

TECHNOLOGY DATA SHEET

Outbreak Intelligence

Proactive Security

New spyware and viruses continue to appear at a rapid rate, with several thousands of new malware detected each month. Attacks now are more targeted and utilize multiple malware variants, diminishing the likelihood of anti-malware vendors obtaining every new malware sample for signature development. This targeted, saturation approach has circumvented the effectiveness of traditional, reactive security technologies such as signature based malware detection. A new, proactive security approach is needed to protect against the growing number of new, unknown malware threats.

Proactive Security Platform

ScanSafe's Web security applications are powered by Outbreak Intelligence (OI), a proprietary security platform that detects zero-hour and known malware threats. By using a combination of multiple, correlated detection technologies, automated machine-learning heuristics, and the industry's largest Web data set, OI provides the most effective solution against new and known Web malware.

Why Outbreak Intelligence

- Protect your organization against malware without solely depending on signatures
- Detect new malware accurately and avoid false positives
- Scan inbound and outbound Web traffic for malware and malware communications
- Leverage multiple, correlated detection technologies, automated machine-learning heuristics, and the industry's largest Web data set
- Detect up to 15% more malware than signature-based security technologies

For more information, visit www.scansafe.com/why

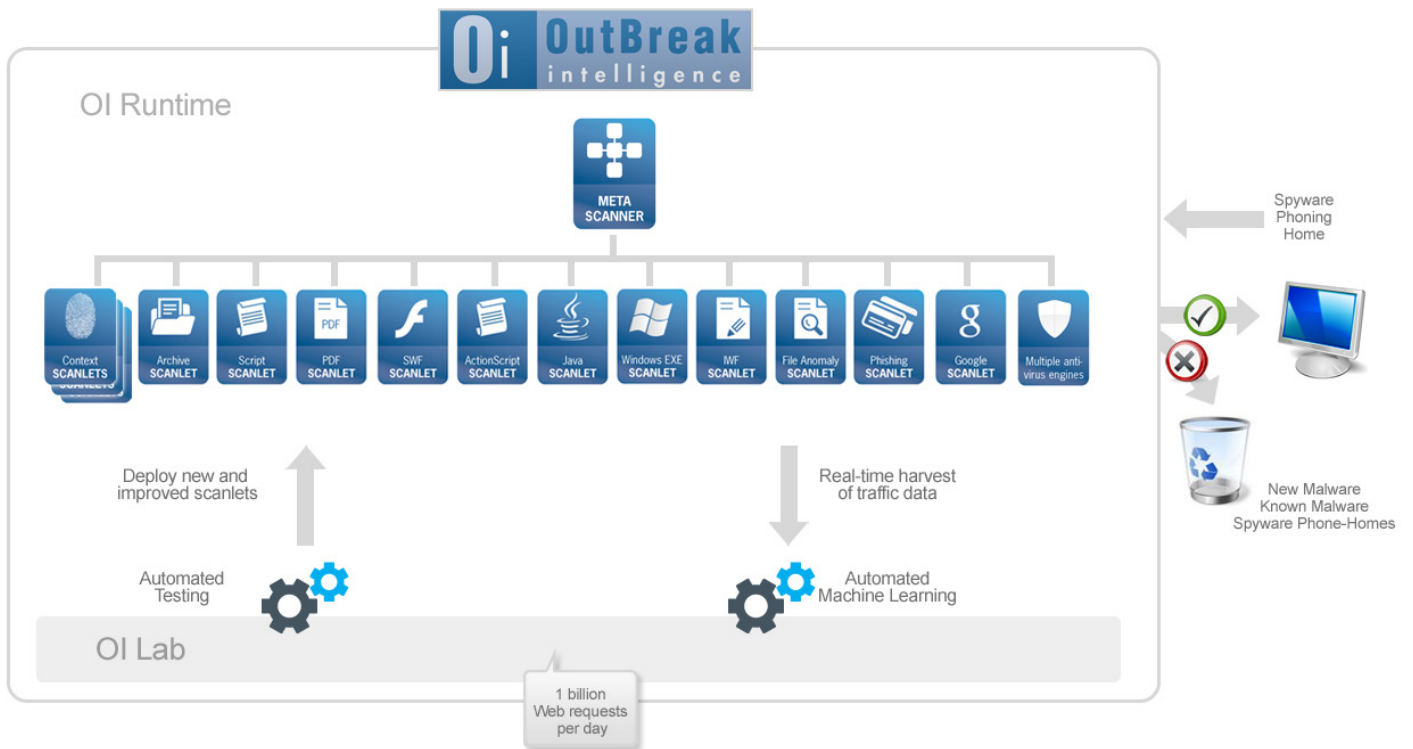


Figure 1: How Outbreak Intelligence works

Detection Technology	Strength	Limitations
Signature <ul style="list-style-type: none"> ▪ Spyware ▪ Viruses 	Reliable identification of known malware	<ul style="list-style-type: none"> ▪ Reactive, cannot identify new, unknown malware ▪ Effectiveness depends on the vendors' possession of malware sample ▪ Library sizes vary ▪ Response times vary
Reputation <ul style="list-style-type: none"> ▪ URL ▪ Code 	Provides historical context for unknown code	<ul style="list-style-type: none"> ▪ Focused on the past, does not consider present behavior ▪ Accuracy depends on heuristic parameters and size of data set
Behavior <ul style="list-style-type: none"> ▪ Traffic ▪ Code 	Provides present context for unknown code	<ul style="list-style-type: none"> ▪ Focused on the present, does not consider historical trends ▪ Accuracy depends on heuristic parameters and size of data set

OI combines signature, reputation, and behavior detection technologies, automated machine-learning heuristics, and a vast Web data set to leverage the strengths of each detection technology, without any of the limitations.

Multiple, Correlated Security Technologies

OI uses multiple signature-based anti-malware scan engines and multiple heuristic detection engines to scan inbound and outbound Web traffic in real time for new and known Web malware.

OI's signature-based scanning detects known Web malware residing on reputable and uncategorized Web pages. Signature detection utilizes multiple, industry-leading anti-malware scan engines, covers all known spyware and viruses, updates hourly and immediately in emergencies, receives new signatures within two hours of new malware detection, and is supported by 24/7 global malware research conducted by the world's largest malware laboratories and collection networks.

ScanSafe's proprietary heuristic engines utilize non-signature detection techniques and automated machine-learning technologies to dynamically generate several thousand fine-grained heuristic parameters that reach beyond the scope of security researchers' prior knowledge of malware. As a result, OI heuristic engines detect up to 15% more malware than reactive signature-based detection.

The URL reputation engine assesses the reputation of a Web page by examining parameters such as IP address information, country of the Web server, history and age of the URL, domain registration information, network owner information, traffic rank of the Web site, URL categorization information, and types of content present.

OI's traffic behavior engine analyzes network traffic patterns to identify suspicious, atypical traffic which would suggest malicious code exploiting a vulnerability or malware communications, for example, from an infected notebook computer to a botnet command-and-control computer.

A code behavior engine determines the behavior of the code by modeling program logic, behavioral rules, and contextual parameters that taken together would suggest good or bad intentions.

The OI code reputation engine examines the Web code itself to determine if it is unusual and possibly malicious. It compares information such as type of code, history and age of the code, frequency of the code, file structure/header/content patterns, and program logic patterns, to code that is known to be good or bad in ScanSafe's massive Web data set. This engine is especially effective for flagging new code that differs from the universe of known good code. The multiple detection engines give their assessments of the code, and these assessments are then combined to produce a comprehensive view of whether or not the new code is malicious.

Industry's Largest Web Data Set

Any non-signature malware detection technology is only as effective as the size of the data set it processes. By leveraging its unique position at the Internet level, OI has unmatched visibility of global Web data and emerging malware threats. OI analyzes several terabytes of Web code each day and has compiled a proprietary Web data set that goes back to 2004. This vast Web data set, unique in the industry, ensures that OI is the most accurate proactive malware security solution available.

Proactively Stopping Malware

Period of Vulnerability:	28 days
Zero-Hour Exploit:	Vulnerability in the way Windows handles Windows Metafile (WMF) image files.
Malware:	Trojan horses, backdoors, and other malware embedded in images.
Distribution:	Images posted on a wide variety of Web pages, including the customer support discussion forum of a major technology manufacturer and other reputable Web sites; email/Webmail; and IM.
Result:	OI's multiple heuristic engines detected the zero-hour malware programs before signatures were available and proactively protected the 15% of ScanSafe's customers that were attacked.

About ScanSafe SaaS Solutions

ScanSafe is the pioneer and largest global provider of SaaS Web Security, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep malware off corporate networks and allow businesses to control and secure the use of the Web. As a SaaS solution, ScanSafe eliminates the burden of purchasing and maintaining infrastructure in-house, significantly lowering the total cost of ownership. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe processes billions of Web requests each month for thousands of enterprise customers.

In 2009, the company was awarded "Best Content Security" solution by SC Magazine Europe for the third consecutive year.

For more information, visit www.scansafe.com

ScanSafe US - 950 Elm Avenue, San Bruno, CA 94066 Tel: +1 650 989 7100 Fax: +1 650 989 6543 Email: ussales@scansafe.com

ScanSafe EMEA - Qube, 90 Whitfield St, London, W1T 4EZ Tel: +44 (0) 20 7034 9300 Fax: +44 (0) 20 7034 9301 Email: emeasales@scansafe.com

