

10 Key Capabilities of Signal Sciences Next-gen WAF and RASP

A look at specific areas that prove Signal Sciences is the web application security technology of choice for modern software teams.

As the application development landscape evolves with faster feature release cycles and the adoption of new and modern languages and cloud platforms, software teams are struggling to secure their rapidly growing web attack surface.

Signal Sciences next-gen WAF and RASP technology is [designed to work quickly and effectively](#), enabling application developers and operations teams to deliver modern, business-critical web applications and APIs that are well protected and running performantly.

There are many vendors claiming to provide effective and scalable offerings to protect applications and APIs, so we want to dig into exactly what makes Signal Sciences the next-gen WAF and RASP technology of choice.

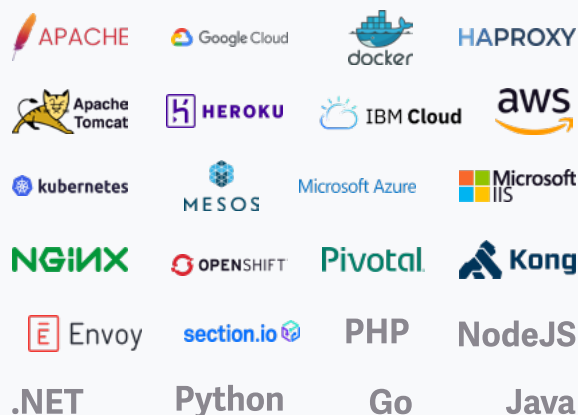
THE 10 KEY CAPABILITIES OF SIGNAL SCIENCES

1. Flexible Deployment Options for Any Architecture
2. Installs Easily Behind Existing Edge Security Tools
3. Protects Your Apps Without Breaking Them
4. Identifies and Blocks Bots and Scrapers
5. Guides Engineers to Fix the Right Things
6. Brings Dev and Ops to the Security Party
7. Defends Mobile Apps
8. Addresses Vulnerabilities with Virtual Patching
9. Provides Operations with Data
10. Automated Blocking that Scales

1. Flexible Deployment Options for Any Architecture—Now and in the Future

Modern software teams deploy applications everywhere: in containers, on multi- and hybrid clouds, load balanced across multiple CDNs, and everything in between. Whether you're using Amazon Web Services (AWS), Microsoft Azure, Google Cloud, some combination, or something altogether different, with Signal Sciences you gain visibility and protection wherever your apps, APIs, and microservices live—and in whatever language they're written. Additionally, to protect legacy applications, Signal Sciences can operate as a reverse proxy. Providing the widest range of installation options in the industry and a single control pane to monitor all your apps, Signal Sciences is a foundational piece of a future-proof strategy that supports your architecture today in addition to where and how you choose to run your apps in the future.

Supported Platforms



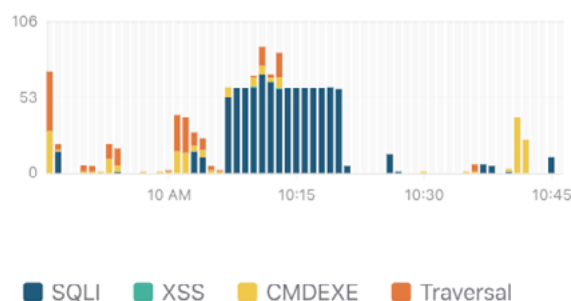
Legacy Apps Supported via Reverse Proxy, e.g.

ASP Perl Scala ColdFusion

2. Installs Easily Behind Existing Edge Security Tools to Catch Missed or Unknown Attacks

Your organization may have made a substantial investment in a CDN or appliance-based WAF, and that's not uncommon. Putting a WAF at the [network edge](#) makes sense to many operations engineers since that's where cached content is utilized to remove the load from web and application servers. It also allows

OWASP Injection Attacks



Signal Sciences can augment existing WAF investments and identify and block unique threats while providing protection against the OWASP Top 10 and beyond.

engineers to check the “compliance” box for security audits. But in practice, customers have requested more specific application-level attack and behavior detail than what these products were designed to provide.

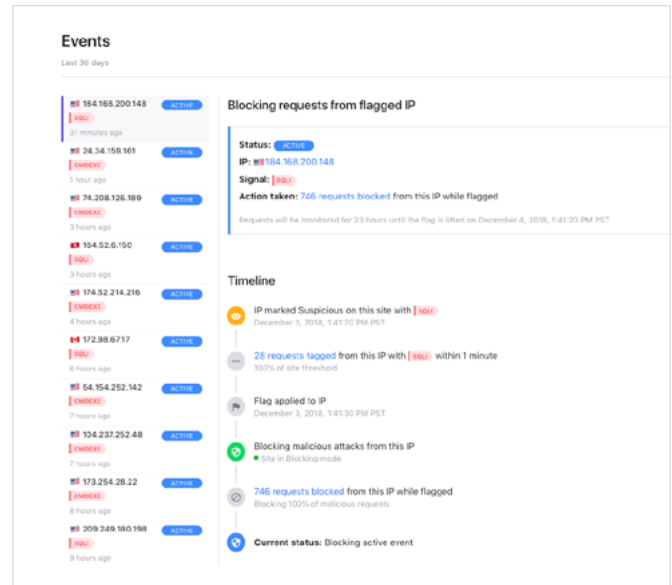
Signal Sciences can install behind these existing technologies to augment existing WAF investments by identifying and blocking unique threats they cannot. With Signal Sciences, you can instrument critical business logic flows to alert if exploit attempts are made against them. Gaining this level of coverage requires instrumentation at the application layer, not at the edge. This method also safely provides a feedback loop to developers and engineers without requiring everyone in the engineering team to have direct access to the CDN or [WAF appliance](#).

3. Protects Your Apps Without Breaking Them

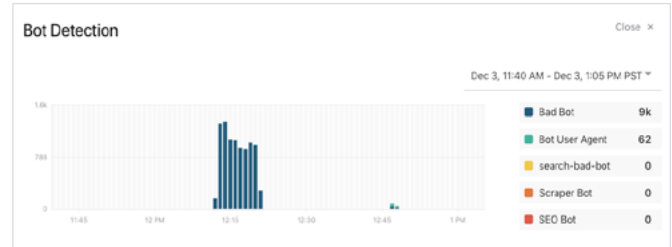
Signal Sciences takes a threshold approach to blocking so you can run our solution in full, automated blocking mode in production with virtually no false positives: 95 percent of our customers trust us to do just that. With threshold blocking, we don't make a decision on each request like other legacy WAFs and RASP products, but we instead look at suspicious payloads over time and with context to determine whether an actual attack is occurring. Our patented approach analyzes over 200 billion weekly production requests with no noticeable performance impact on the applications and APIs we help our customers protect.

4. Identifies and Blocks Bots and Scrapers to Protect Your Resources

Attackers use automation and botnets to acquire valuable data, especially from content rich sites in the media, e-commerce, and technology businesses. With Power Rules, you can enable thresholding rules around abusive behavior such as content scraping and eliminate serving up content and resources to malicious users, potentially saving on infrastructure costs. With thresholding rules enabled, you can block high-volume, malicious requests without a single false positive. You can use the same threshold-based approach to prevent malicious automated attacks via bots deployed to perpetrate application DDoS and account takeovers. Lastly, you can also utilize whitelisting and blacklisting for known good and bad sources to allow or deny requests as necessary, reducing noise in your environment.



A 30-Day Events report summarizes attacks blocked (left column) and the volume of malicious requests blocked from a flagged IP address (upper right). Our Timeline view shows why the IP was flagged as malicious as well as current status (active or past event).



With rate-limiting rules enabled, Signal Sciences blocks high-volume malicious bot requests.

5. Guides Engineers to Fix the Right Things

Engineers never have a shortage of bugs to fix, but the challenge is understanding which ones to prioritize. Signal Sciences provides clear reports on the most common attack types and targets to help your teams focus on what exactly is under attack. Engineering and security managers use this real-time data to best utilize their resources, including what types of training needs to be reinforced depending on the attack tactics used against their apps and APIs in production. Developers and security engineers are able to self-service data to get a better understanding of the bigger picture of attacks against their code.

6. Brings Dev and Ops to the Security Party with Actionable Data

Security cannot be an afterthought. Aligning security, dev, and ops teams is crucial for all three groups to understand the requirements of security in the development lifecycle before issues arise that impact you and your bottom line. Signal Sciences shows all stakeholders how requests are impacting their app or service and provides the self-service data to prove it. Data around application attacks, anomalies, and behavior is available via customizable dashboards and APIs, along with the toolchain products your teams are already using. Teams can easily create alerts when critical thresholds are triggered, sending messages through to the systems they use. Examples of how we enrich your current toolset include:

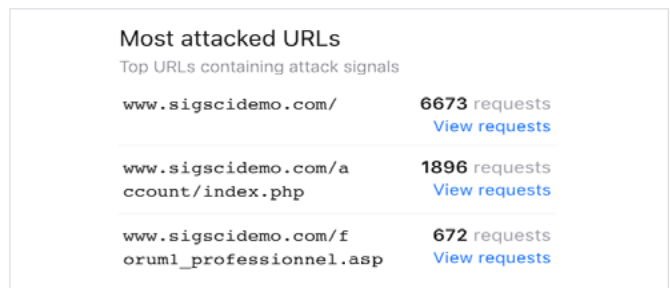
- **SIEM integrations** into Splunk, ArcSight, Sumo Logic, and others with fully documented REST/JSON APIs
- **Webhooks to common DevOps tools** like Slack, PagerDuty, Datadog, and Jira provide full event details of alerts



The screenshot shows the 'Overview' page for a specific site. It displays a table with columns: Site, Attack requests, Attack types, Attack sources, and Flagged IPs. The 'Attack requests' column shows 129,246 blocked requests (+16.89%) and 145,358 total requests (+17.57%). The 'Attack types' column lists SQLi (31%), Traversal (26%), and CMDexe (25%). The 'Attack sources' column shows 78% from a specific source, 5% from another, and 3% from a third. The 'Flagged IPs' column shows 136 flagged IPs.

Sites	Attack requests	Attack types	Attack sources	Flagged IPs
Nov 22, 2018 - Dec 4, 2018	129,246 blocked (+16.89%) 145,358 requests (+17.57%)	31% SQLi 26% Traversal 25% CMDexe	78% 5% 3%	136 flagged IPs

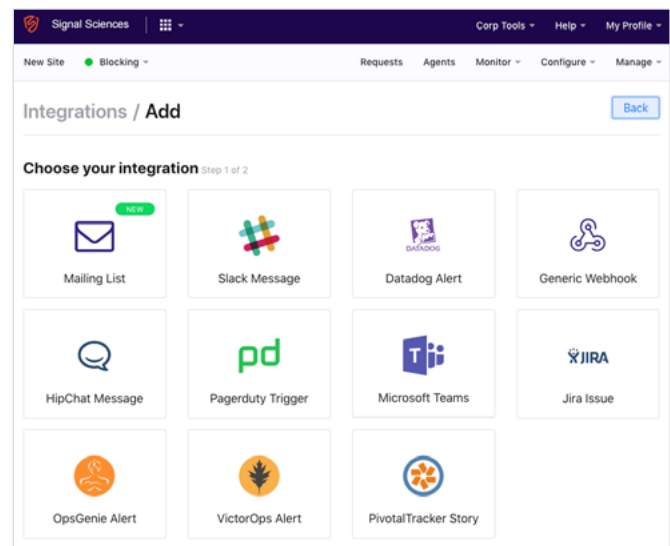
An example overview report shows the volume, types and sources for attacks against a single site: this key information helps your team focus their resources.



The screenshot shows the 'Most attacked URLs' section. It lists the top URLs containing attack signals. The first URL is www.sigscidemo.com/ with 6673 requests. The second URL is www.sigscidemo.com/account/index.php with 1896 requests. The third URL is www.sigscidemo.com/forum1_professionnel.asp with 672 requests.

Most attacked URLs	Top URLs containing attack signals
www.sigscidemo.com/	6673 requests View requests
www.sigscidemo.com/account/index.php	1896 requests View requests
www.sigscidemo.com/forum1_professionnel.asp	672 requests View requests

Example of specific URLs receiving the most malicious requests. Your team can get more context by drilling down to a "Requests" report for each attacked URL.



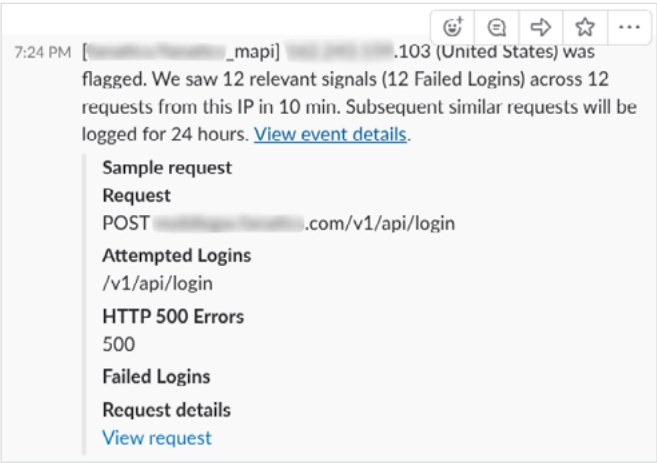
Data that Signal Sciences surfaces can be utilized to create alerts broadcast via several devops tools.

7. Defends Mobile Apps with the Same Powerful Capabilities

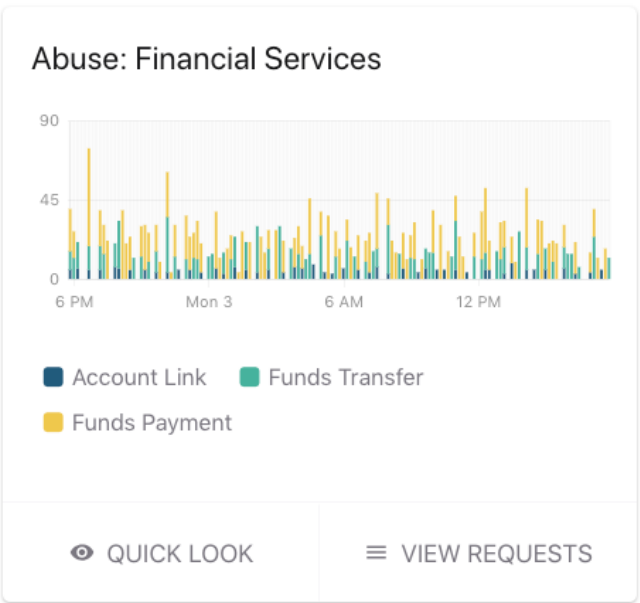
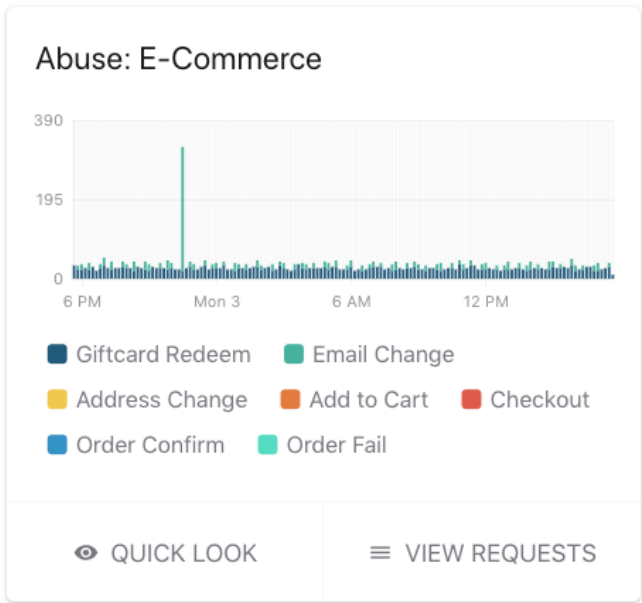
Signal Sciences provides the broadest coverage against real threats and attack scenarios across any modern architecture, including the mobile apps that empower your customers to access your products and services anywhere. As mobile applications rely on APIs to transfer critical data from application servers, Signal Sciences provides you with visibility by installing after the traffic is decrypted at the web server or code layer. Without performance impact, you can leverage Signal Sciences to optimize and secure your mobile app experiences.

Through Power Rules, you can monitor any business logic that is unique to your mobile application. For example, you can view the number of transactions per minute, checkouts per hour, discount codes used, and so on. With added visibility that doesn't impact the performance and user experience of your mobile app, your teams can gain insight into particular use and abuse patterns that were formerly difficult to find, buried in log data.

Signal Sciences also defends the authentication flows in any mobile app by detecting and blocking requests from known bad IPs that abuse authentication events like account creation, password reset, or other brute force or account takeover attempts. And because Signal Sciences is able to block with virtually zero false positives, legitimate users will not be denied access to your mobile app—so your business continues uninterrupted.



Example alert from Signal Sciences sent to Slack that highlights a dozen failed logins from the same IP address.

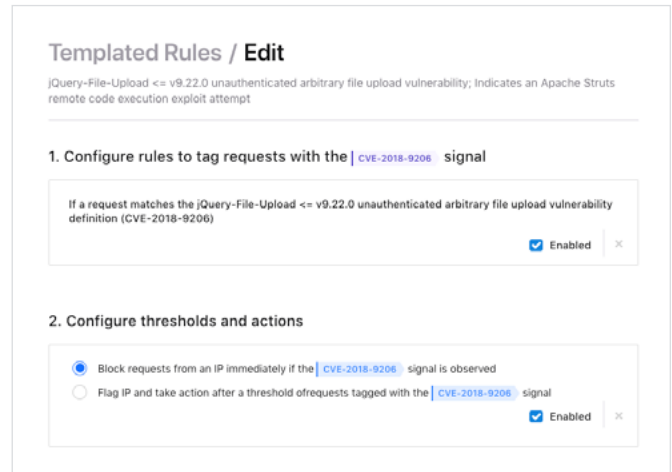


With Signal Sciences you can monitor key application events in your apps and mobile APIs for potential misuse and abuse.

8. Addresses Vulnerabilities with Virtual Patching

Software creates new vulnerabilities that attract attackers who unleash payloads to exploit the weaknesses. Because the vulnerability-to-exploit cycle occurs in hours, you need proactive defense against attacks to buy time while fixing the underlying systems. This is exactly what Signal Sciences provides through virtual patching enabled by Power Rules: you can apply virtual patches that address various Common Vulnerability and Exposures (CVEs) and immediately block requests containing the CVE exploit. Within the console, customers can use templated Power Rules that cover various CVEs in a default list.

The example above right displays a Power Rule that applies a virtual patch to address CVE-2018-9206 in which attackers can exploit older versions of the jQuery File Upload package to carry out several malicious activities, including data exfiltration and malware infection.



Templated Rules / Edit

jQuery-File-Upload <= v9.22.0 unauthenticated arbitrary file upload vulnerability; Indicates an Apache Struts remote code execution exploit attempt

1. Configure rules to tag requests with the **CVE-2018-9206** signal

If a request matches the jQuery-File-Upload <= v9.22.0 unauthenticated arbitrary file upload vulnerability definition (CVE-2018-9206)

☒ Enabled

2. Configure thresholds and actions

☒ Block requests from an IP immediately if the **CVE-2018-9206** signal is observed

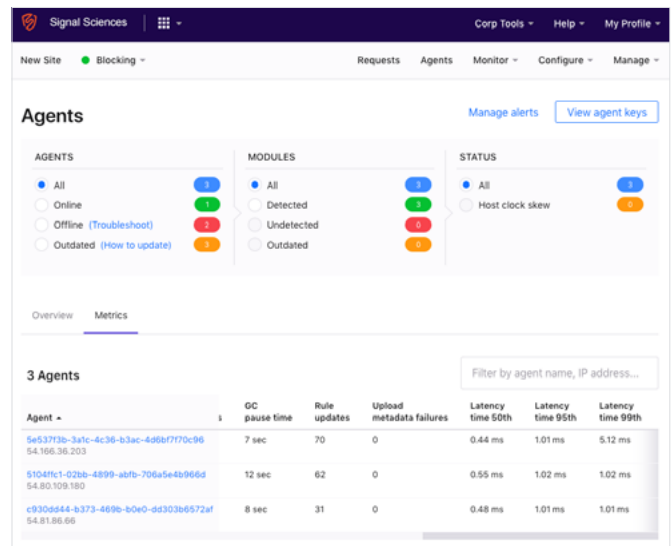
☐ Flag IP and take action after a threshold of requests tagged with the **CVE-2018-9206** signal

☒ Enabled

In this example templated Power Rule, Signal Sciences will apply a virtual patch that will block requests that attempt to leverage CVE-2018-9206, a vulnerability that can lead to remote code execution.

9. Provides Operations with Data to Ensure Site Uptime and Performance

Signal Sciences patented module-agent [architecture](#) fails open and connects asynchronously with Cloud Engine, our powerful cloud-hosted analytics backend. Net result? Your applications' uptime, availability, and communication function as if we weren't even there. We built our agent to expose metrics that operations teams rely on, from CPU and memory usage to how much delay the agent adds to each request (no more than one to three milliseconds). We also built our API so these metrics pull into the systems your operations teams already use. Other WAF and RASP vendors don't have APIs for these metrics and provide little detail in their UI, and only a few document 2X latency on the roundtrip from request to decision.



Signal Sciences

Agents

3 Agents

Agent	GC pause time	Rule updates	Upload metadata failures	Latency time 50th	Latency time 95th	Latency time 99th
5e5373b-3afc-4c36-b3ac-496b7770c96 54.166.36.203	7 sec	70	0	0.44 ms	1.01 ms	5.12 ms
51048c1-02b6-4899-abfb-706a5e4b966d 54.80.109.189	12 sec	62	0	0.55 ms	1.02 ms	1.02 ms
c930d844-b373-4696-b0e0-d4303b6572af 54.81.86.66	8 sec	31	0	0.48 ms	1.01 ms	1.01 ms

Agent health and KPIs, such as latency, can be easily monitored within the Signal Sciences Console.

In addition, Signal Sciences can surface metrics that are meaningful to operations teams—things like client-side and server-side errors, large response times, sizes, errors, even broken links in the code. These data points can point to critical issues either in your application's business logic or server configuration and helps teams triage issues faster.

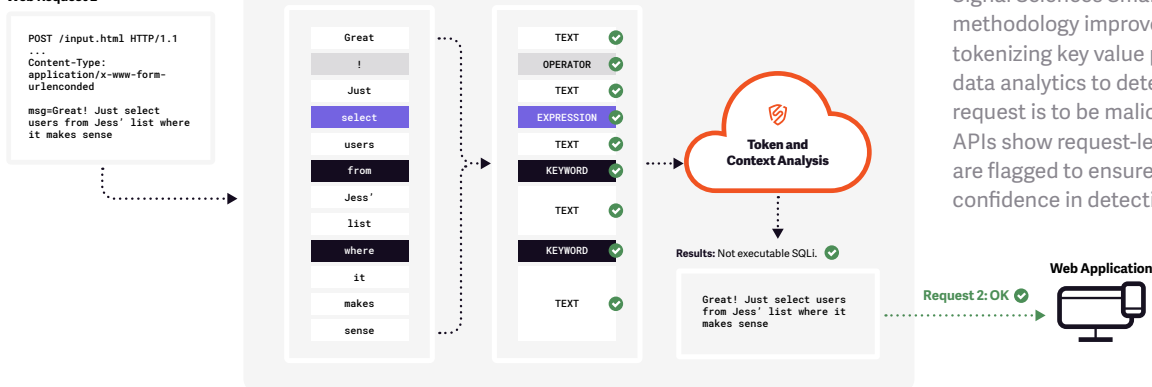
10. Automated Blocking That Scales Without Rules Tuning

Let's be frank about the effectiveness of legacy WAFs within the context of multi-cloud and rapid development cycles and releases: they don't stand a chance. With legacy WAFs, which require learning mode and constant signature tuning to rule out false positives, the aggressiveness of blocking rules gets tuned down or completely turned off for fear of breaking the application. We're able to do this with SmartParse, our proprietary detection method designed to make instantaneous decisions in line to determine if there are malicious or anomalous payloads present in requests. By evaluating the context of the request and how it would actually execute, SmartParse makes highly accurate detections. Designed to run at scale—currently processing over 200 billion weekly production requests—our detection approach requires no tuning or configuration, and virtually eliminates false positives so you can scale protection without dealing with the maintenance overhead that legacy WAFs require.



A "Response Anomalies" chart is an example of how Signal Sciences provides visibility into operational data points like anomalies and application behavior that comes enabled right out of the box.

Web Request 2



Signal Sciences SmartParse detection methodology improves accuracy by tokenizing key value pairs and using big data analytics to determine how likely the request is to be malicious. Dashboards and APIs show request-level details when IPs are flagged to ensure transparency and confidence in detections and decisions.

The AppSec Solution for Modern Development Teams

These key capabilities are essential to ensuring that a web application security solution meets the needs of modern development, operations, and security teams looking to iterate and release software quickly and securely. Signal Sciences has deployment options that are both easy to install and provide complete coverage.