

Huntsman intelligent threat prevention

WebDefense and MailControl

Huntsman provides vital protection against zero-day threats that exploit the window of exposure inherent with signature-based anti-virus products. Huntsman, an integral component of SurfControl's on-demand Web and e-mail security solutions, has never let a zero-day threat reach a customer.

The threat of new viruses, trojans, spyware and other malware is accelerating and putting organizations more at risk than ever before, and Gartner estimates the average clean-up cost to be over \$100,000 for a company of 500 employees.

The reason for the continuing threat from malware is that its authors are highly skilled in creating new or 'zero-day' threats that exploit the 'window of exposure'; the time between a new threat being released and the availability of effective protection from a traditional anti-virus vendor. The window of exposure can be anything from a few hours to weeks depending on how serious the anti-virus vendor perceives the threat to be.

How malware writers exploit the window of exposure

Malware writers have access to botnets - vast networks of compromised systems that can propagate large-scale e-mail attacks incredibly quickly, enabling them to spread malware to a wide audience during the window of exposure.

Additional attack vectors are also being employed to evade traditional defenses. Blended threats, such as an e-mail containing a URL that takes users to a website where malware is automatically downloaded, is an increasingly popular method.

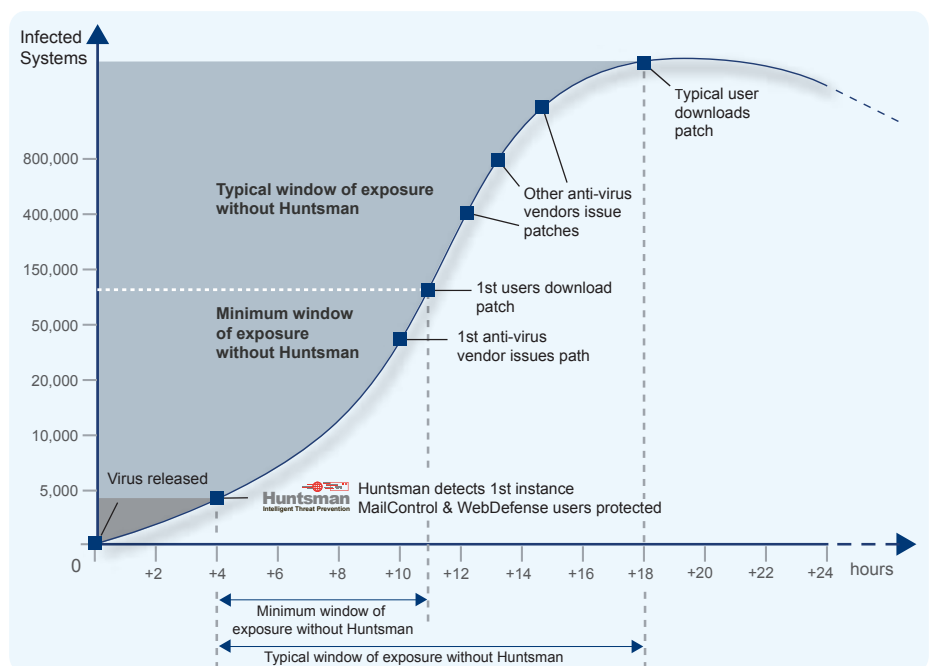
By writing multiple variants of a new piece of malware and releasing them simultaneously or within a short period of time, malware writers force anti-virus vendors to issue multiple updates which consume resources, slow update releases and lengthen the window of exposure.

The final blow for established signature-based anti-virus solutions is that malware writers test their new creations against all the major anti-virus products so that when they release them into the wild they know that they will successfully infect many systems.

How an organization can protect itself

Huntsman is a new breed of heuristics-based intelligent threat prevention technology. It is one of the threat filters in SurfControl's on-demand e-mail and Web security services alongside traditional anti-virus engines and human threat analysis.

Huntsman blocks zero-day threats and closes the window of exposure. Since its launch in 2003 Huntsman has blocked millions of e-mails containing a threat that was not blocked by any of the three commercial anti-virus engines that our services also use. To date, Huntsman has never let a zero-day threat reach a customer.



Huntsman has delivered this perfect record for three main reasons:

- It is exceptionally good at identifying zero-day threats
- Defenses are updated immediately upon detection of the first appearance of a threat
- Malware writers cannot test their new creations against Huntsman prior to releasing them

Huntsman identifies zero-day threats

Huntsman is an integral component of SurfControl's on-demand security solutions. As such it has access to additional threat data contained in the e-mail itself and Huntsman analyzes every e-mail with a battery of tests including:

■ Payload analysis

The size and type of an attachment is a good indicator of a present threat. For example small .exe files or small .zip files containing a single executable file are usually viruses.

■ Context analysis

The structure of the e-mail is examined: anomalies such as forged headers or obfuscated attachment file names are characteristic of a threat-laden e-mail. The e-mail delivery also carries important data; if it originates from a poor reputation sender or a consumer DUL (Dial Up Link) then there is a strong chance that a compromised system is the source. Huntsman performs pro-active checking such as attempting to connect back with the sender of a suspicious e-mail.

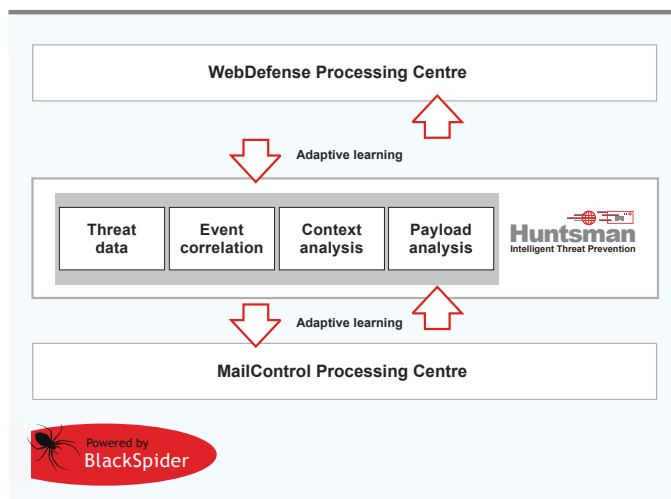
■ Event correlation

Co-ordinated attacks can be easily identified by examining patterns of events. Examples include polymorphic viruses that appear with different payloads or in different e-mails. Analyzing activities such as the rate of e-mail arrival, or presence in different attack vectors - i.e. Web and e-mail give a holistic view of an attack, and the data required to block it.

■ Threat data volume

The success of contextual and correlation analytics is largely dependent on the data available for analysis. Huntsman analyses over 20 million e-mails and 1 million unique MTA connections every day, across all customers, in its search for zero-day threats.

Huntsman intelligent threat prevention



Cannot be evaded by malware writers

Huntsman has 'private' heuristics, it cannot be purchased and tested in isolation. This means that a malware writer cannot author a threat and test it against Huntsman prior to release. Today's well resourced malware writers purchase all major anti-virus solutions and test their new malware against them to ensure they will not be blocked until an update is issued.

Huntsman delivers instant cross-service zero-day threat protection

Huntsman operates in real-time. From the first instance when a new threat is identified, defenses are updated and the entire customer network, across Web and e-mail services is protected.

Why Huntsman cannot be matched by product heuristics

Some signature-based anti-virus products have claimed heuristic capabilities. However these have limitations both in their ability to detect new threats and to quickly and effectively update threat defenses. They are deficient compared to Huntsman for the following reasons:

■ Public heuristics

Product heuristics are 'public', i.e. they can be purchased and new malware tested against them to ensure they will not be blocked.

■ Speed of protection

Product heuristics relies on threat data to be captured by products installed in customer networks, uploaded to the vendor, analysis to be performed and updated threat prevention data to be downloaded to the customer installation. This introduces delays and is dependent on all these processes being successfully executed.

■ Cross-service protection

No product (or other service) offers the real-time, cross-service protection of Huntsman.

■ Context and event correlation

Product heuristics only analyze the threat payload, they have no capability to analyze the delivery mechanism such as the e-mail structure and delivery characteristics.

■ Volume of threat data

Product solutions (and some on-demand services as well) drop many e-mails at the connection level to save bandwidth and maintain performance – they learn nothing from the threat data.

Management of e-mails blocked by Huntsman

E-mails blocked by Huntsman are quarantined alongside those blocked by the anti-virus engines. The same management capabilities exist – notifications can be issued and an administrator can examine and, if necessary, release the e-mail.

Benefits of Huntsman

- 100% record in blocking zero-day threats
- Protects MailControl and WebDefense services
- Protects from first appearance of a new threat

Example of Huntsman zero-day threat capture record - March 2006

This table shows that Huntsman blocked over 42,000 e-mails which had passed through the 3 commercial anti-virus engines used in the MailControl service. After passing the blocked e-mails back through the anti-virus engines they were identified as carrying a virus, trojan, spyware or other malware. The window of exposure is the time between Huntsman blocking the first example of a threat and it being identified by the first updated anti-virus engine.

Virus name	Instances stopped by Huntsman	Window of exposure closed
Trojan-Downloader.Win32.Small.cnk	15,624	8.5 hours
Trojan-Downloader.Win32.Agent.abb	11,657	5 hours
Trojan-Downloader.Win32.Agent.adu	5,168	2.8 hours
Trojan-Downloader.Win32.Small.coc	3,646	3 hours
PWSteal.Tarno.T	3,484	3.1 hours
Trojan-Dropper.Win32.Small.anc	3,005	2.4 hours
Others	271	Average 32 hours
Total	42,855	

Key benefits of SurfControl's on-demand Web and e-mail security solutions: WebDefense and MailControl

Huntsman's intelligent threat prevention technology is integral to SurfControl's on-demand Web and e-mail protection solutions that deliver effective threat protection with an overall lower total cost of ownership.

✓ WebDefense




- Protects against Web-based threats including viruses, trojans, worms and phishing attacks
- Prevents lost productivity through unauthorized or excessive employee Web usage
- Safeguards employees from illegal or inappropriate Web content
- Protects webmail from malware threats
- Reduces legal liability of having illegal content in your network
- Reduces IT costs by optimizing network bandwidth availability
- Easy, flexible and low cost deployment with no hardware or software required and minimal integration
- Single point of policy enforcement for multiple sites and roaming users with no single point of failure
- Minimized total cost of ownership

✓ MailControl

- E-mail threats are blocked at the Internet level – away from your network
- Huntsman intelligent threat prevention technology analyzes all e-mail to identify new threats in real-time and update defenses to close the window of exposure
- Easy, flexible and low cost deployment with minimal integration
- Multiple anti-virus engines for industry best practice
- Real-time global updating of e-mail security policies
- Single solution for multiple sites with no single point of failure
- Highly available architecture ensures continuity of e-mail services
- E-mail disaster recovery – e-mails are queued if the customer's mail server is not available

SurfControl - Raising the level of protection

SurfControl's global reach, financial strength and dedicated focus on providing Internet and e-mail security solutions positions us as *the* trusted security partner with our customers. We have been providing secure content management solutions since 1997 and we have many thousands of satisfied clients across the world. This allows us to build future solutions based on the known demands of our customer base.

	Web Protection	E-mail Protection	Endpoint Protection
 <p>On-Demand</p>	✓	✓	
 <p>Network Appliances & Software</p>	✓	✓	
 <p>Desktop/Laptop</p>	✓		✓



No obligation proof of concept

Discover immediate protection from e-mail and Web threats, risk-free.

www.surfcontrol.com