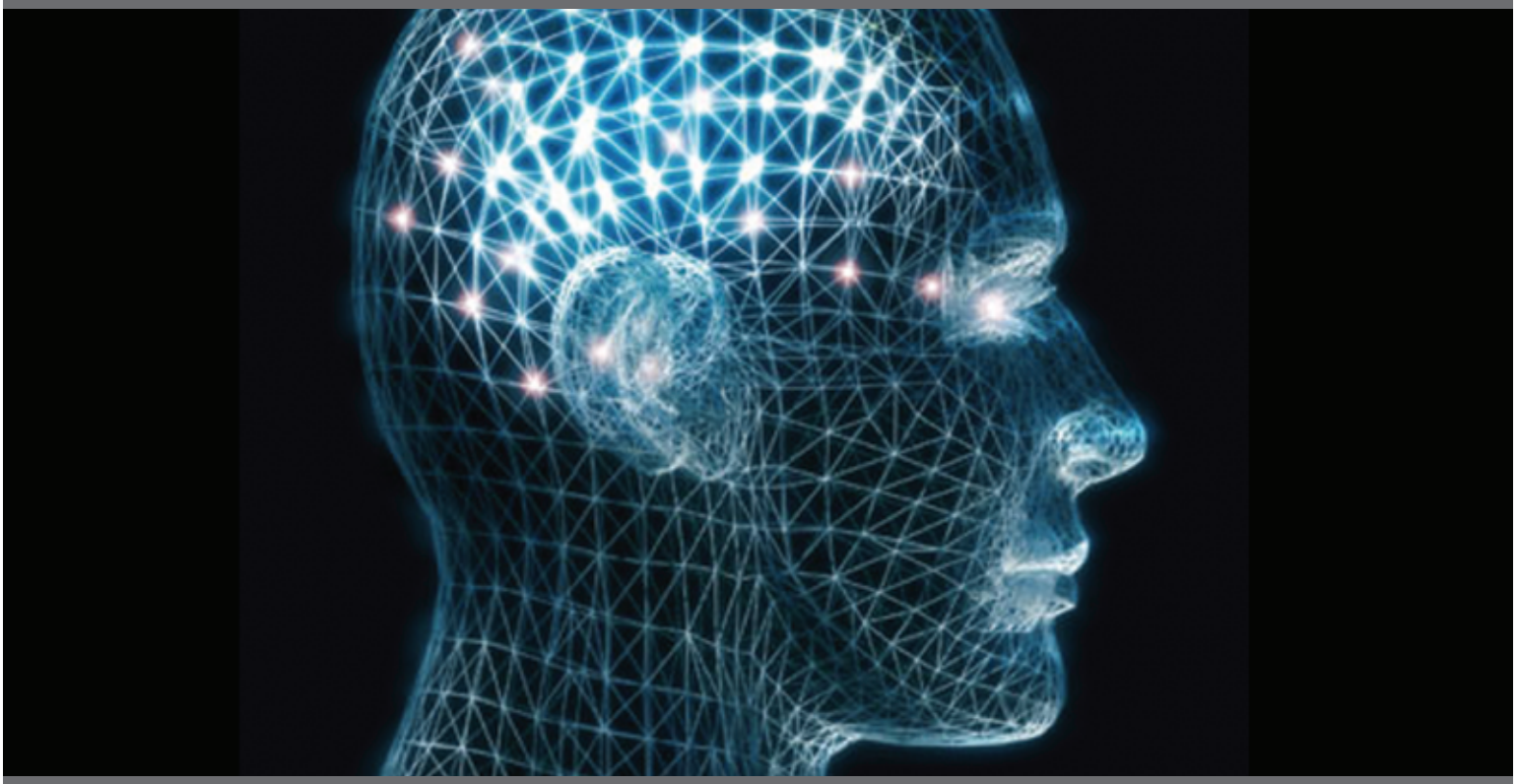
WHITE PAPER

Cyveillance®



# The new protection paradigm: Intelligence-Led Security

A next-generation, knowledge-based approach to security that intelligently detects and predicts threats to consumers and business assets wherever they may be

## INTELLIGENCE-LED SECURITY

## TABLE OF CONTENTS



**© 2007 Cyveillance, Inc.** All rights reserved

*This paper discusses the use of intelligence to bolster traditional security approaches in today's highly connected, borderless world.*

## EXECUTIVE SUMMARY

## The move from trailing to leading security indicators

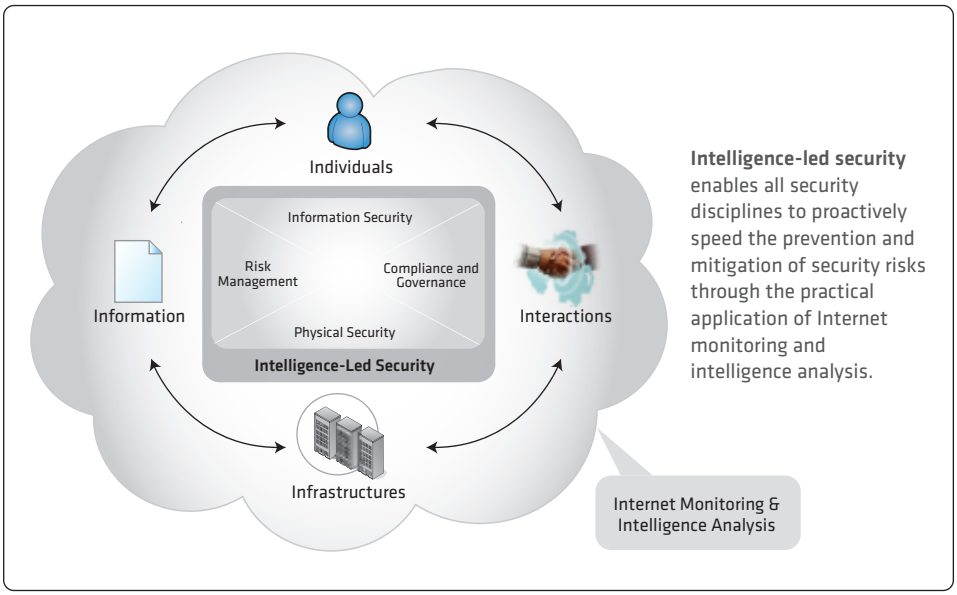
Businesses and consumers are not adequately protected by prevalent security methods that focus only on low-level technical controls and post-attack mitigation. To address the need for more comprehensive, strategic protection methods, companies are starting to converge their physical security, information security, business continuity, and various risk management and compliance practices. Security convergence is a good idea, but an even more fundamental paradigm shift is taking place as well—a move toward proactive, intelligence-led security.

Intelligence-led security is an approach that integrates intelligence analysis methods, tools and processes to effectively manage security risk in today's Internet environment. It is a practical application of Internet monitoring and intelligence analysis, which draws on advanced search strategies and pattern recognition to identify, detect and analyze existing and potential threats to businesses and consumers—in terms of information, infrastructure and interactions. By identifying threats generated by cyber criminals, predators, extremists, activists, insiders and others early, actions can be optimized to speed the prevention and mitigation of security risks.

The move to an intelligence-led security paradigm is fundamentally necessary if our protection efforts are to rise to the current challenges. Because it is knowledge based, intelligence-led security can "think ahead" of threats and deliver:

- A proven, cost-effective early-warning system for threats against consumers and businesses
- A holistic security view, featuring the ability to fully protect information and infrastructure, as well as individuals and their interactions
- A practical application of global Internet monitoring and intelligence analysis, enabling highly effective physical security, information security and risk management
- Integration of large amounts of captured data, analysis methods, automated tools and processes into streamlined support for enterprise decision making
- Advanced search agents, crawlers, honeypots and pattern recognition to identify, detect, analyze and predict threats

Intelligence-led security identifies threats generated by cyber criminals, predators, extremists, activists and insiders early in the attack cycle, so actions can be rapidly optimized to prevent and mitigate impacts. The intelligence-led security approach that is described in this paper is currently available in several forms: security portals, Security Operations Center (SOC) services, live data feeds, and bundled into OEM software and Web application products.




**Intelligence-led security** enables all security disciplines to proactively speed the prevention and mitigation of security risks through the practical application of Internet monitoring and intelligence analysis.

## INTRODUCTION

### Security at a crossroads

According to Gartner and other industry watchers, steady increases in security budgets have not led to steady increases in the safety of critical business processes and consumer activities. This is because traditional physical and information security methods are focused on **trailing indicators,** such as viral signatures, incident response and forensics, that are mainly tactical and after the fact. Trailing-indicator security is necessary, but it tends to be reactive and localized, with a reliance on local mitigations, such as better laptop antivirus software or stronger door locks for the warehouse.

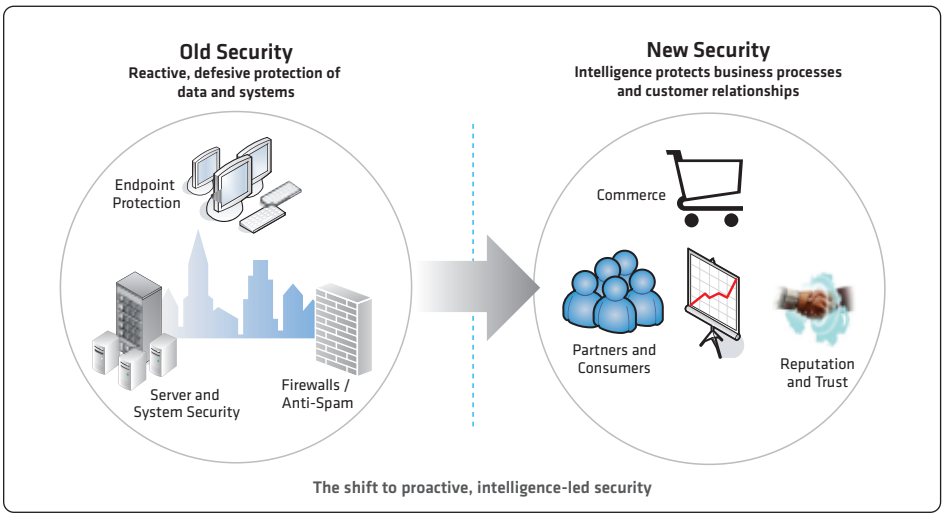
Traditional security focuses on hardening the perimeter to guard against outsider entry to physical locations and networks while simultaneously preventing employees from visiting unauthorized access points. While some very basic intelligence can be collected from classic security technologies, such as intrusion detection systems, firewalls, badge systems and security cameras, it is inherently limited to localized activity.

In contrast, the emerging knowledge-based security paradigm is the opposite of local and reactive because it looks for **leading indicators** among a wide range of global intelligence sources. The shift from tactical, trailing-indicator security to expansive, intelligence-led security is already visible at leading companies that are starting to use findings derived from the public Internet as an early-warning system that can detect and predict threats from both the cyber and physical worlds.

Intelligence-led security is a necessary outcome of the current commercial model, which integrates distributed businesses, consumers, partners and suppliers in dynamic interactions that crisscross real-world and cyberspace trading venues. In a highly interdependent and complex business environment, there is no safety in a security posture that is inward facing and reactive. Given that the traditional enterprise perimeter has been eradicated with people connecting to the Internet from multiple devices and networks at any time and from anywhere, the security challenge now encompasses a vast range of activities that are largely distributed



Cyveillance®




The shift to proactive, intelligence-led security

and decentralized. The business world is becoming borderless in the sense that customers and partners can now connect from multiple devices, via multiple networks, and from multiple locations–which means that the defense perimeter needs to be "virtualized" and applied to business and consumer assets wherever they happen to be.

In a borderless commerce system where customer and enterprise assets are highly distributed, an expansive, 360-degree, intelligence-led security strategy is needed to sense and respond to threats on a continual basis. This requirement is similar to the need met by government and military intelligence agencies that monitor and protect national and strategic interests. Intelligence-led security provides early warnings of dynamic, rapidly changing global threats to enable a more outwardly focused, proactive risk mitigation posture for security, which bolsters present-day reactive approaches.

## Getting smart about intelligence

Significant precedents for the intelligence-led security imperative are seen in the area of national security. After 9/11 and recent policy challenges in the Middle East, there was a lot of soul searching about whether threats could have been anticipated with better intelligence. Many improvements in military and national defense intelligence were proposed and initiated, including the incorporation of more "open source," outwardly facing threat detection into the intelligence mix. Something similar needs to take place in the business community.

> **"Knowledge is the critical component in defeating an asymmetric threat situation. A good defense in an asymmetric struggle can only come from an understanding (knowledge) of the threat and therefore an ability to combat it or stop the threat before it materializes."**
>
> – Tom Quiggin, "Seeing the Invisible: National Security Intelligence in an Uncertain Age," 2007

Traditional military warfare and intelligence models are symmetrical, with one combatant aligned against the other along a well-defined border or perimeter. In symmetrical warfare, the primary job of intelligence is to provide visibility into threats that are "behind enemy lines." When the symmetrical warfare model is applied to enterprise security, the area inside the firewall perimeter is considered safe, and the area outside the perimeter is considered untrusted.

**The New Craft of Intelligence**

*Above all, the new craft of intelligence is comprehensive, reliable, swift, and relevant to the challenges of all threat forms, especially nontraditional threat forms. The new craft of intelligence, properly affected, provides an asymmetric advantage in dealing with any challenges, be they violent or nonviolent, state or non-state, immediate or long term.*

– **The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats** (U.S. Army War College Report, 2002)



Cyveillance®

As can be seen clearly in today's military conflict zones around the globe, threat vectors are now largely asymmetrical, i.e., not organized neatly along a border or battle line. This is true in the business world, too. Asymmetric threats are outside and inside our systems, businesses, factories, homes and schools. Asymmetric threats are a growing fact of life, so our security postures have to be recast to make our defenses viable in this new context. Since asymmetric threats don't conform to clear-cut borders and perimeters, security must adopt an intelligence-led approach that gathers and analyzes information from a wide range of sources and locations, with a goal of identifying and predicting threats to distributed businesses and consumers.

Going forward, the theater of conflict is everywhere and nowhere in particular. Continuously generated, 360-degree intelligence is paramount to survival.

The spread of asymmetric threats also involves a shift from compartmentalized to globalized theaters of conflict. Traditional military intelligence has been deployed on several levels. **Tactical intelligence** is highly time sensitive and perishable, and it supports local conflict. When tactical intelligence fails, it compromises local engagements that are limited in scope. **Operational intelligence** works at the regional level, where an intelligence failure can jeopardize assets throughout an entire region. Finally, **strategic intelligence** addresses threats with national and global implications, and failure can reach catastrophic proportions.

This hierarchical, geographical approach to intelligence is typical of symmetrical threat protection. But in the era of highly asymmetric military and commercial conflicts, it is not so easy to distinguish between local, regional and global threats. A seemingly tactical threat (e.g., a teenager using a laptop computer on a university network) can incur millions of dollars worth of damage to brand equity and infrastructure halfway around the world. Consequently, the distinction between local and global threats is no longer very useful. Going forward, the theater of conflict is everywhere and nowhere in particular. Continuously generated, 360-degree intelligence is paramount to survival.

## Intelligence-led security—a practical approach

To protect the full scope of business and consumer interests, intelligence-led security needs to capture, store, process, filter and analyze information from many sources. If budgets were no obstacle, corporate security officers could hire their own armies of human "intelligence agents" to operate wherever business is conducted, constantly monitoring and tracking commercial activities, looking for threats. This is neither practical nor affordable, but there is another way. An economically viable approach to intelligence-led security is found in the ever-growing mountains of visible and hidden data that exist in global cyberspace. This wealth of raw data can be cost-effectively harvested with leading-edge automation, and then filtered, analyzed and presented to the security team and other enterprise stakeholders in an easy-to-assimilate and highly relevant format.

Virtually all major business threats and opportunities leave traces on the Internet. By collecting, filtering and analyzing these traces, intelligence-led security creates a stream of actionable intelligence that can protect consumers and key business assets. Blue-chip corporations see the need for using intelligence to create a more proactive security posture to speed prevention and mitigation of risk, and they are already working on intelligence-led programs.

The "open source" visible and hidden online data used by intelligence-led security is captured from Web pages, blogs, wikis, Internet Relay Chats (IRCs), message boards, botnets, newsgroups, auction sites, P2P networks, FTP sites, spam, phishing content, search engines, and other content repositories. The collection and analysis of this data enable the detection of business threats long before they show up in intrusion logs and operational reports.

Intelligence-led security is an approach that integrates intelligence analysis methods, tools and processes to proactively address security risk in today's climate of highly asymmetric threats and opportunities.

Intelligence-led security is practical and affordable, and it addresses some of the most serious headaches of today's security teams, including the protection of revenue-generating and cost-saving customer interactions by safeguarding customer e-mail, Web and e-commerce activities. It can be used to spot threats and subtle risk trends that will adversely impact traveling corporate executives, plant facilities, storefronts, and other physical assets. And, it represents a common approach used to address insider threats, information leaks, and the abuse of brands and corporate intellectual property anywhere on the Internet or in the physical world.

How is intelligence-led security actually deployed? Intelligence platforms can be integrated directly into the enterprise business processes and management framework through portals and Web services. Intelligence can also be integrated directly into commercial and consumer OEM software and appliances, as well as online services, which protects users automatically as they surf the Internet, use e-commerce sites, and access interactive Web content.

In summary, intelligence-led security is an approach that integrates intelligence analysis methods, tools and processes to proactively address security risk in today's climate of highly asymmetric threats and opportunities. Intelligence-led security is a practical application of Internet monitoring and intelligence analysis, which draws on advanced search strategies and pattern recognition to identify, detect and analyze actual and potential threats to businesses and consumers. Because it can process and digest vast amounts of online data, intelligence-led security is uniquely able to protect enterprise and consumer information and infrastructure, as well as individuals and their interactions. By identifying threats generated by cyber criminals, predators, extremists, activists, insiders and other blackhats, decisions and actions can be optimized to speed the prevention and mitigation of security risks.

*The remainder of this paper discusses the use of intelligence-led security for protection of customer interactions, corporate information, employees and infrastructure. The compliance and governance benefits of intelligence-led security also are discussed.*

## PROTECTING CUSTOMERS AND REVENUES

Information security solutions are focused on protecting data and systems at select key points in the infrastructure and in some aspects of the end-user process. Firewalls and VPN gateways are put in place at the network perimeter; SSL and user authentication protect online e-commerce transactions. But none of these methods protects the entire user experience. For instance, an e-commerce Web site can deploy SSL to encrypt transactions flowing from the customer's browser to the Web server, but this still leaves the customer open to a wide range of serious threats that can result in: lost revenue, lost competitiveness, lost reputation, lost

customer trust, and substantial legal and operational costs. Conventional security methods struggle to address today's threat environment, which includes:

- Web sites that distribute malware
- Phishing scams
- Numerous identity theft schemes
- Counterfeit and gray market product sales
- Customer diversion and brand abuse

## Malware

So-called "drive-by downloads" are a good example of a threat that is not addressed by SSL, user authentication, VPNs, or other conventional information security methods. Drive-by downloads often occur when the online customer is somehow enticed by trusted brands, logos, and "special offers" to visit a fraudulent site where malicious software (malware) is downloaded automatically to the user's system in the course of normal Web browsing activities. The malware can contain a wide range of threats, including keyloggers and screen scrapers that can steal passwords, credit card numbers, and other personal details. The malware can also install "bot" software that forces the user's PC or portable device to participate in illegal and damaging "botnet" exploits that target valuable business and Internet resources with spam and Distributed Denial of Service (DDoS) attacks.


To protect employees and valued customers from fraudulent sites and malware, and related Web site threats, intelligence-led security monitoring platforms use advanced automation to continuously scan more than 150 million sites, testing for safety risks including browser exploits, malware and fraud schemes. Each site is rigorously evaluated and assigned a "site safety index" rating that can be used directly in browsing software and Web applications to alert users to online dangers before they visit dangerous sites. The safety index covers such risks as browser hijacks, auto-redirects, auto-downloads, dangerous affiliations, history of fraud, malware and objectionable content. Automated technology continually monitors and tracks the evolution of fraudulent sites and malware across the global Internet, looking for threats that can adversely impact the customer experience. By safeguarding the customer surfing experience, the intelligence-led approach protects customer trust and online revenue streams while reducing help desk calls.


**A leading online service provider bundles URL-based intelligence directly into its browsing software to proactively warn Web surfers before they visit potentially damaging sites.**

**Data vs. Information vs. Intelligence**

*The days of confusing secrets with intelligence are over. The new craft of intelligence carefully distinguishes between data, which is the raw text, image or signal; information, which is collated data of generic interest and generally broadcast; and intelligence, which is information that has been deliberately discovered, discriminated, distilled and delivered to meet a specific decision-making requirement. Intelligence is defined by the end product, not by the source mix.*

– **The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats** (U.S. Army War College Report, 2002)



Cyveillance®

## Phishing

Phishing has rapidly grown to become one of the most prevalent and profoundly damaging online threats. Typically, users receive an e-mail that directs them to a fraudulent Web destination that masquerades as a legitimate business where login details, account numbers and passwords are stolen. Phishing allows blackhats and criminals to take advantage of the trust that customers place in brands. The cost of phishing is seen in fraud-related losses, decreased revenues and damaged customer trust.


To protect users from phishing, automated technology can scan spam e-mail, domain registrations and the Web for sites that exhibit suspicious and malicious behavior. When phishing sites are detected, they are distributed to large Internet service providers that block surfer access to the dangerous sites. By using automated intelligence gathering to detect and mitigate phishing attacks, the intelligence-led solution safeguards customer interactions. Ultimately, consumer trust in the security of online applications is vital to businesses that count on the tremendous cost savings that online self-service applications provide.


**A major bank embraced intelligence-led security to quickly mitigate phishing attacks against its customers and make itself a harder target in an effort to discourage future phishing attacks.**

## Identity theft

Data breaches, phishing attacks, malware, and many other forms of fraud result in large volumes of personally identifiable information making its way to the open Internet. Every day, thousands of personal credentials, in the form of credit cards, social security numbers and more, are collected, traded and sold on hidden areas of the Internet. Once the information is compromised, it is only a few clicks away from fraud or identity theft. The cost to banks and online merchants is staggering, as much of this data ends up being used for fraudulent transactions. The cost to consumers is equally devastating, as identity theft results in damaged credit and huge hassles.


In response to the growth of identify theft and related offline and online exploits, the intelligence-led approach uses automation to discover and report on stolen identity data on a global basis. Automated intelligence gathering locates millions of compromised credentials and personal details that are made available to banks, merchants and OEM partners through real-time data feeds. Identity theft intelligence can alert e-commerce vendors to high-risk transactions, which stops fraud and related financial losses before they occur. Intelligence-led solutions can also protect online vendors against fraudulent credit applications that involve stolen identities and financial histories. The captured and analyzed identity data can also be fed to customers themselves to alert them to the fact that their identities may be compromised online, which is an important aspect of protecting consumer trust.

**"The ultimate objective of intelligence is to enable action to be optimized."**

– Dr. R. V. Jones
Chief
British Scientific Intelligence
World War II

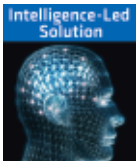


Cyveillance®


**A large retailer that issues its own branded credit cards integrated an intelligence-led approach into its existing anti-fraud practices to reduce fraud-related losses and protect its customers. After using this intelligence-led approach, the retailer found that its average fraud savings was more than $4,500 per account.**

## Counterfeit and gray market products

In addition to malware, phishing and identity theft, customers are threatened by a wide range of counterfeit and gray market products that result in poor product and brand experiences. Fraudulent products are typically substandard and poorly supported, and they can even be dangerous to the health and well-being of consumers. Billions of dollars of revenue are lost each year to counterfeit, stolen and gray market products. The loss of direct revenues is only part of the picture, as can be clearly seen in the recent "counterfeit toothpaste" scare, in which consumers reportedly faced health issues from counterfeit versions of a well-known toothpaste. In this case, the direct loss of revenue from the counterfeit product is only a fraction of the revenue that can be lost when consumers switch to other brands because of doubts placed in their minds by media reports.




To combat product fraud, an intelligence-led approach uses automated information gathering to comprehensively monitor the Web and identify sites selling counterfeit and gray market goods. There are many ways to capture intelligence on counterfeit goods—in the online retail process, on auction sites, in the wholesale and channel management process, and in various discussion forums and online information-sharing venues. Automated intelligence gathering in Web, messaging and spam content can be augmented by human expert analysis, enabling effective detection and tracking of counterfeit goods and fraudulent channels. Intelligence-led methods can ensure profit margins are preserved for a wide range of consumer goods, including luxury items, pharmaceutical products, computers, and other high-ticket items. As a result of intelligence-led alerts, both online and "brick-and-mortar" retailers can protect the customer experience while safeguarding revenue streams and brand equity.


**A major pharmaceutical manufacturer uses intelligence-led security to protect online customers from dangerous counterfeit drugs that are sold via fraudulent Web sites. The approach enables the manufacturer to recapture revenues that would otherwise be lost to the counterfeiters and, more importantly, protects consumers from the potential health risks associated with fake product.**



Cyveillance®

## Unauthorized brand use

Competitors, fraudsters and predators are constantly devising new schemes to leverage corporate brands for their own commercial gain. The unauthorized use of a brand means lost revenue and eroded customer trust.


An intelligence-led approach to brand abuse enables brand holders to identify threats early and stop misuse before significant damage occurs. Continuous scanning of the Web, domain registrations and other online sources can identify many forms of unauthorized brand use, including:

- Cybersquatting – unauthorized brand use within registered domain names
- Typo-piracy – misspelled brand names within registered domain names
- Pay-per-click abuse – search engine ads that contain unauthorized brands and trademarks in the copy
- Traffic diversion schemes – unauthorized use of brands and logos on sites for the purpose of influencing search engine rankings
- Unauthorized associations and claimed relationships – authorized businesses and sites using brands on sites claiming to have a partnership, affiliation or other endorsement

Without the right approach, it's difficult for companies to know how their brand identities, logos, trademarks and intellectual property are being deployed across cyberspace and around the globe. Fortunately, online threats to brands can be identified, tracked and analyzed with automated intelligence-gathering methods that detect both large and small brand use infractions, no matter where they are. Using both text and image recognition, specialized technology can comprehensively monitor the Internet, identifying relevant instances of logos and content misuse.


**A Fortune 500 consumer products manufacturer uses intelligence-led security to comprehensively scan the Web looking for competitors and predators trying to divert customers through unauthorized use of their brand and logos. With the help of intelligence-led security, the manufacturer ensures its customers are not hijacked to the wrong sites, protecting its revenues and the online experience of its customers.**


**A large successful credit information services company uses automated online intelligence gathering to find Web sites set up by competitors to damage its practice with deceptive consumer claims.**



Cyveillance®

## PROTECTING INFORMATION, PHYSICAL ASSETS AND INDIVIDUALS

Intelligence-led security measures are uniquely able to protect revenues and brand assets. But that's only part of the picture. There is another major aspect of intelligence-led security that is creating a major paradigm shift in the area of enterprise information protection. In the extended enterprise era, business processes and workflows are no longer kept safely inside the corporate perimeter—today, data knows no boundaries. With external hackers and internal thieves looking for valuable intellectual property, data protection has become a tremendous challenge for information security professionals and business process owners. Some sources of leaked and stolen data include:

- Statements related to the privacy, confidentiality or security of customer information
- Design plans and technical discussions among employees
- Online or offline leaks of confidential company information and financial data
- Customer identities, personal data and financial transaction records
- Threats against network assets including Denial of Service attacks
- Instructions concerning access to or operation of intranet, extranet and public Web sites

### Protecting confidential information


In today's Internet-centric world, there is a substantial likelihood that stolen, lost or leaked corporate information will show up somewhere on public or hidden online venues. By continuously monitoring and analyzing vast online sources, automated technology can detect and alert the security team to data leaks before they are discovered internally. By monitoring millions of Web sites, chat and discussion sites, blogs, auction sites, search engines, FTP sites, P2P systems and online communications, an intelligence-led security approach provides an early-warning system for information compromise.

In some cases, intelligence-led security can proactively detect online discussions that involve plans for information compromise in the near future. There are documented cases in which advanced intelligence enabled the mitigation of threats to information before damage occurred. Without the intelligence-led approach, it is virtually impossible for companies to track and monitor all the movements of critical and sensitive data. With intelligence-led methods in place, valuable intellectual property, and confidential company and customer data are given proactive 24x7 year-round protection. New, automated technologies can even search for information leaks and theft in a variety of international languages and data formats.



Cyveillance®


**A leading insurance company uses online intelligence gathering to watch for trade secrets, confidential documents, and other intellectual property that may have leaked to the Internet. In one case, it discovered its law firm had inadvertently exposed legal documents through a laptop containing an improperly configured P2P client. Early detection allowed the insurance company to disconnect the laptop from the P2P network before data was downloaded by third parties.**

## Protecting physical assets and employees

Threats to the customer experience and information assets are a large part of the security challenge, but the growing trend towards blended attacks and cascading damages are forcing organizations to converge physical and information security services. The physical aspects of security include the controlled access to buildings, equipment and facilities, as well as protection against:

- Planned boycotts against products and services
- Organized demonstrations that are potentially brand damaging or violent
- Planned activities to interrupt business operations and events
- Smear campaigns and dissemination of misinformation
- Physical threats against employees, corporate officers, facilities and resources
- Solicitations to conspire against the organization


Due to the ubiquitous nature of the Internet, it's possible for intelligence-led security solutions to detect and predict attacks on physical corporate assets, including offices, facilities, traveling employees, conferences and media events. Most activists, extremists and vandals use the Internet to coordinate their activities. Online intelligence gathering can often identify groups that are in the planning stages of their activities.


**A major utility company uses online intelligence gathering as an early-warning system to detect planned demonstrations and actions on the part of extreme activists who could damage corporate property or injure employees.**



Cyveillance®

## INTELLIGENCE-LED COMPLIANCE AND GOVERNANCE

In the current climate of regulation and compliance requirements, security professionals must contribute to compliance. Traditional firewall, VPN, intrusion protection and antivirus technologies do play a role in compliance and vulnerability management, but they are by no means a complete solution. In the fullest sense, compliance and governance must have an awareness of a wide range of threats to company operations and business activities, including visibility into:

- Looming class action or competitive lawsuits
- Breach of attorney-client privileged information
- Violations of company policy in the public domain
- Authorized or public discussion of regulatory compliance issues
- Insider trading, stock manipulation and other securities violations
- References to unreleased financial information
- Premature and unauthorized merger and acquisition disclosures

### Avoiding litigation and fines


Intelligence enables risk management solutions with an expanded perspective that includes a vast range of external threat sources and areas of potential risk exposure. For example, automated intelligence gathering can continuously monitor for large- and small-scale litigations against the organization, including any mentions of planned actions on message boards, search engines, blogs, and various formal and informal news sources. An intelligence-led solution can also analyze and report on references to insider trading and stock manipulation. In cases where employees or partners inadvertently discuss sensitive compliance and regulatory issues online, the intelligence-led approach will capture and archive these threats and report them to security managers who can take immediate actions. As a result of the comprehensive and timely nature of intelligence-led security, potential litigation damage and compliance-related financial penalties can often be reduced or eliminated.


**A leading insurance company used intelligence-led security during the aftermath of a national disaster to detect unscrupulous law firms that were canvassing for participants in a spurious class action suit. Advanced intelligence about the activities of this law firm provided the insurance company with extra time to prepare a response and avoid tremendous legal fees.**

### Ensuring business partner compliance

In the age of the extended enterprise, the activities of partners, franchisees, agents and other affiliates have a tremendous impact on business success and customer trust. But having established, well-documented online channel policies and guidelines is no guarantee of compliance. In fact, 30 percent of business partners regularly violate established polices. These violations negatively impact revenue, increase exposure to business risks, and harm valuable brand equity.



Cyveillance®


Intelligence-led security can continually monitor partner Web sites to ensure they are compliant with business guidelines. This includes appropriate use of logos, presence of competitors, inappropriate deep linking, privacy policy violations and other security risks, such as improperly configured SSL certificates. By proactively detecting and correcting compliance violations, enterprises can optimize financial performance across the extended enterprise and create a consistent customer experience across the Internet.


**A major hotel chain had ongoing problems with franchisees who were openly representing competitive hotel chains, bidding on unauthorized keywords in pay-per-click advertising, and not linking to the corporate reservation system. Through proactive intelligence about the online activities of their business partners, the hotel was able to recapture millions of dollars in revenue and create a consistent customer experience for its customers across all its partner sites.**

## IN CONCLUSION

With today's complex extended enterprises and dynamic consumer buying patterns, it is getting increasingly difficult to compartmentalize threats into isolated security practice areas like information security, physical security and fraud. Today's threats are often blended and can include multiple cascading threat vectors and human engineering aspects. Attacks can originate from partners, external employees, extremists, criminals or hackers anywhere on the Internet. With the combination of advanced automation and highly trained human analysts, the intelligence-led approach is now enabling security teams to make an important paradigm shift towards a more outwardly aware, customer-focused and proactive security posture.

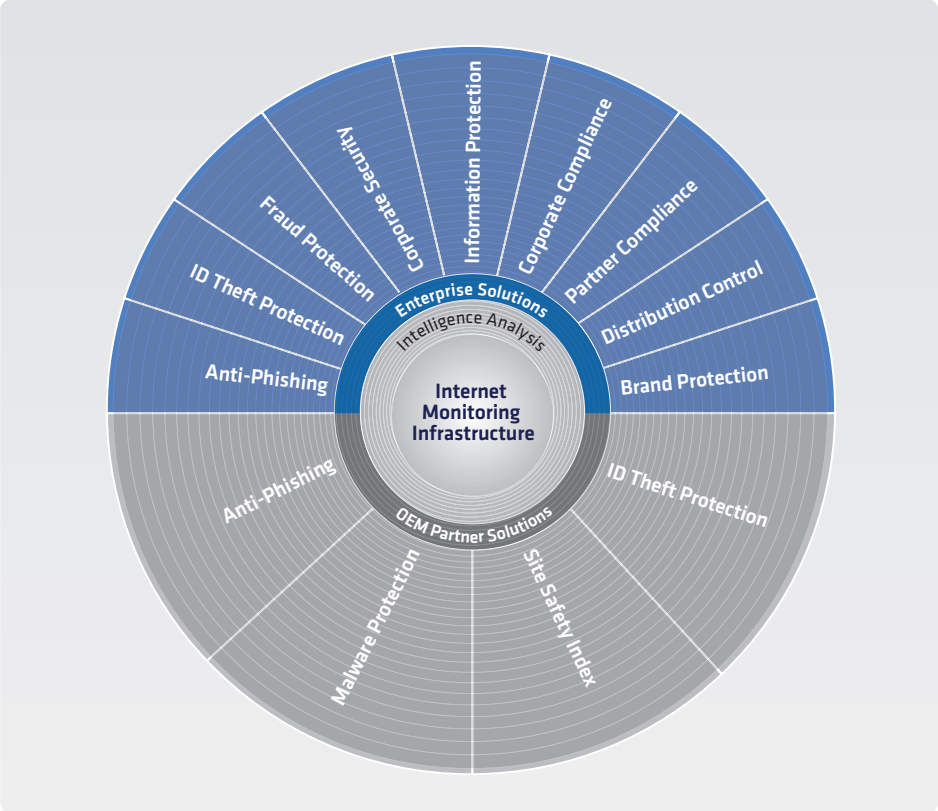
## ABOUT CYVEILLANCE

Cyveillance, the world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals and their interactions, enabling its customers to preserve their reputations, revenues and customer trust. Cyveillance serves the Global 2000 and OEM Partners—protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and service providers that include AOL and Microsoft.

Supported by specialized, proprietary technology and expert human analysts, Cyveillance provides enterprises and OEM partners with real-time cyber intelligence. Cyveillance has developed a proprietary monitoring technology that continuously and rapidly collects information from a vast array of online sources, discovering relevant information from both visible and "hidden" content that would otherwise go undetected.



Cyveillance®




**Cyveillance advantages include:**

- Broad and deep monitoring technology coverage of the visible, hidden, disconnected and transient portions of the Internet
- Proprietary content processing engines are language agnostic and use text, image and behavior-based techniques to identify threats
- Real-time delivery of intelligence through secure customer portals, alerts, data feeds and Web services
- An exceptionally adaptable intelligence platform that easily adapts to address the latest threats
- Highly accurate and relevant intelligence eliminates false positives and non-actionable information
- Online risk experts in all facets of cyber intelligence, security and related disciplines
- Solutions to the broadest set of risks, including:
  - Malware
  - Phishing and pharming
  - Fraud
  - ID theft
  - Threats to executives and facilities
  - Insider threats and information leaks
  - Corporate compliance issues
  - Business partner non-compliance
  - Counterfeit and gray market product distribution
  - Brand abuse and customer diversion

**For more information, please visit www.cyveillance.com.**

Cyveillance enables companies to proactively speed the prevention and mitigation of security risks. Cyveillance intelligence-led security solutions for Enterprise and OEM partners identify, detect and analyze existing and potential threats to infrastructure, information, individuals and interactions.

**Infrastructure**:
- Plants and facilities
- Networks
- Business assets
- Resources

**Information**:
- Intellectual property
- Trade secrets
- Financial information
- M&A plans

**Individuals**:
- Executives
- Customers
- Partners
- Children

**Interactions**:
- E-commerce
- Personal credentials
- Credit cards
- Passwords

**Cyveillance, Inc.**
1555 Wilson Boulevard
Suite 406
Arlington, VA 22209-2405
888.243.0097
www.cyveillance.com
info@cyveillance.com

Cyveillance®