values when issued

Figure 3 VIRTIS Vi Advanced Shielding Plan for all YOUR detected issues

For each of YOUR detected exploitable flaws, VIRTIS Vi Security Researchers, Analysts, Engineers and Developers will determine shielding options and propose a pragmatic approach to either eliminate or reduce your risk. In many cases, complete mitigation is possible; when it isn't, the residual risk will be specified, and/or additional remedial action required by the customer specified.

If you don't have a security testing report, then VIRTIS Vi still offers a range of Monitored and Audited controls. Skilled staff executing robust processes will scan, review, tune, monitor, report and respond. DDoS and baseline Application Change Tolerant WAF shields will be deployed to protect your application to world's best standards.

Why WAFs Deployments Fail

Problem 1: WAFs don’t do enough

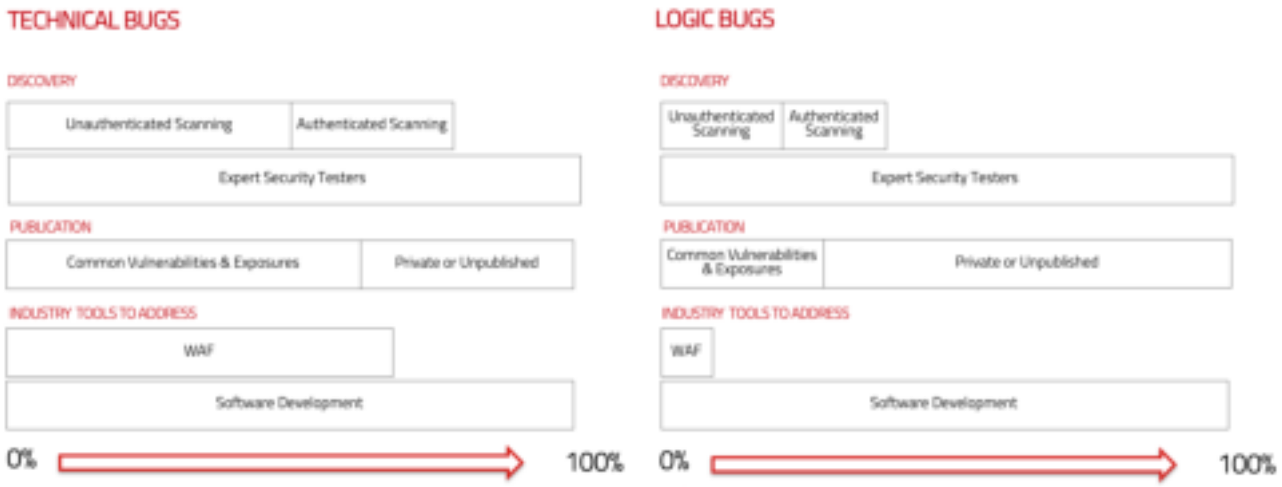


Figure 4 Common Discovery, Publication and Remediation of Web Application Security Bugs

Technical Bugs

Common exploits and coding mistakes (or mistakes by omissions) e.g. lack of input validation, direct object referencing etc.

WAFs have a predefined number of controls that predominantly analyze requests from a client to either detect explicitly bad requests based on known attacks, or explicitly good requests based on learned known application behaviour.

In this manner they can address large array of technical threats and these map through to the protection of technical vulnerabilities.

Logic Bugs

Code is working as designed, however attackers can manipulate the logic for nefarious means. These logic flaws occur within the context of the application itself, hence WAFs are unable to address them. These need to be addressed by software developers.

The security community has conducted many ‘000,000s of Penetration Tests and have concluded that of those issues discussed approximately 50% are Technical and 50% Logical.

Gartner’s Perspective

At the Gartner Security & Risk Management Summit in 2017, in their State of Application Security presentation, Gartner classified threats facing web applications and API as either DOS, Exploit, Abuse of functionality or Access Violation.

Gartner concluded that external devices could be effective at addressing DOS and Exploit threats (Technical Bugs) but that SDKs and DevSecOps is required to assist developers to address the Abuse of functionality and Access Violation problems (Logic Bugs).

So how does this relate to your vulnerabilities? Consider the following real world example

Security Bug Reference	Class	Severity	Threat	Score	Status
45850184	SQL Injection	5	5	15	WAF REGEX Mitigation
45850185	Insufficient Authorization	5	5	15	Developer to fix
45850186	Cross Site Scripting	4	5	14	WAF REGEX Mitigation
45850187	Insufficient Authentication	4	5	14	Developer to fix
45850188	Information Leakage	3	5	13	Developer to fix
45850189	Credential/Session Prediction	4	4	13	Developer to fix
45850190	Insufficient TLS Protection	4	3	12	DDoS Mitigation
45850191	Insufficient TLS Protection	4	3	12	WAF Platform Mitigation
45850192	Brute Force	3	4	12	Developer to fix
45850193	Session Fixation	4	2	11	Developer to fix
45850194	URL Redirector Abuse	3	2	10	Developer to fix
45850195	Predictable Resource Location	3	2	10	Developer to fix
45850196	Content Spoofing	3	2	10	Developer to fix
45850197	Insufficient Session Expiration	2	2	9	Developer to fix
45850198	Insecure Session Cookie	1	1	7	Developer to fix
45850199	Non-HTTP Only Session Cookie	1	1	7	Developer to fix
45850200	Autocomplete Attribute	1	1	7	Developer to fix

Figure 5 Real example of WAF mitigation vs Software developer remediation from a Pen Test report

Unfortunately, as shown in figure 5, for a large number of high value online applications, the delta between what can be protected by a WAF and that detected by a skilled Penetration Tester is substantial.

Even 99% remediated is still 100% vulnerable and a WAF on it's own falls well short of this mark.

VIRTIS
We Keep You Protected

VIRTIS Vi Answer 1: Modify application behaviour without touching code

In addition to a WAF for rudimentary threat protection and simple bugs, VIRTIS Vi implements a programmable interception proxy. With this proxy VIRTIS Vi developers are able to create custom software objects to manipulate the contents and context of the message flows between the customer & VIRTIS Vi and VIRTIS Vi & the server independently.

With this custom developed message logic manipulation, VIRTIS Vi developers are able to resolve the vast major of exploitable logic flaws. Figure 6 is a case study example of what VIRTIS Vi was able to deliver within 5 days.

Reference	Class	Severity	Threat	Score	Status
45850184	SQL Injection	5	5	15	Transform Content
45850185	Insufficient Authorization	5	5	15	Transform Logic
45850186	Cross Site Scripting	4	5	14	Transform Content
45850187	Insufficient Authentication	4	5	14	Transform Logic
45850188	Information Leakage	3	5	13	Transform Content
45850189	Credential/Session Prediction	4	4	13	Transform Logic & Content
45850190	Insufficient TLS Protection	4	3	12	DDoS Mitigation
45850191	Insufficient TLS Protection	4	3	12	WAF Platform Mitigation
45850192	Brute Force	3	4	12	Add Logic Control
45850193	Session Fixation	4	2	11	Transform Logic & Content
45850194	URL Redirector Abuse	3	2	10	Transform Content
45850195	Predictable Resource Location	3	2	10	Transform Logic
45850196	Content Spoofing	3	2	10	Transform Logic
45850197	Insufficient Session Expiration	2	2	9	Transform Logic
45850198	Insecure Session Cookie	1	1	7	Transform Content
45850199	Non-HTTP Only Session Cookie	1	1	7	Transform Content
45850200	Autocomplete Attribute	1	1	7	Transform Content
45850207	Autocomplete Attribute	1	1	7	Transform Content

We Keep You Protected

Problem 2: WAF's break the application for normal users

The False Positive Problem

When deploying Cloud WAF templates or controls, typically a 'tuning' period is required. During this phase the WAF is in a staging mode where the policy is applied to traffic. If a violation occurs the event is alerted, but the traffic is not blocked.

A skilled operator then views the alert log and assesses whether taking a blocking action would be legitimate or whether the WAF is alerting on something that is actually allowed. If the situation is the latter, i.e. a False Positive, then the WAF policy must be tuned to not alert in that specific case.

Once the policy has been thoroughly tuned to minimise future False Positives it is switched into blocking. Note: if machine learning has been used to create this policy, it is often very difficult to get management to agree to transition into blocking.

If tuned correctly, further False Positives should be rare but are still possible/inevitable, the industry states that False Positive rates of 0.2% are best practise. So on 1000 blocks, 2 are mistakes.

The process for handling false positives must be robust. There must be a communication mechanism to enable users that claim that they have been blocked by mistake to get their complaint through to an expert who can assess whether their request is legitimate, can technically resolve the issue and can assess whether the fix would result in incremental security risk to the application.

All of this has to occur in minutes. Delays in this area, with the WAF blocking legitimate traffic, are the primary reason a large number of WAF projects fail.

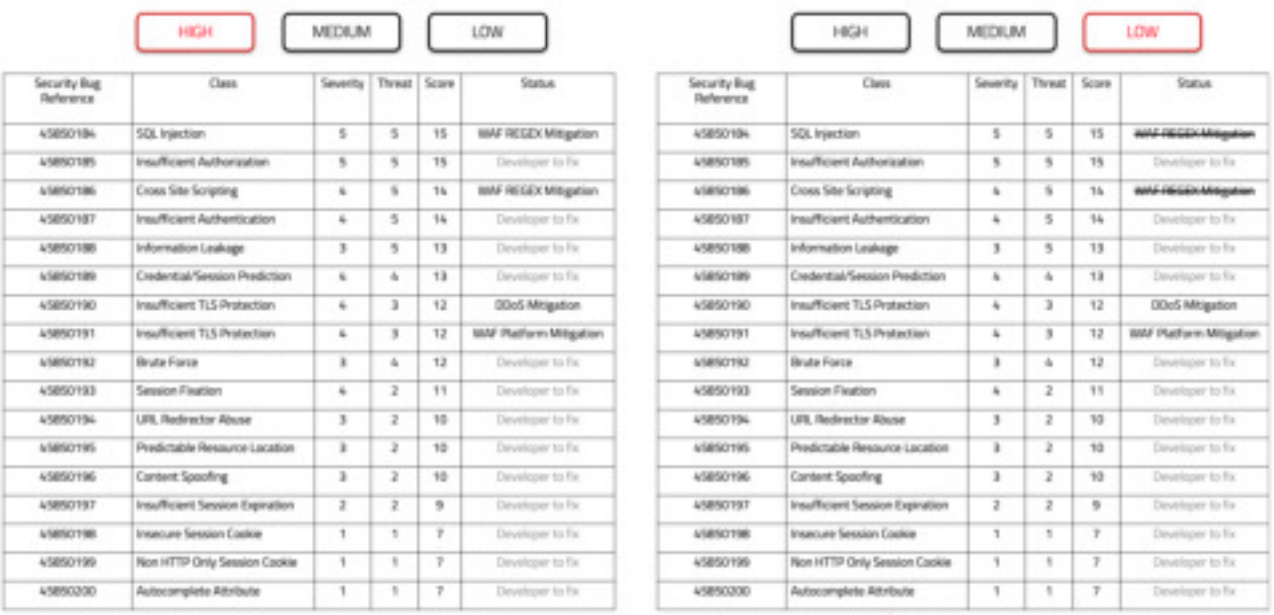
It is not uncommon for false positives to take weeks to resolve and during the interim for the WAF to be removed from blocking mode completely. In these situations, getting the WAF back into blocking mode requires rigorous testing and IT management assurances. In many cases these assurances are never given the WAF deployment scrapped.

Cloud WAF Solution to False Positives

Understanding that there is an imperfect operational environment with non-expert operators, the Cloud WAF suppliers typically offer a *security slider* where predetermined security "levels" can be selected. The underlying continuum of controls that are progressively disabled have been researched and determined by the Cloud WAF security analysts and engineers.

On reporting of a false positive the unskilled customer operator can then reduce the security level until the false positive disappears. In this manner, False Positives are "blind" swapped for False Negatives ("blind" in that the operator is not aware of exactly which risks they are exposing the organisation to).

This approach is in line with the Cloud WAF goal of *assisting* with some application exploit issues. The alternative of having the security control completely removed is considered worse.



Security Bug Reference	Class	Severity	Threat	Score	Status
45850184	SQL Injection	5	5	15	WAF REGEX Mitigation
45850185	Insufficient Authorization	5	5	15	Developer to fix
45850186	Cross Site Scripting	4	5	14	WAF REGEX Mitigation
45850187	Insufficient Authentication	4	5	14	Developer to fix
45850188	Information Leakage	3	5	13	Developer to fix
45850189	Credential/Session Prediction	4	4	13	Developer to fix
45850190	Insufficient TLS Protection	4	3	12	DDoS Mitigation
45850191	Insufficient TLS Protection	4	3	12	WAF Platform Mitigation
45850192	Brute Force	3	4	12	Developer to fix
45850193	Session Fixation	4	2	11	Developer to fix
45850194	URL Redirector Abuse	3	2	10	Developer to fix
45850195	Predictable Resource Location	3	2	10	Developer to fix
45850196	Content Spoofing	3	2	10	Developer to fix
45850197	Insufficient Session Expiration	2	2	9	Developer to fix
45850198	Insecure Session Cookie	1	1	7	Developer to fix
45850199	Non HTTP Only Session Cookie	1	1	7	Developer to fix
45850200	Autocomplete Attribute	1	1	7	Developer to fix

Security Bug Reference	Class	Severity	Threat	Score	Status
45850184	SQL Injection	5	5	15	~~WAF REGEX Mitigation~~
45850185	Insufficient Authorization	5	5	15	Developer to fix
45850186	Cross Site Scripting	4	5	14	~~WAF REGEX Mitigation~~
45850187	Insufficient Authentication	4	5	14	Developer to fix
45850188	Information Leakage	3	5	13	Developer to fix
45850189	Credential/Session Prediction	4	4	13	Developer to fix
45850190	Insufficient TLS Protection	4	3	12	DDoS Mitigation
45850191	Insufficient TLS Protection	4	3	12	WAF Platform Mitigation
45850192	Brute Force	3	4	12	Developer to fix
45850193	Session Fixation	4	2	11	Developer to fix
45850194	URL Redirector Abuse	3	2	10	Developer to fix
45850195	Predictable Resource Location	3	2	10	Developer to fix
45850196	Content Spoofing	3	2	10	Developer to fix
45850197	Insufficient Session Expiration	2	2	9	Developer to fix
45850198	Insecure Session Cookie	1	1	7	Developer to fix
45850199	Non HTTP Only Session Cookie	1	1	7	Developer to fix
45850200	Autocomplete Attribute	1	1	7	Developer to fix

Figure 6 Using Dashboard controls to "blind" swap false positives for false negatives

This approach also exposes the organisation to another threat. As the unskilled operator is proficient in removing controls when requested, a hacker can game the helpdesk by falsely reporting a false positive in an attempt to get their exploits through.

VIRTIS Vi Answer 2: Deploy Application Change Tolerant Policies, with expert monitoring and tuning

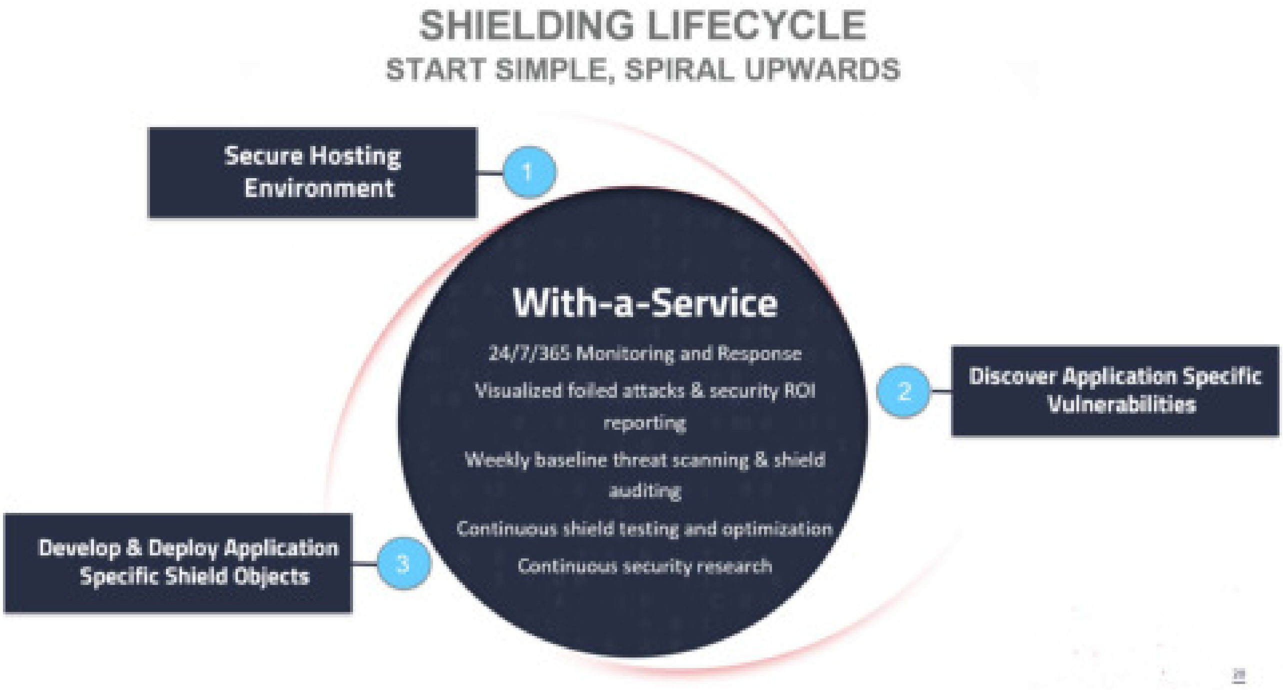

SHIELDING LIFECYCLE
START SIMPLE, SPIRAL UPWARDS
Secure Hosting Environment
1
With-a-Service
24/7/365 Monitoring and Response
Visualized foiled attacks & security ROI reporting
Weekly baseline threat scanning & shield auditing
Continuous shield testing and optimization
Continuous security research
2
Discover Application Specific Vulnerabilities
3
Develop & Deploy Application Specific Shield Objects

Figure 7 The VIRTIS Vi Shielding Process

After observing a large number of failed WAF deployments, VIRTIS Vi's Security Analysts, Engineers, Developers and Researchers have created, and continually enhance, a Base Policy that is designed to offer both:

1) as broad threat protection as possible, and
2) high application change tolerance

This enables VIRTIS Vi to rapidly deploy a highly researched baseline shielding with minimal chance of False Positives both during initial deployment and ongoing operation.

For additional shields that are either:

1) highly application change intolerant, or
2) require significant VIRTIS Vi tuning or custom development

VIRTIS Vi only deploys these when they are required to address specific real application security risks, typically as documented by a Pen Tester.

For avoidance of doubt, VIRTIS Vi *will* allow the threat through if both:

1) The application is not vulnerable to the threat
2) Blocking the threat would make it application change intolerant

The analogy with the medical fraternity is striking. Medication with side effects is only prescribed once a relevant condition is confirmed and the trade-offs considered.

VIRTIS Vi uses the same approach with Vulnerability Intelligence guiding shield deployments.

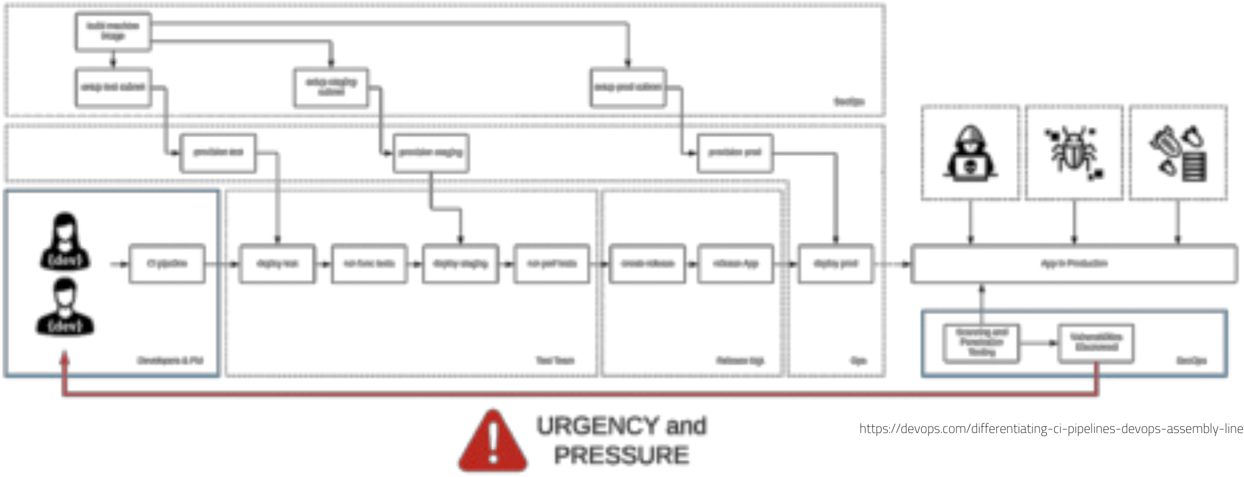
Using this methodology VIRTIS Vi is currently maintaining a False Positive ratio of 0.0002% or 2 False Positives per ‘000,000 blocks, approximately ‘000 times better than current industry best practice.

However, given False Positives can still occur, VIRTIS Vi has a robust process to address them. Expert VIRTIS Vi Security Researchers, Analysts, Engineers and Developers are available 24/7 to assess whether the False Positive claim is legitimate (hackers often attempt to game inexperienced helpdesk operators), technically resolve the issue and assess whether the fix results in incremental security risk to the application. The VIRTIS Vi operator will then follow a pre-determined Customer Change Management process to implement the change.

VIRTIS Vi's average False Positive resolution time is currently <15mins.

Problem 3: WAF's slow Continuous Integration/Continuous Delivery (CI/CD) software development pipelines

As more and more enterprises use technology to transform their businesses, then the need to deploy quality software at speed has become paramount. CI/CD has emerged as a practical methodology to establish a consistent and automated way to build, package, and test applications. Using this (or similar) methodologies has enabled many organizations to reduce weekly release cycles to days or even hours.



https://devops.com/differentiating-ci-pipelines-devops-assembly-lines/

Figure 8 How a typical DevOps assembly line deals with detected security bugs

If security bugs are detected, either during the testing process or post deployment, they either (depending on severity) stop the release or fixes get rolled into the next practical release. For critical bugs that are detected post deployment, the impact of the assembly line can be substantial.

In an environment with this release velocity, adding a device like a WAF, that requires a multi week tuning period before they can enforce security policy, is impractical. In many cases these devices are left in alerting only mode, and in others removed all together.

VIRTIS Vi Answer 3: Deploy Application Change Tolerant Policies Firstly & Provide Transformational Fixes within Hours

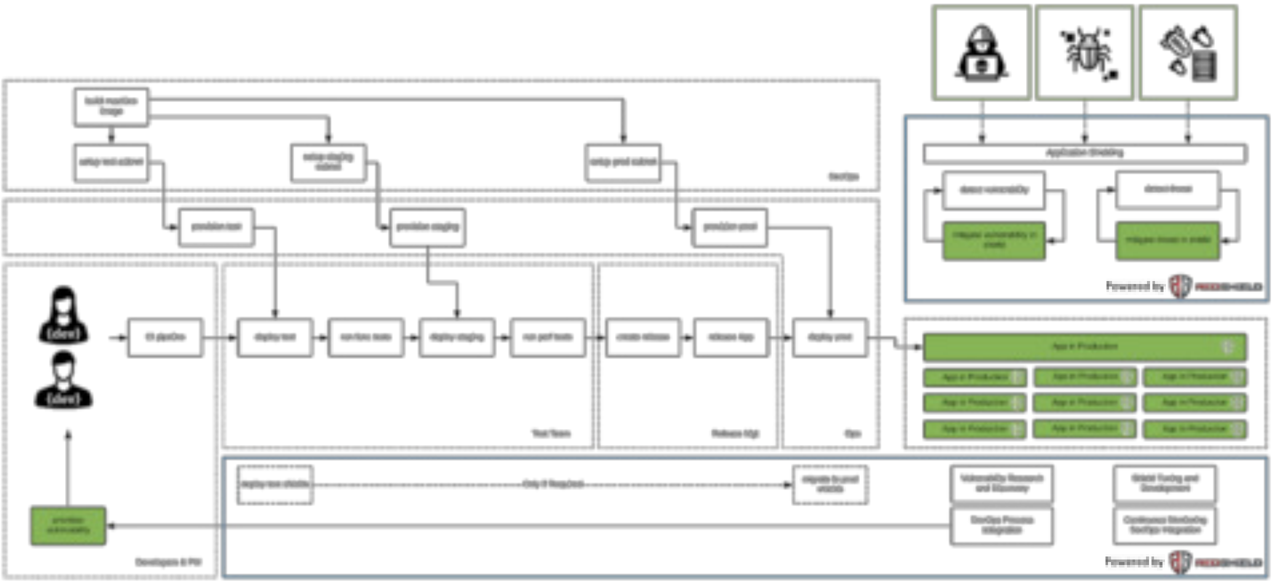


Figure 9 How a typical DevOps assembly line deals with detected security bugs with VIRTIS Vi

With VIRTIS Vi the Application Change Tolerant deployment is key for generic threat protection. Applications can safely change over time without the fear of major disruption. IF any incompatibilities are detected during the assembly line process or post deployment, remedial action occurs swiftly.

More importantly, if new issues are reported via security researchers, VIRTIS Vi can vet the report and provide an immediate shielding option for the development team to consider. Leveraging the existing shield library, transformation shields that require minimal customization are normally available. For any required customization or a unique shield build, VIRTIS Vi's own DevOps team kicks into action, typical delivering within minutes to hours.

Finally, given VIRTIS Vi provides a bolt on DevOps assembly line for security bug fixes, even if your applications don't have their own assembly line, they effectively do with VIRTIS Vi. This includes legacy, third party, highly audited apps that are difficult to modify, especially those obtained through merger and acquisition.

Problem 4: WAFs performance is unmeasured

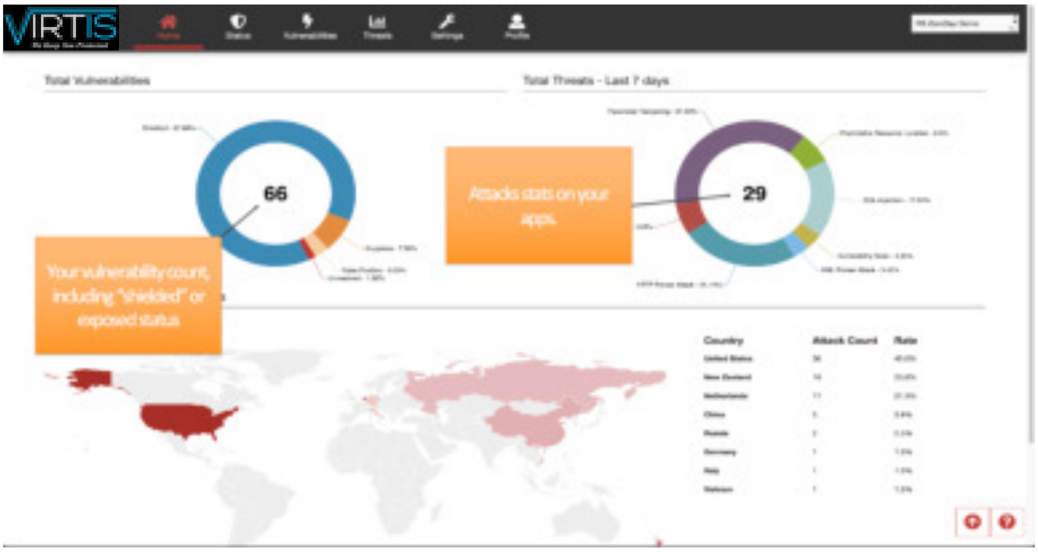
WAFs block threats, and often in very large numbers, however determining whether any of these attacks would have resulted in incidents is very difficult. Therefore, it is not possible to report on the value that the product has delivered. Additionally, if configuration, infrastructure or application software changes are made, either by design or error, there is typical no process to detect and report on the impact.

VIRTIS Vi Answer 4: Continually Audit the deployment and encourage additional security testing

VIRTIS Vi audits customer deployments weekly with unauthenticated Vulnerability Scanning. Deeper issues are audited on a time schedule agreed with the customer.

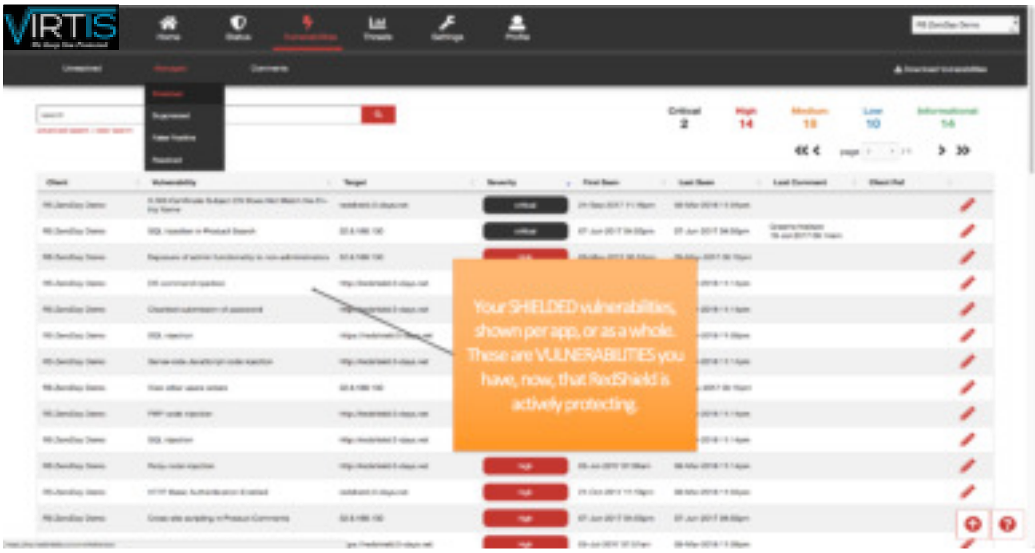
These audits are performed with the Shields up and the with Shields down, hence VIRTIS Vi can quickly assess whether the vulnerability still exists in the application and if it does, is it exploitable through VIRTIS Vi.

This enables VIRTIS Vi to report on which shields are actively protecting from real issues and by correlating attack traffic report on incidents actually saved, a new concept that VIRTIS Vi has patent pending.


VIRTIS
Home
Status
Vulnerabilities
Threats
Settings
Profile
Total Vulnerabilities
Total Threats - Last 7 days
66
29
Attacks stats on your apps.
Your vulnerability count, including "shielded" or exposed status

Country	Attack Count	Rate
United States	34	[illegible]
New Zealand	14	[illegible]
Netherlands	11	[illegible]
China	5	[illegible]
Russia	2	[illegible]
Germany	1	[illegible]
Italy	1	[illegible]
Vietnam	1	[illegible]

Figure 10 VIRTIS Vi Portal summarizing attack and vulnerability status of all applications under management



Your SHIELDED vulnerabilities, shown per app, or as a whole. These are VULNERABILITIES you have, now, that RedShield is actively protecting.

Figure 11 VIRTIS Vi Portal showing vulnerability protection status

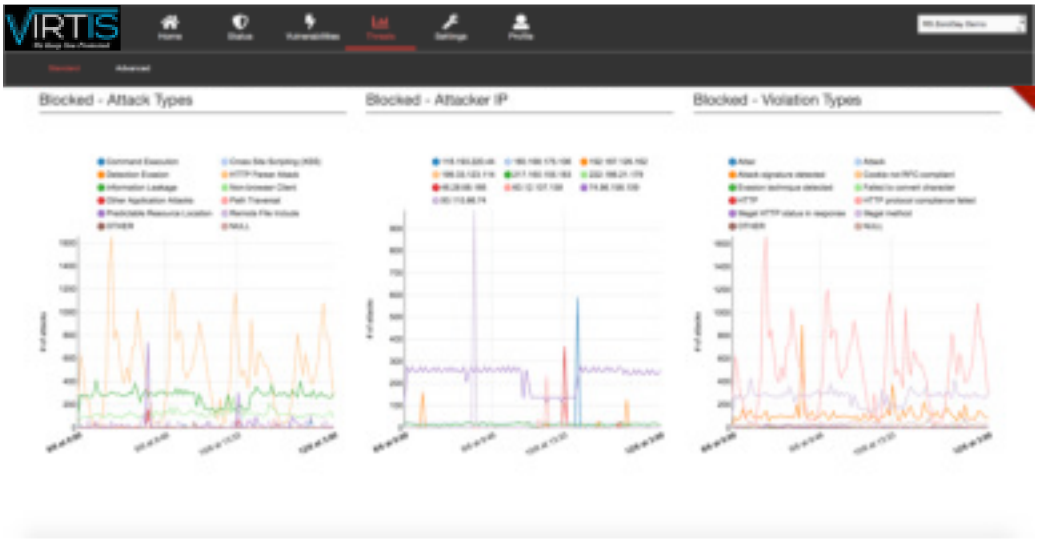


Figure 12 VIRTIS Vi Portal Attack Traffic that has been blocked

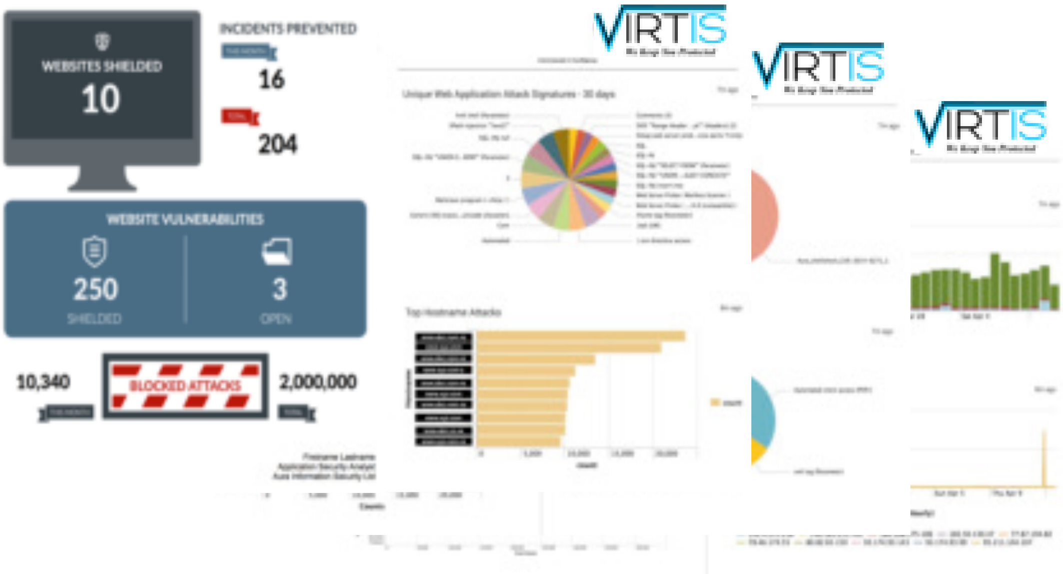


Figure 13 VIRTIS Vi Analyst Commented Reporting including Incident reporting – where attack traffic matches shielded vulnerabilities

Problem 5: The skills and processes required to optimise and operate WAF's are hard to source and impossible to retain

Given the task at hand is to thwart highly skilled adversaries whilst minimising disruption to the normal functioning of a business-critical application, this is not an environment where novices should be deployed to learn the trade via trial and error.

However, with WAF's being specialised tools that require a detailed understanding of networking, applications and security, finding resources with the appropriate skills is difficult. Then retaining them indefinitely is impossible. Given these challenges, requiring these key operators to be on call 24/7, to address incidents in the night, is not something that can realistically requested.

Then, even if the resources can be sourced, the processes to draw them into a team that delivers a consistent measured outcome takes significant time to develop and mature.

Microfocus has studied how SoCs globally have been developing their process maturity with reference to the Carnegie Mellon University CMMI measure (termed SOMM by Microfocus).

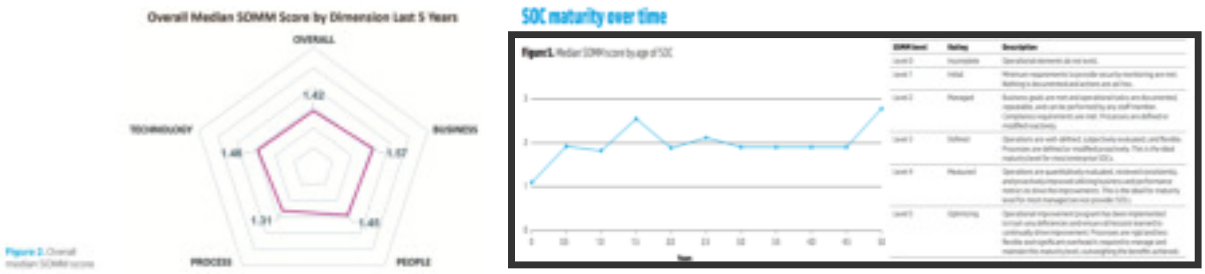


Figure 14 Microfocus' Security Operations Maturity Model Scoring

The results show that it takes organizations on average 5 years (or 10,000hrs) to establish robust processes.

VIRTIS Vi Answer 5: Provide the service as “Do it for me”

With VIRTIS Vi, we provide the skilled and organized resources to supplement our advanced tools and systems. Our Offense and Defense principles each have greater than 20,000 hours in the component technologies. They both have world class knowledge in Scanners, Pen Tests, WAFs, DDoS, Interception Proxies, Software Development, SIEMs, Service Desks and Security Research. They mentor their teams in the finer points of the security deployment and operation plus ensure that the specialist tools and learning systems we develop and deploy are subject matter expertise aware and supervised. To date, we have achieved over 9,000% increase in resource productivity.

The processes that VIRTIS Vi has established are based on SANS best practices in vulnerability management. We are currently executing at a CMMI approach 3.0.

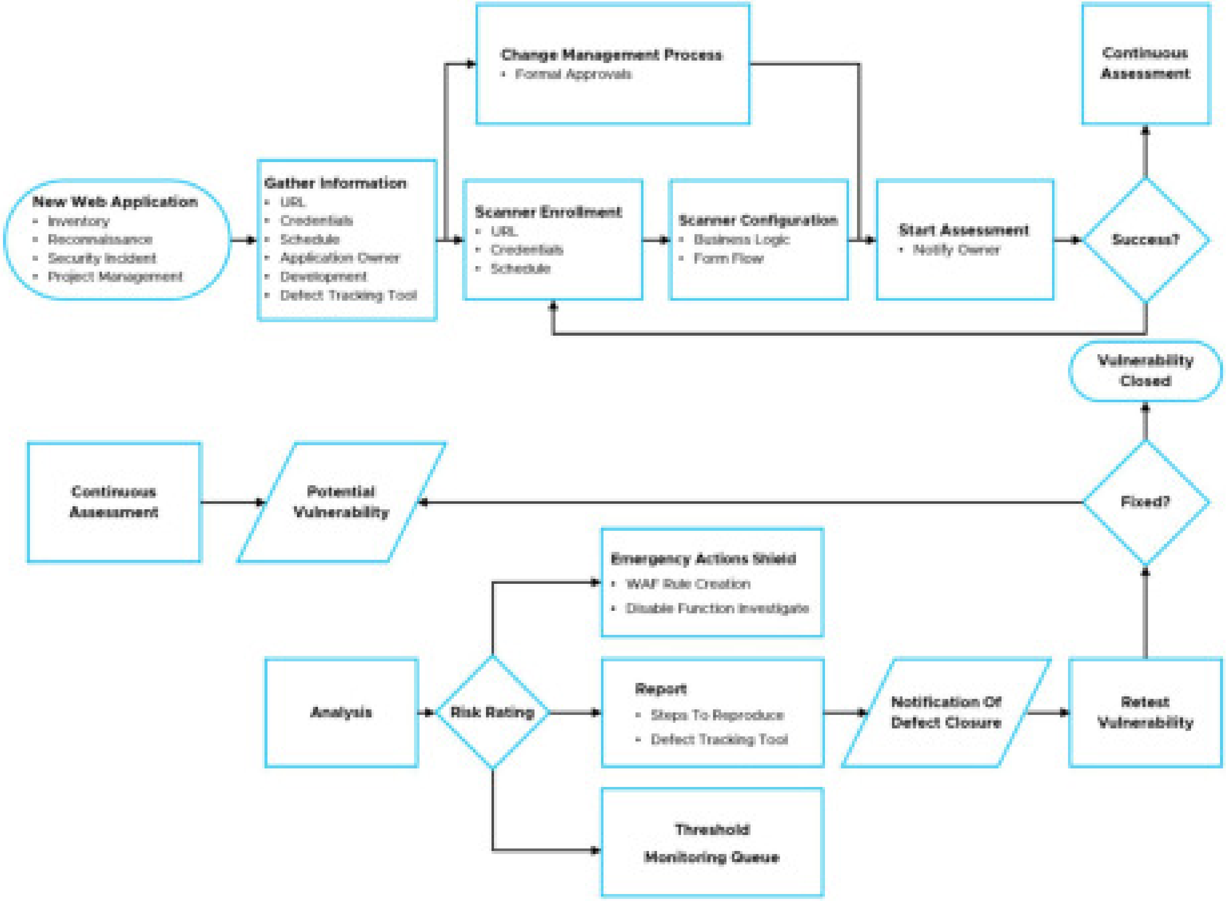


Figure 16 SANS Best Practice in Vulnerability Management

Summary

Equipment Lifecycle Management Comparison

Multiple tools are required within the vulnerability management process, each of these tools need to be lifecycle managed to ensure that they remain state of the art in the fight to secure your environment.

	CLOUD WAF AS-A-SERVICE	VIRTIS EXPRESS AS-A-SERVICE
DDoS	✓	✓
WAF	✓	✓
Interception Proxy (to Host Microservice code objects)	x	✓
Reporting Portal	✓	✓
Equipment Monitoring	✓	✓
Multiple Vulnerability Scanners	x	✓
Vulnerability Management Portal	x	✓
SIEM	Uplift	✓
Service Monitoring	x	✓

Platform Management Comparison

Staying on top of patching, upgrades and support issues both for each component tool and the integrated solution is an important cost consideration.

	CLOUD WAF AS-A-SERVICE	VIRTIS EXPRESS AS-A-SERVICE
Upgrades	✓	✓
Patch Management	✓	✓
Vendor Support Calls	✓	✓
Integration	✓	✓

Shielding Technology Comparison

The bad guys just need one hole to get in; you need a broad range of defenses to keep them at bay.

	CLOUD WAF AS-A-SERVICE	VIRTIS Vi EXPRESS AS-A-SERVICE
Vol. DDoS up to 1Gbps/2Tbps	✓ /Uplift	✓
Generic Asymmetric DoS/Advanced	✓ /Uplift	✓ /Enterprise
Protocol hardening & fair use policy enforcement	✓	✓
Generic WAF Signature filtering/Advanced & Custom	✓ /Uplift	✓ /Enterprise
Advanced WAF evasion & bypass defense	x[1]	✓
Bot Defense/Advanced	Uplift	✓ /Enterprise or Worker
REQ/RES Rewrite	x	Enterprise
Microservice application logic transformation	x	Worker

[1] Evasion & bypass defense varies between Cloud WAF providers. Some have defenses, most don't. New attack techniques & defenses are being continually developed that must be dynamically addressed.

VIRTIS
We Keep You Protected

Vulnerability Management Comparison

Against an infinite landscape of threats, finding your issues, understanding short- and long-term options and acting is key to an effective vulnerability management program.

	CLOUD WAF AS-A-SERVICE	VIRTIS Vi EXPRESS AS-A-SERVICE
Weekly operation of vulnerability scanners	x	✓
Import of 3rd party vulnerability data (other vulnerability scanners, code scanners, vulnerability intel feeds, pen tests, bug bounties)	x	✓
Expert verification/false positive management of detected vulnerabilities	x	✓
24/7 monitoring of NVD and other vulnerability & threat intelligence feeds plus deployment of vendor/VIRTIS Vi custom shields	x	✓
Expert vulnerability analysis & risk scoring	x	✓
Determination of remediation and mitigation options, with expert recommendation	x	✓
Vulnerability incident detection & customer specific response procedures	x	✓
Expert knowledge base with analyst helpdesk for vulnerability & treatment options decision making	x	✓
Workflow management of customer risk treatment decisions (disable, accept, fix in software, shield), communicated in the portal	x	✓

Shielding Deployment Comparison

Expertly deploying then continually enhancing, tuning and testing your shields is what is required. VIRTIS Vi believes that basic security controls and part time teams are not enough. The bad guys are evolving fast, and your security operation must run faster.

	CLOUD WAF AS-A-SERVICE	VIRTIS Vi EXPRESS AS-A-SERVICE
Dashboard driven WAF rule selection	✓	x^2
Expert driven WAF rule selection	Uplift	✓
Vulnerability lead WAF rule selection	x	✓
REQ/RES rewrite selection and customization	x	Enterprise
Worker selection, custom development and/or customization	x	Worker
Customer Specific Change management lead deployment for any Adds/Moves/Changes	x	✓
Expert deployment Audit	x	✓
24/7 security analyst, engineer, researcher & developer helpdesk for emergency shield creation and deployment	x	✓

VIRTIS
We Keep You Protected

Operation and Assurance Comparison

Using the tools, auditing and expertly responding to information that they are providing is the point of these tools within a vulnerability management and security operations team

	CLOUD WAF AS-A-SERVICE	VIRTIS Vi EXPRESS AS-A-SERVICE
24/7 equipment monitoring	✓	✓
Incident Response	Uplift	✓
Weekly shield audit	x	✓
24/7 service and security alert monitoring	x	✓
Incident detection	x	✓
Customer Specific Incident Response	x	✓
Multi-layered service availability monitoring	x	✓
Current false positive rate	0.2%-0.02%	<0.0001%
Current false positive resolution method	Security slider with blind risk acceptance	Security expert tuned & audit
Current false positive resolution time	Undetermined	<15mins

Reporting Comparison

Understanding your risks requires a clear understanding of the status of your issues and proposed defenses as well as trends in attack. Additionally, to understand the Return on Investment on your security operations, clearly being able to see when these defenses stopped an attack that would have been successful is important.

	CLOUD WAF AS-A-SERVICE	VIRTIS Vi EXPRESS AS-A-SERVICE
Attack traffic	✓	✓
Traffic Volumes	✓	✓
SIEM data and search	Uplift	✓
Unresolved Vulnerabilities	x	✓
Shielded Vulnerabilities	x	✓
Resolved Vulnerabilities	x	✓
Suppressed Vulnerabilities	x	✓
Shield activation (attack matches vulnerability)	x	✓
Expert analyst commented monthly log review	x	✓
Expert analyst commented monthly log monthly reporting	x	✓
Forensic Analysis	Uplift	Uplift

VIRTIS
We Keep You Protected