SOURCEFIRE FIRESIGHT™: CONTEXT-AWARE AND ADAPTIVE SECURITY

"Context-aware and adaptive security will be the only way to securely support the dynamic business and IT infrastructures emerging during the next 10 years.[1]"

Neil MacDonald, Gartner

INTRODUCTION

Sourcefire FireSIGHT™ is innovative contextual awareness and automation technology that reduces operating costs while allowing network security to keep pace and be effective against dynamic forces. FireSIGHT technology:

- Provides comprehensive visibility into the network—including hosts and other devices, applications, services, and more—–and continually monitors how it's changing over time.
- Automatically assesses new threats to determine which are relevant and business-impacting, helping to focus response efforts and adapt defenses to quickly address changing conditions.
- Enables the automation of critical security activities such as policy tuning, saving time and effort, while ensuring protections and countermeasures are maintained in an optimal state.

Sourcefire FireSIGHT technology achieves security agility by providing an essential "closed loop" between attack or change detection, incident analysis, and response.

By providing a comprehensive and detailed view into the network, FireSIGHT technology makes security analysis more effective and security staff more productive. FireSIGHT eliminates the need to consult multiple disparate management systems to glean the data required to assess and respond to security events.

By compiling and maintaining a detailed baseline of the network and its resources, FireSIGHT can automatically determine which attacks pose the greatest risk. Without burdening staff, this automated assessment and prioritization process focuses analysts' attention on areas where incident response and mitigation efforts are most impactful.

Rapid access to the discovery data provided by FireSIGHT pays dividends during attacks and incidents as well, when a quick and informed response is essential. Access to information extends beyond network resources, providing identifying links between individuals and security incidents.

Forming the foundation of Sourcefire's Agile Security™ vision, FireSIGHT awareness and automation technology supports the ability to See, Learn, Adapt, and Act–reducing the cost and improving the effectiveness of network security.

This paper explores the challenges with delivering effective security today, why traditional static approaches fail to provide the protection we need, and how FireSIGHT technology can provide the missing insight and automation necessary to fully protect.

CHALLENGES OF SECURITY TODAY

The real world is dynamic and complex; and securing your environment is a major challenge.

IT infrastructures are in a state of constant change. The perimeter has dissolved and we are now connecting to applications in the network and in the cloud, all being accessed by an ever increasing set of devices that we don't control. There are over 2 billion devices connected to the Internet today—with a projection of that growing to 50 billion by 2020. Initiatives such as mobilization, consumerization, and virtualization—along with much more open and interconnected networks—have led to a computing environment that's in constant flux.

Figure 1. IT environments are open and changing rapidly.

[1]"The Future of Information Security is Context Aware and Adaptive," Neil MacDonald, Gartner, 14 May 2010, ID Number: G00200385

SOURCEfire®

New resources are deployed, configurations change, and applications are added at a dizzying pace. But traditional network security solutions are essentially static—they can't "see" these changes. In essence, they continue to protect the network as it initially existed—leaving new or changed resources undefended. Traditional, static network security tools are essentially out of date as soon as they're deployed.

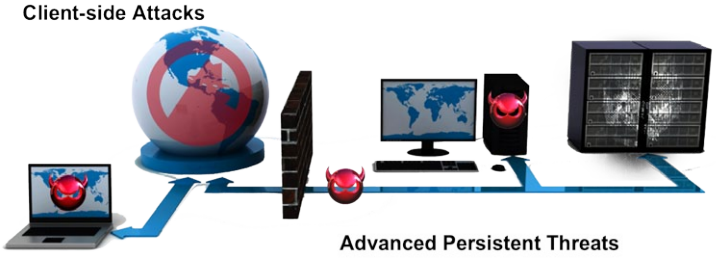

Figure 2. Threats are increasingly complex.

Not only are networks changing constantly, but threats are increasingly complex. Nearly three-quarters of attacks are only ever seen on a single system, and threat lifecycles are routinely measured in hours. This creates many attractive attack vectors for the bad guys.

Attacks are increasing because of the financial and geo-political gains for organized crime and nation states, where attackers are sophisticated, well financed and highly motivated. Whether hackers, script kiddies, client-side attacks, or advanced persistent threats, these attacks are targeted, effective, and have serious repercussions.

Organizations have adopted a variety of approaches to address these challenges.

TRADITIONAL APPROACHES FAIL TO PROTECT

Traditional network security products simply can't keep pace with increasingly dynamic networks and rapidly growing complexity. As a consequence, they don't deliver the protection organizations need and expect. Each historic approach has various shortcomings outlined below.

> *"Traditional approaches lack the contextual data needed to understand the network and the implications of a specific attack."*
>
> **– Martin Roesch, Founder and CTO, Sourcefire**

Firewalls and intrusion detection/prevention systems: As the mainstay of network defenses for years, such tools are at a fatal disadvantage from the outset, since they make no provision for either capturing or analyzing the range of contextual data that's needed to learn about and adapt to changes in networks and threats. They generate literally megabytes of alerts, but on their own are incapable of actually using any of that data to directly improve defenses.

Next-generation firewalls (NGFW): NGFWs, a more recent entrant on the security front, offer a partial solution to the need for contextual data by providing access to information about users and applications (and, of course, access controls over same). This certainly has the potential to improve security, by reducing attack surface and by providing a means of enforcing policy mandates and acceptable use policies. But typical NGFWs are still an incomplete solution, since so much other information is missing. For instance, many NGFWs do not have access to data about vulnerabilities associated with attack targets. So, they can't help gauge the probable impact or relevance of an attack. While important, gaining insight into applications and users alone does not in and of itself form a new defense.

Unified threat management (UTM) systems: UTMs consolidate multiple security functions into a single system, providing a broader range of data. But adding data without correlated analysis doesn't automatically yield more clarity. UTMs lack meaningful integration between discrete security functions, and lack any ability to adapt or evolve in response to changing conditions. In the end, UTMs just make existing challenges more difficult by adding more undifferentiated events and alerts to the bewildering array already on hand.

Consolidated security management systems: Faced with a lack of integration and context-aware inline defenses, some have sought to solve the problem by collating and correlating security data at the "back end." Vendors employing this approach typically use a proprietary management system as an integration point between point products, consolidating data to try and provide the requisite visibility and context. These efforts often flounder on multiple fronts.

In many cases, consolidated management products are parochial—visibility is provided only into a single vendor's products. Third-party products can't be integrated. So, either breadth or depth of information (or both) is often lacking. Where integration between different management components is provided, it varies in both quality and the level of functionality delivered. Analysts may still be forced to switch from one part of the system to another to try and gain a consolidated view of activity. Information can't be assumed to be up-to-date either. As a result, little incremental improvement to security visibility is realized. That lack of integration also hampers automation efforts, further limiting gains.

Security event/information management (SEIM) systems: SIEMs offer some promise, up to a point —they are still primarily analysis tools, not inline protection systems. SIEM vendors have become more adept at providing links to different security systems, so security and operations teams stand a better chance

	ELEMENT	TYPICAL FIREWALL	TYPICAL NGFW	TYPICAL IDS/IPS	WEB GATE-WAYS	NGIPS WITH FIRESIGHT	NGFW WITH FIRESIGHT
DETECT	NETWORKS	●	●	●	○	●	●
	APPLICATIONS/ SITES (URLS)	○	●	○	●	●	●
	USERS (IDENTITY)	○	●	○	○	●	●
	VULNERABILIITIES	○	○	○	○	●	●
	HOST PROFILES	○	○	○	○	●	●
	CLIENT APPLICAITIONS/ MOBILE DEVICES	○	○	○	○	●	●
	VIRTUAL MACHINES	○	○	○	○	●	●
	BEHAVIOR ANOMALY	○	○	●	○	●	●
CONTROL	LAYER 7 ACCESS	○	●	○	○	○	●
	USER ACCESS	○	●	○	○	○	●
	SITE ACESS	○	●	○	●	○	●
						CONTEXTUAL AWARENESS	

Figure 3. Traditional defenses lack the insight that fully context-aware solutions provide.

of accessing information about events from across their networks. But such systems may not provide the depth of information or level of detail needed to provide the full contextual data to evaluate specific threats in real time. In addition SIEMs generally don't provide automated real-time response capability, so they do little to advance event responsiveness.

It's clear that today's technologies only partially address the dynamic IT and complex threat environment. To solve these challenges, customers desire comprehensive network visibility and are looking for ways to regain a measure of control, keep pace and better protect themselves. Sourcefire FireSIGHT awareness and automation technology enables this.

FIRESIGHT: VISIBILITY AND AUTOMATION MAKES NETWORKS MORE SECURE

We can't hope to protect our networks if we don't understand them—how they're configured, what they're being used for, who is using them, and how the environment is changing. A key capability of FireSIGHT is to provide essential visibility into the network to capture this information. But FireSIGHT technology goes further, using this data to automatically update network defenses—evaluating events and modifying protections to maintain an optimal security posture. All the while providing critical guidance on event priorities to security teams.

The goal of capturing information about changing network resources and operations is to provide a solid contextual basis for making informed decisions.

- Context helps us understand which events are significant—and which are not.
- Context provides us with the perspective we need to evaluate changes to the environment.
- Context provides nuanced understanding to determine if a user's activity is appropriate or a threat.

Context requires we understand the entire environment, not just a subset of resources or some levels of a protocol stack. FireSIGHT technology provides in-depth 'full-stack' data on network resources, users, and activity.

FireSIGHT provides a breadth of data within each category.

- **Network Map and Devices**. A comprehensive and complete profile of all types of devices connected to the network. Supported devices include mobile phones, tablets, printers, virtual machines, and many other resources.
- **Network Behavior**. Alterations and changes in configurations, connections, and information flow, a reliable indicator of system compromises.
- **Operating Systems**. Including specific versioning information, yielding insights into potential risks and security issues.
- **Vulnerabilities**. Spanning multiple resources and years of historical records.
- **Applications, Services, and Protocols**. Including the ability to highlight unauthorized applications and insecure or unneeded services–proven attack vectors.
- **Users/Identity**. Understand exactly who is on your network, what they're doing, and where they're located.

VISIBITY CATEGORIES	SAMPLES	SOURCEFIRE NGIPS & NGFW	TYPICAL IPS	TYPICAL NGFW
Threats	Attacks, Anomalies	✔	✔	✔
Users	AD,LDAP, POP3	✔	✘	✔
Web Applications	Faacebook, Chat, EBay	✔	✘	✔
Application Protocals	HTTP, SMTP, SSH	✔	✘	✔
Client Applications	Firefox, IE6, Chrome	✔	✘	✘
Network Servers	Apache 2.3.1, IIS4	✔	✘	✘
Operating Systems	Windows, Linux	✔	✘	✘
Routers & Switchers	Cisco, Nortel	✔	✘	✘
Wireless Access Points	Linksys, Netgear	✔	✘	✘
Mobile Devices	IPhone, Android	✔	✘	✘
Printers	HP, Xerox, Canon	✔	✘	✘
VoIIP Phones	Avaya, Polycom	✔	✘	✘
Virutal Machines	VMWare, Xen	✔	✘	✘

Figure 4. Sourcefire FireSIGHT provides full-stack visibility into network resources, users, and activity.

In addition to providing a wide breadth of data, FireSIGHT technology delivers a deep level of detail. Levels of information provided include:

- **Trends and High-Level Statistics**. For managers and executives, understanding security posture at a moment in time, as well as how it's changing, for better or worse.
- **Reporting**. Addressing both general and focused information needs, driven by an individual's responsibilities or concerns.
- **Event Detail and Forensics**. Providing an understanding of "what happened," so it can be prevented in the future; supporting breach containment efforts; and aiding in law enforcement and legal actions.
- **Workflows**. Using information to drive responses to an event, improving response management.

The visibility into network resources that FireSIGHT technology provides is a critical foundation on which to improve security. But it's just the first step.

FireSIGHT takes network protection to the next level by providing automation that actually works to improve network defenses, while reducing operational costs.

FIRESIGHT: CONTROL IN CONTEXT

With the ability to learn and adapt, FireSIGHT technology delivers the control in context that's essential to addressing today's dynamic security environments. The overall Sourcefire 3D® System has been optimized to leverage this visibility to assess attacks and proactively respond and adapt to changes.

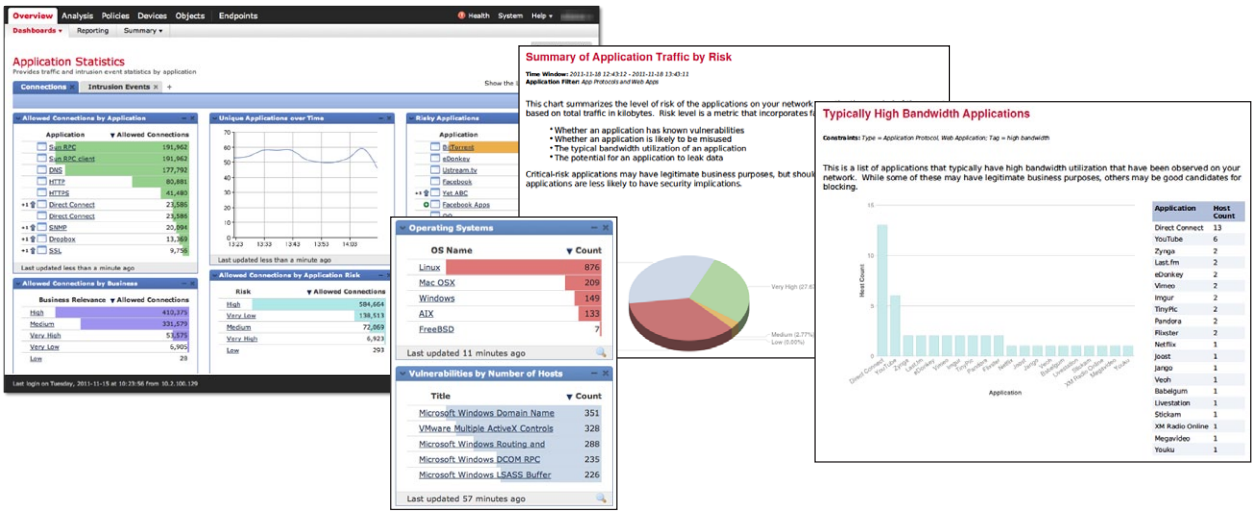

Figure 5. FireSIGHT enables both 'at-a-glance' summary information as well as detailed reporting.

IMPACT FLAG RATING & COLOR	ADMINISTRATOR ACTION
1	Act Immediately, Vulnerable
2	Investigate, Potentially Vulnerable
3	Good to Know, Currently Not Vulnerable
4	Good to Know, Unknown Target
0	Good to Know, Unknown Network
5	Good to Know, Blocked

Figure 6. Sourcefire's impact flags automate event analysis and allow security analysts to focus their attention on the security events that matter most.

For example, FireSIGHT can automatically correlate observed attacks with detailed configuration and vulnerability profiles of targeted endpoints. FireSIGHT can evaluate a given attack–perhaps a Windows-based exploit–with its target–a Linux server–to discover the threat is irrelevant. As a result, FireSIGHT technology will instruct Sourcefire Defense Center® to automatically dismiss the event, suppressing the alert. Meaningless noise is eliminated, and analyst productivity is improved. Similarly, that same attack directed against a vulnerable target would result in a high priority event. By focusing analyst attention on actual security threats, resources are used more effectively, response and mitigation activities begin sooner, and organization security posture is advanced.

"Events requiring manual reviews have been reduced from over 20,000,000 per month down to approximately 2,000 per month. By using Sourcefire FireSIGHT, we have been able to reduce the time and number of staff who are dedicated to analyzing our data, re-utilizing these SOC resources for other activities."

– Network Security Analyst, Global 500 Software Provider

FireSIGHT technology enables insight into changes in the network, such as the emergence of new resources, and can automatically implement detection changes to maintain the desired security posture. FireSIGHT recommended rules recommend which threat detection signatures to enable or disable. For example, if FireSIGHT determines that a protected network segment is only running Linux systems supporting Web services and NIS, then FireSIGHT can recommend disabling any rules pertaining to any Windows hosts and various Windows-specific services.

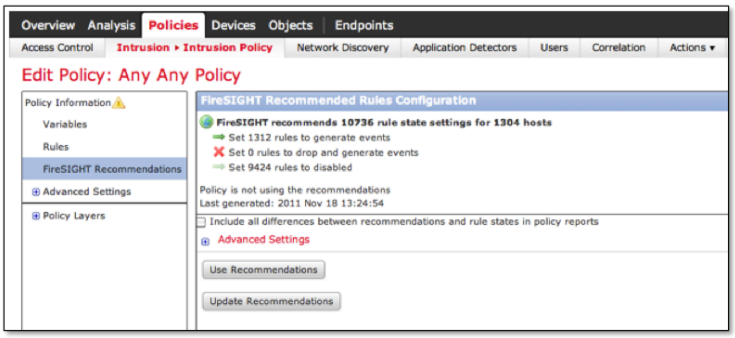

Figure 7. FireSIGHT recommended rules maximize appliance performance and significantly reduce, or virtually eliminate, the manual effort required to tune defenses.

But networks change over time. If a vulnerable system appears, it's crucial to both note the change and update defenses accordingly. Upon detecting a change in the environment, FireSIGHT can automatically recommend and even implement the necessary responses. In the previous example, FireSIGHT might first respond by activating the appropriate Windows security inspection rules, protecting the newly added resources. At the same time, the emergence of an unexpected–and unauthorized–resource would trigger an alert prompting an analyst to investigate the rogue system.

The time needed to respond to security events is a critical success factor for mitigation and restoration efforts. Unfortunately, such efforts are often slowed as analysts and operations staff perform time consuming searches for information about both network resources and the users associated with security events. The detailed network map and user identity correlation provided by FireSIGHT provides ready access to this data, delivering specific information in a timely fashion.

CONCLUSION: THE SOURCEFIRE DIFFERENCE

Rapidly changing resources and evolving threats require security systems both deliver and leverage a high level of visibility and insight into networks in order to provide effective protection. Complete vision is required for accurately detecting, evaluating, and responding to attacks. Sourcefire FireSIGHT technology uniquely provides the key capabilities essential to realizing this goal.

- **Depth and Breadth of Information**. FireSIGHT provides the broad range of information needed to effectively detect and automatically respond to emerging attacks and security risks. FireSIGHT also provides varying levels of insight into data, from a high-level perspective on trends to detailed, low-level forensics assessments of attacks.
- **Low-Impact Data Capture**. FireSIGHT gathers almost all information passively with no impact to ongoing network activity or system operations. FireSIGHT delivers a faster deployment at a lower cost, reduces the potential for service disruptions, and reduces ongoing operational expenses.
- **Control in Context**. FireSIGHT uniquely captures and uses information close to the network front-line, where security decisions and assessments must be made. Up-to-date information is readily available to guide event response, inform threat assessments, and take decisive action.

FireSIGHT ensures network protections are deployed appropriately, and maintained automatically, as networks and threats change over time. FireSIGHT enhances the quality of network security while helping to deliver the lowest possible operational expense. As demonstrated in countless deployments and independent evaluations, FireSIGHT ensures optimal security protection.

ABOUT SOURCEFIRE

Sourcefire, Inc. (Nasdaq:FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize network security risks. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire provides customers with Agile SecurityTM that is as dynamic as the real world it protects and the attackers against which it defends. Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with numerous patents, world-class research, and award-winning technology. Today, the name Sourcefire has grown synonymous with innovation, security intelligence and agile end-to-end security protection. For more information about Sourcefire, please visit www.sourcefire.com.