Sourcefire Application Control saves money, improves security and minimizes legal liability by controlling applications that introduce vulnerabilities, evade existing protections, expose sensitive information, overuse bandwidth or violate usage policy. In addition, optional URL Filtering allows organizations to apply category- and reputation-based web site filtering to enforce acceptable use policies and reduce risks of exploit or infection.

MANAGE RISKS WITH APPLICATION CONTROL

As employees feel more empowered than ever to use any application they feel will help them do their job, organizations need to strike a balance between encouraging productivity and minimizing risks. Whether deployed as a Next-Generation IPS (NGIPS) or as a Next-Generation Firewall (NGFW), Sourcefire Application Control provides this balance and gives you several advantages over traditional firewall and IPS policies alone, including:

Reduced attack surface and inspection requirements
By limiting the number and types of applications that are allowed to function on the network, administrators can reduce the number of vectors that attackers could use to access sensitive information, and can block advanced malware attempting to communicate covertly.

Control port- and protocol-hopping apps that evade traditional firewalls
While traditional firewall policies enforce policy based on the IP address, port or protocol alone, Sourcefire Application Control identifies each application and allows or blocks it on a per user or user group basis. Limit exposure to peer-to-peer file sharing, gaming, collaboration, video streaming, chat and other risky or non-productive applications that often evade traditional firewall protections.

Enforcement of mobile application policy to reduce BYOD risk
In a Bring-Your-Own-Device (BYOD) world, you can’t control the endpoint. So it makes sense to control what the endpoint can do at the network level. Sourcefire Application Control can help you identify mobile devices and the applications they use, so you can limit their access to sensitive portions of the network.

Limit the exposure created by social media applications
Similar to the BYOD challenge, administrators have little control over what information is shared or emailed through social media sites. Sourcefire Application Control allows you to limit who does what (by user, user group, network, zone, etc.) with social media applications.
Granular control over applications, bandwidth, and acceptable use policies

Sourcefire classifies applications by type, category, risk level and business relevance, so that you can easily identify the types of applications that pose a risk or are wasting network and human resources. Then granularly apply controls to allow, monitor or block access by specific users, groups or network resources. You can set separate rules within a policy to take different actions for different traffic.

Optional URL filtering of over 280 million domains

This optional subscription service allows you to apply category and reputation-based web content filtering policies. Over 280 million URLs are categorized into 80+ categories and are updated daily.

A refined interface to make policy changes in seconds

Sourcefire Application Control policy is facilitated by an easy to use, drag and drop, single management page within the Defense Center that allows administrators to make additions or changes to their policies with just a few clicks.

ULTIMATE DEPLOYMENT FLEXIBILITY

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Active Control</th>
<th>Passive Alerting</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGIDS out of band behind firewall</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>NGIPS inline behind firewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NGFW deployed as firewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Sourcefire Application Control can be deployed in several ways for ultimate flexibility:

- As a NGIDS – An out of band, layer 2 detection point with passive alerting of application usage
- As a NGIPS – An inline, layer 2 enforcement point with active enforcement of application policy
- As a NGFW – An inline, layer 3 enforcement point with active enforcement of application policy
This affords the flexibility to deploy application detection and control as your requirements dictate, without the need to introduce new hardware, detection or management points within the network.

THE WORLD’S MOST EFFECTIVE THREAT PREVENTION

Sourcefire offers the best network protection that money can buy—period. Sourcefire is the leader in NSS Lab’s Security Value Map for IPS based on security effectiveness and total cost of ownership. As the creator of Snort®, the de facto standard for intrusion detection and prevention, our roots are in security. Our FirePOWER™ Appliance lineup achieves unprecedented throughput performance, cost-effectiveness and scale. Sourcefire FireSIGHT® increases accuracy and automation by using contextual awareness to understand the composition of your network. This agile engine automatically tunes itself to protect new assets as they enter the network, reducing administrative burden and staying one step ahead of malicious hackers.

ADDED PROTECTION WITH URL FILTERING

With Sourcefire Application Control you can take contextual awareness to the next level by adding an optional URL Filtering subscription. Mitigate sophisticated client-side attacks—and improve employee productivity—by controlling access to more than 280 million URLs in over 80 categories.

URL filtering has been architected as a hybrid solution. Over 280M URLs are tracked in the cloud. To speed performance, a subset of the complete dataset, roughly 20 million URLs, is downloaded to the Defense Center and in turn distributed to appliances that are licensed to perform URL Filtering. This smaller subset covers >90% of the most commonly visited URLs. Customers have the option to query the cloud dataset to add URLs not included in the 20M dataset.

When an end user attempts to connect to a URL that is not permitted, the browser is redirected to a custom web page indicating that the user has been blocked from visiting a particular URL.

PROTECTION FOR VIRTUAL ENVIRONMENTS

Sourcefire offers Application Control and URL Filtering solutions for VMware 64-bit virtual platforms. Sourcefire Virtual Appliances provide the capability to inspect VM-to-VM communications, providing the same control and protection as their physical counterparts.

KEY INTERNET STATISTICS

- Active sites: 193 million¹
- Global users: 2.2 billion²
- IP Addresses: 3.8 billion³
- Average number of new web pages each day: over 1 billion⁴

¹ Netcraft Web Server Survey
² www.internetworldstats.com
³ www.domaintools.com
⁴ Official Google Blog, googleblog.blogspot.com
## SPECIFICATIONS

### Application Control
- >1200 applications detected (visit [sourcefire.com/app-center](https://sourcefire.com/app-center) for a complete directory of currently supported applications)
- Applications classified by Risk and Business Relevance
- Access actions for application traffic:
  - Allow (pass but inspect traffic)
  - Trust (pass with no further inspection)
  - Monitor (log traffic connection event)
  - Block (block with no further inspection)
  - Block with Reset (block and reset connection)
  - Interactive Block (pass traffic to HTTP customizable response page to either block or to warn or allow user to accept liability before proceeding to allow connection)
- Supported platforms: all FirePOWER™ 7000 and 8000 Series Appliances
- Prerequisites: requires 5.1 or greater, Control License or NGFW Edition, DC with FireSIGHT™, Virtual – VMware 64-bit
- Update frequency: approximately weekly

### URL Filtering Subscription
- >280 Million Top Level Domains
- 82 granular categories
- 43 languages
- Sophisticated website reputation scoring with high classification accuracy
- Customizable interactive HTTP response page for designated or blocked sites
- Prerequisites: requires 5.1 or greater, Control License or NGFW Edition, DC with FireSIGHT
- Update frequency: continuously for cloud URL database, approximately daily download to DC for localized URL list.

## TAKE THE NEXT STEPS TOWARD AGILE SECURITY

To learn more about Sourcefire Application Control and URL Filtering and other solutions that provide Agile Security®, contact a member of the Sourcefire Global Security Alliance™ today to view a demonstration, request an onsite evaluation, or schedule a meeting, or visit us [www.sourcefire.com](http://www.sourcefire.com) for more information.