

SOURCEFIRE RETAIL SERVICES

# Next-Generation Protection for Retail Services

## USING AND PROTECTING INFORMATION FOR A COMPETITIVE ADVANTAGE

Regardless of the state of interest rates, prices, and other economic factors, the art and singular objective of retailing remains unchanged: to provide customers with goods and services that keep them coming back for more. However, the proliferation of merchants throughout the highly successful '90s coupled with the more recent growth of online shopping options have clearly resulted in a buyer's market. As consumers have shifted their purchasing criteria to demand more value, better service, and greater convenience, creating and sustaining a competitive advantage has become a much more challenging prospect. Consequently, retailers are having to evolve from practicing art to treating the operation of their businesses as a science. Greater precision is needed to more quickly, efficiently, and accurately balance the demand and supply sides of the retail equation.



Not surprisingly, the essential ingredient for providing greater precision is better information. Answers to the ageless retailing questions must be obtained more efficiently from all points in the end-to-end chain of operations and, importantly, in a more timely fashion. What is it that consumers want to buy right now? What are the primary, secondary, and tertiary factors influencing their purchase decision? How can it be ensured that they have an outstanding shopping experience? Exactly how great is the demand for product X? Is there an optimum quantity in stock, or do orders in the supply chain require modification? These are the currents that must be interpreted and then navigated on an almost continuous basis for retailers to establish greater operational efficiency, profitability, and sales.

It is with this in mind that the retail industry, traditionally conservative when it comes to change and associated investments, is now embracing information technology in a wholesale manner. Companies such as Wal-Mart and Dell have clearly demonstrated the gains to be had, for example, by streamlining their supply chains, forming closer relationships with supply chain partners, and leveraging the Internet to manage purchases, shipments, and even to sell their products. Batch processing is being replaced by real-time information exchange enabled by a range of network-based applications. Even the customer-facing components are being transformed, as the "store of the future" becomes the reality of today, with in-store networks supporting self-service kiosks, digital signage, and customized, on-the-spot advertising and mark-downs.

Of course, this increased usage and dependency upon information, the need to gather, analyze, redistribute, store, and, in general, manage it from end-to-end, also includes a responsibility to protect it. Clearly, purchasing preferences and other customer-specific data must be kept confidential. However, it is also essential to ensure the integrity and availability of all of the related data, as well as the networks and systems used to process it, particularly as these increasingly become the lifeblood upon which retailers depend.


Needless to say, this only accounts for a handful of the key issues, trends, and relatively unique conditions which characterize the retail industry. Indeed, a variety of other factors also contribute to the wide range of challenges facing network and security administrators operating within such businesses. For example:



- ▶ Clearly it would be inappropriate to classify the networks and systems of retail companies as “critical infrastructure.” However, there is in fact one point of intersection between the retail world and networks that are designated as such. Specifically, batch and real-time exchanges of transaction details with credit card companies and other financial institutions create a linkage to an environment that is much more tightly controlled, and even regulated. One significant implication is that virtually all merchants who process credit card transactions are subject, at least in part, to the Payment Card Industry (PCI) Data Security Standard. From an information security perspective, this establishes a minimum standard of due care that must be maintained. In general it conveys the need for affected companies to implement a comprehensive set of administrative, physical, and technical safeguards to protect their networks and systems, and, in turn, the information they transport and store. Emphasis is placed on establishing robust access controls and subsequently being able to monitor and audit for undesirable activities, in particular, by using both host and network intrusion detection and prevention systems (per requirement 11.4).
- ▶ A highly competitive marketplace inevitably leads to shrinking margins. Thus, while it is necessary to improve the flow of information along the entire chain of operations, it is also necessary to control costs when doing so. Enabling productivity gains and lower cost of ownership are essential requirements of all supporting systems, including those associated with maintaining privacy and security.
- ▶ Cost control is also the driver behind the broad set of initiatives that are designated in aggregate as supply chain management. The relevant point here is that regardless of the individual objectives (e.g., inventory optimization, distribution optimization, least-cost sourcing), there is a need to share information with a broad and highly diverse cast of supporting parties. In turn, this means opening up access to various systems, taking advantage of relatively inexpensive public network services (i.e., the Internet), and subsequently having to protect one’s own computing environment from potential threats originating from the “other side.”
- ▶ The growing need to “go global” also introduces very similar requirements. Often achieved through mergers and acquisitions or strategic alliances and franchises, executing upon a global strategy typically entails establishing connections to and sharing information with parties that have differing, and largely unknown degrees of protection when it comes to information security.
- ▶ With very few exceptions, it is an absolute necessity that retailers complement their physical stores with an online shopping option. This, of course, means having to deal with the wide range of threats that an Internet-based store front brings with it (e.g., fraud, the spread of worms and viruses, and malicious hacking)
- ▶ Increasingly, both achieving operational excellence and ensuring a positive shopping experience are becoming dependent on supporting a plethora of network-based applications (e.g., traffic counting systems, customer loyalty programs, warehouse management systems, transportation management systems, self-service kiosks, in-store employee training). This translates into the need to better ensure the availability, capacity, and performance of associated networks and systems.
- ▶ These very same drivers are also causing retailers to embrace a wealth of new technologies and solutions. Examples include the use of VoIP (Voice Over Internet Protocol) to reduce inter-store communications, the use of various wireless technologies to help un-tether sales associates, and the use of RFID (Radio Frequency Identification) tagging to assist with inventory management. The implication is that the IT department must now secure an even greater collection of systems and applications and, is therefore, in need of even further ways to improve their own operational efficiency.
- ▶ Of course, just because “the new” is being embraced does not mean that “the old” is automatically being abandoned. True to their conservative heritage, many retailers will continue to operate legacy systems as they make a piece-wise transition into the new generation of information technology. These systems are often fully inter-connected with more modern ones and continue to perform mission-critical functions. However, supporting them can be quite challenging. Skilled personnel are in short supply and updates from original manufacturers are far and few between – if available at all. The result is that many retailers must contend with operating systems that are exposed to network-borne threats but which can not afford to be taken out of service for remediation – assuming applicable patches are even available in the first place.

Overall, it is clear that a highly competitive landscape is forcing retailers to transform the way they conduct business. Information technology must be embraced further every day, not only to automate business processes but also to enhance the customer experience. This means putting greater volumes of information at risk by making it accessible via electronic means. However, at the same time this landscape is also elevating the importance of having a positive brand identity – a crucial characteristic when everything else is quite literally a commodity. The net result is that ensuring the continued trust of their customers, and consequently the strength of their brand, depends on retail companies diligently maintaining the security of their information systems.

## MANAGING THE BROADER LANDSCAPE



Of course, in addition to its own set of challenges, the retail industry must also address a majority of the issues and security related trends impacting the Internet community at large. For example, beyond the PCI Data Security Standard, most retail organizations must also comply with one or more of the pieces of more broadly applicable privacy and governance-related legislation (e.g., the various state-level breach notification acts, Sarbanes-Oxley, or similar governance codes established in other countries). To be clear, even when organizations are not explicitly subject to these laws, it is important to recognize that volunteer adherence with some of the more relevant measures is still considered “best practice.”

Regulations and compliance aside, there are plenty of other globally applicable security issues to keep retail companies busy. Threats, in the form of new attacks, are emerging faster than ever, especially relative to the time of disclosure of their associated vulnerabilities. In other words, the window of opportunity to take corrective action between the time that a vulnerability is announced and the time that an attack against that vulnerability emerges in the wild is dwindling. Just a few short years ago that window was typically three to six months. The Zotob worm, and the Witty worm before it, cut into that time considerably, reducing the window essentially to a few days. Implementing patches in this timeframe, assuming they are even available, is simply impractical.

As if this were not enough, today’s threats are faster, smarter, more prevalent/frequent, and even more elusive.

- ▶ **Slammer doubled its infection count every 8.5 seconds and reached 90% of all vulnerable hosts on the Internet within 10 minutes. And that was over two years ago! This just goes to show that the potential for flash threats – ones which can spread within 30 seconds – is very real.**
- ▶ **Blended threats utilize multiple attack mechanisms, giving them better odds of having an impact even in protected environments. Worse yet, attackers are focusing their efforts higher up the stack computing stack. By targeting application-layer vulnerabilities they are dramatically reducing the effectiveness of the vast majority of commonly deployed security tools, which are focused predominately on providing lower-layer protection.**
- ▶ **Automated tools and exploit development kits continue to “lower the bar” in terms of the knowledge and effort required to launch an attack. The result is both a greater volume and increasing sophistication of malware that is being released into the wild and directed at specific targets.**

The net result is that in 2004 nearly 40,000,000 hosts were infected, impacting an estimated 75% of all Internet-connected organizations. And all indications point to these trends continuing into the foreseeable future. Furthermore, it is unreasonable to expect that the financial services industry is immune to these conditions. Indeed, while the vast majority of security incidents are never disclosed, there are still a handful of published examples and related evidence that support this conclusion. For example:



- ▶ In January of 2003, approximately 13,000 Bank of America ATMs were rendered inoperable by the Slammer infection.
- ▶ In June of 2005, payment processor CardSystems acknowledged a security breach in which account records for 40,000,000 credit cards were exposed, with approximately 200,000 of those confirmed to have been stolen/compromised.
- ▶ The Global Security Survey of financial services institutions conducted by Deloitte Touche Tohmatsu in 2005 revealed that approximately one third of responders had their systems compromised in some way over the previous year.

"In the PCI standard, it states we must use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. There are two kinds of IDS/IPs on the market. One, you plug in and don't ever want to hear from again. Then there's the other kind that lets you get useful information about your network. That's what we have with Sourcefire."

**Michael Morgan**  
Network Security  
Administrator  
BankersBank Card Services

### Staying Ahead of the Zotob Worm

- 8/12/05** - Sourcefire Vulnerability Research Team (VRT) responds to a Microsoft Windows Plug-and-Play (PnP) vulnerability announcement that came out a few days earlier—issuing an advisory and releasing a number of rules to detect all attempted exploits against the PnP vulnerability.
- 8/14/05** - The Zotob worm is identified in the wild.
- 8/15/05** - After thorough analysis of the worm, Sourcefire notifies customers that rules were already in place to detect Zotob activity.
- 8/17/05** - Variants of Zotob as well as other attacks emerge. Sourcefire VRT verifies that all are covered by original rules update.
- 8/19/05** - Sourcefire publishes instructions on how to leverage the power of Sourcefire Real-Time Network Awareness (RNA) and the Sourcefire 3D System Policy and Response engine for further Zotob detection.

Finally, it should also be apparent that conventional approaches and security tools are doing very little to stem the flood of incidents. Clearly, these inadequacies indicate the need for a next-generation security solution. This solution must be unobtrusive – not impeding the flow of legitimate traffic – yet still highly effective at stopping real threats. One that is able to address the unique challenges facing the financial services industry, but which, above all else, remains economical and easy to use. One that provides protection during all phases of the attack lifecycle: before, during, and even after.

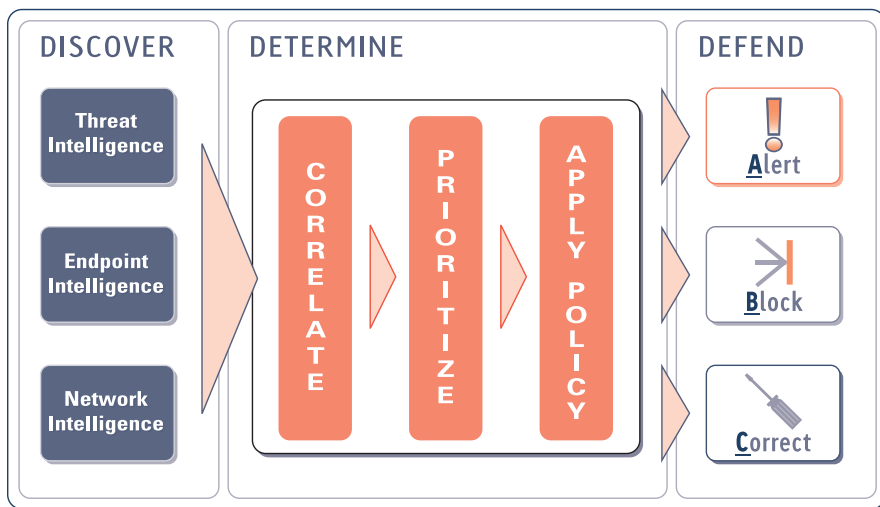
## THE SOURCEFIRE 3D SYSTEM - A NEW LEVEL OF TRUST

Sourcefire's ground-breaking 3D approach – Discover, Determine, and Defend – is a comprehensive intelligent network defense system that unifies intrusion and vulnerability management technologies to provide the most effective, real-time protection against today's real-world challenges. Combining expert knowledge, detection, and analysis of threats, vulnerabilities, network events, and endpoint intelligence provides an unmatched degree of coverage – actually fulfilling the need to track attacks and potential compromises across all vectors all the time – before, during, and after an attack.

Comprised of three main components, the Sourcefire 3D System is uniquely capable of addressing the full range of security trends, issues, and challenges confronting not only the power industry, but also shared by many other utilities and energy related businesses.

### Component One:

Sourcefire Intrusion Sensors and Agents are at the heart of the Sourcefire 3D System. They provide defense-in-depth for all networks by monitoring and analyzing network traffic, stopping known bad elements in their tracks and alerting administrators of otherwise suspicious activity. By enhancing the award-winning SNORT® technology and adding an easy-to-use interface, optimized hardware, and



powerful data analysis capabilities, Sourcefire Intrusion Sensors provide the most effective network monitoring and intrusion prevention technology available today.

High-fidelity detection accuracy is

“Sourcefire RNA is like a magic eye that watches everything happening on your network.”

Network World

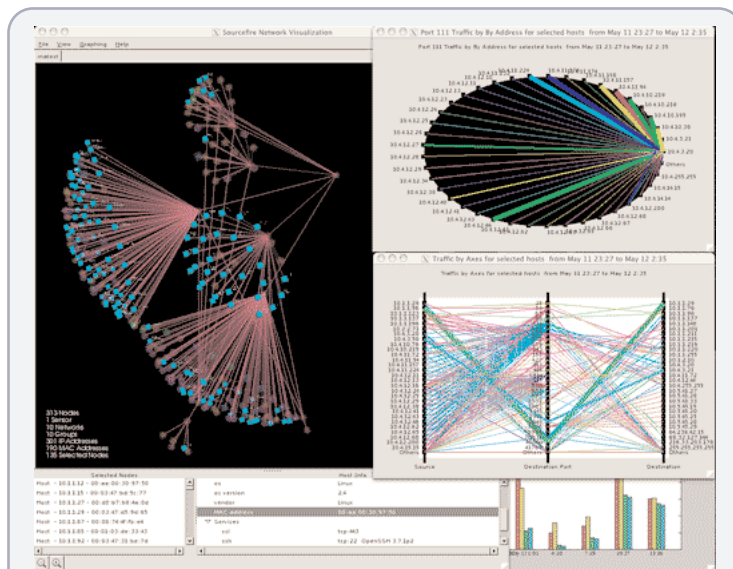
“My concern was that the false positives were camouflaging the real attacks. Sourcefire offers a whole different way of approaching the problem using passive network discovery, behavior profiling, and vulnerability analysis technology. The combination shows me which events really matter. It eliminates the problem of being inundated by events. Now I can marry the vulnerability status of the server and application to an event and target ones that matter.”

Matthew Keogler  
Senior Security and Network Engineer  
Autotrader.com

ensured by using a comprehensive combination of detection techniques – for example: protocol anomaly, heuristics, behavioral anomaly, and fashion signatures/pattern matching. It also comes from having a robust and highly granular rules language, which enables pinpoint isolation of bad elements without having to impact any of the legitimate items in a communications stream. The result is both fewer false positives and fewer false negatives ... a critical prerequisite to increasingly automating threat prevention activities.

Superior effectiveness is also derived from the timely availability of new algorithms and signatures. In this regard, Sourcefire’s VRT is an invaluable resource. The Sourcefire VRT is a group of leading-edge intrusion detection and prevention experts working to proactively discover, assess, and respond to the latest trends in hacking activity, intrusion attempts, and vulnerabilities. By focusing on the characteristics of vulnerabilities immediately subsequent to their being announced, the Sourcefire VRT is frequently able to provide protection (e.g., in the form of detection rules) prior to the emergence of an associated attack.

**Component Two:** Sourcefire RNA Sensors act as the eyes and ears of the Sourcefire 3D System. These sensors add a layer of intelligence to network monitoring that has never been seen before within the network security industry. They constantly monitor network assets, identifying potential vulnerabilities and alerting administrators in real time to anomalous network behavior. Sourcefire RNA Sensors also persistently provide context, enabling breakthrough advances in terms of accuracy, effectiveness and usability of intrusion detection and prevention technology.



The Sourcefire RNA Visualization Module alerts you when anomalous behavior is detected on the network. When that happens, the specific node begins to blink.



Indeed, information obtained by Sourcefire RNA can be used both before and after the emergence of an attack to facilitate remediation, as well as to tune Intrusion Sensors, making them more efficient and less likely to generate false positives. This RNA-generated information can also be used to identify previously unknown (i.e., day-zero) or otherwise undetected attacks, and to support generation of new, highly effective detection rules for these threats.

With its passive monitoring and analysis capabilities, Sourcefire RNA effectively complements Intrusion Sensors, extending their reach beyond just that traffic which passes directly through them. Its broad coverage and wide range of functionality make RNA the ideal approach to effectively and efficiently monitor a highly complex power plant environment. Overall, Sourcefire RNA's unique combination of attack detection, always-on passive discovery, targeted active scanning, behavioral profiling, and vulnerability analysis delivers the most comprehensive view of the security events occurring on an network – an essential foundation for effective network defense.

### Component Three:

The Sourcefire Defense Center is the brains of the Sourcefire 3D System, providing advanced analysis capabilities and coordinating the activities of the two types of sensors. This high performance management tool is especially well suited for large and distributed enterprise networks. It simplifies the complicated issues usually associated with intrusion detection and prevention deployments by incorporating policy management, data aggregation, correlation, and reporting into a single centralized solution that enables power companies and utilities to make the most of distributed sensor infrastructures.

Sourcefire Defense Center is delivered with a built-in high performance database capable of handling millions of events and supporting in-depth forensic analysis for identification of both discrete occurrences and long-term security trends. Packaged as a complete, pre-configured system and including an intuitive, efficient interface, Sourcefire Defense Center is not only a snap to install but also easy and convenient to use on a daily basis.

## PROVIDING NEXT-GENERATION PROTECTION FOR THE RETAIL INDUSTRY

As a state-of-the-art intrusion detection and prevention solution, the Sourcefire 3D System is appropriate for any and every Internet-connected organization concerned with protecting its computing resources and electronic information. However, the Sourcefire 3D System is also particularly well positioned to address the aggregate issues and trends facing retailers.

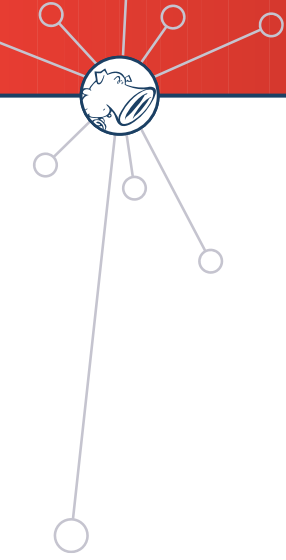
- ▶ **Ensuring the confidentiality of customer information and the integrity and availability of crucial supply and demand side data, not to mention the reputation and brand of your company, demands the use of best-of-breed information security solutions. The Sourcefire 3D System is such a solution.**
- ▶ **The Sourcefire 3D System stops attack traffic regardless of its point of origin, thereby providing a must-have layer of security when supporting connections originating from untrusted and potentially insecure hosts (e.g., those owned and operated by diverse supply chain partners). In doing so, it also provides a “virtual patching” capability. This enables difficult-to-manage legacy equipment (e.g., out-dated point-of-sale systems) to stay in operation until their next scheduled maintenance period despite having identified weaknesses.**

### The Fourth Component: The Snort Community



As the creators of Snort® – an open source network intrusion prevention

and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods – Sourcefire, and thus its customers, enjoy a truly unique advantage: the Snort Community. With greater than 3,000,000 downloads and over 150,000 active users, Snort is undisputedly the most widely deployed intrusion detection and prevention technology worldwide and has become the de facto standard for the industry. Its highly engaged user community is an unmatched resource, providing early warnings of new threats, generating and publishing specialized rule sets, and providing immediate feedback and quality control services on new code and content. In essence, it's like having a 100,000 person team for development and technical support! It is also highly likely that a portion of this community is near at hand, given that the majority of students learning about intrusion detection and prevention on campuses today are being taught using Snort.

- 
- ▶ **By combining monitoring, vulnerability management, and attack prevention functions all in a single solution, the Sourcefire 3D System efficiently helps ensure compliance with virtually all privacy and security related best-practice guidelines and regulatory requirements – both those that exist today, such as the Payment Card Industry (PCI) Data Security Standard, as well as those which will inevitably emerge going forward.**
  - ▶ **The Sourcefire Intrusion Sensor’s in-depth and highly flexible rules base inherently accommodates a great diversity of protocols, applications, devices and technologies. Out-of-the-box coverage for common modern technologies (including wireless networking and convenient handheld devices) can be supplemented by extensible coverage for virtually any type of communications traffic.**
  - ▶ **Sourcefire RNA sensors can demystify complex and far-flung IT environments associated with large, distributed networks, or with the conglomerations that are the result of M&A activity within the industry. Complementary passive and active scanning techniques yield a comprehensive and up-to-date inventory of communications infrastructure, applications, and potential vulnerabilities. Not only does this efficiently provide unmatched visibility into an organization’s IT environment, but it also facilitates proactive remediation and automatic protection of deficient systems.**
  - ▶ **A high degree of detection accuracy, signature/rule coverage that extends up the computing stack, and vulnerability based rules ensure that the rapidly emerging, smarter, and more elusive threats of today and tomorrow are kept in check. Practical automation of threat mitigation activities also enables fast-moving worms to be stopped in their tracks, while also enabling network and security operations staff to be more efficient.**
  - ▶ **Highly tunable sensors operating on custom hardware and a purpose-built database for the management platform yield high-performance (i.e., low latency, high capacity) components capable of supporting both the high steady state and peak traffic volumes triggered during holiday periods and other flash events.**
  - ▶ **Items such as a built-in, high-capacity database, management coverage and integration with open-source Snort® implementations, the Snort user community, and an easy-to-use, centralized management application all facilitate having a comprehensive attack protection solution even on a tight budget.**

The bottom line is that above and beyond all of these capabilities the Sourcefire 3D System is the only product that provides next-generation true intrusion prevention. State-of-the-art intrusion sensors are complemented by essential Sourcefire RNA technology to more effectively prevent all threats, from all vectors, all of the time – providing protection before, during, and even after an attack.

### About Sourcefire

Sourcefire, Inc., a world leader in intrusion prevention, is transforming the way organizations manage and minimize network security risks with its 3D Approach - Discover, Determine, Defend - to securing real networks in real-time. The company’s ground-breaking network defense system unifies intrusion and vulnerability management technologies to provide customers with superior network security. Founded in 2001 by the creator of Snort®, Sourcefire is headquartered in Columbia, MD and has been consistently recognized for its innovation and industry leadership by customers, media, and industry analysts alike – with more than 18 awards and accolades since January 2005 alone. Recently, the company was positioned in the Leaders Quadrant of Gartner’s “Magic Quadrant for Network Intrusion Prevention System Appliances” report and the Sourcefire 3D System was named “Best Security Solution,” at the 2006 SC Magazine Awards. At work in leading Fortune 1000 and government agencies, the names Sourcefire and founder Martin Roesch have grown synonymous with innovation and intelligence in network security.

©2006 Sourcefire, Inc. Sourcefire 3D System, Sourcefire RNA, Intrusion Sensor, RNA Sensor, Defense Center, Sourcefire Success Pack, Sourcefire VRT and Snort are trademarks or registered trademarks of Sourcefire. All rights reserved.

