

# CounterStorm-1™

## THE MOST EFFECTIVE DEFENSE AGAINST KNOWN, ZERO-DAY AND TARGETED ATTACKS

### DANGEROUS THREATS TO YOUR BOTTOM LINE

Known, zero-day and targeted attacks are among the most common, destructive and expensive threats facing today's corporations.

- **Known attacks** have long plagued corporate networks, requiring frequent and complicated security patches that are quickly outdated.
- **Zero-day attacks** present a new and particularly serious threat. Developed specifically to exploit software vulnerabilities before patches are available, zero-day attacks are not recognized by traditional security products: they enter your network undetected, giving you absolutely no time to prepare your defense.
- **Targeted attacks** are aimed at specific industries or companies. These exploits may be based on insider information and come from within an organization's network interior. This customization makes targeted attacks almost impossible to detect with traditional security products and means waiting even longer for vendor-supplied fixes.

### The Gathering Storm

And the challenge continues to grow. Attacks are increasing in speed, frequency and sophistication as well as severity. Industry analysts predict that 1% of future worm attacks will result in 35% of all worm-related damage.

### CounterStorm-1 Stops Attacks in Seconds

CounterStorm-1 is an advanced network security appliance specifically designed to stop zero-day, known and targeted attacks in seconds. CounterStorm-1 employs an integrated suite of sophisticated engines that are uniquely correlated to provide unparalleled accuracy and speed in identifying and automatically stopping the new generation of increasingly destructive attacks. Using patent-pending technology, CounterStorm-1 immediately halts attacks in the network and quarantines compromised machines, preventing widespread, costly damage.

- Highly advanced technologies automatically neutralize attacks within seconds.
- Does not require signatures or patches: recognizes current attacks and automatically adjusts to future threats.
- Highly accurate detection technologies mean no time-consuming false positives.
- Easy to install, deploy and manage across the entire enterprise.

### FEATURES:

#### ADVANCED TECHNOLOGY FOR STOPPING KNOWN, ZERO-DAY AND TARGETED ATTACKS

Based on multiple patent-pending technologies, CounterStorm-1 prevents widespread, costly damage by accurately and automatically detecting and stopping attacks.

#### KEY BENEFITS

**Ensures Business Continuity:** Detects and stops attacks in seconds, allowing for uninterrupted business operation, even during attacks.

**Reduces Network Downtime:** Works in active mode without fear of lost productivity from false positives.

**Lowers IT Costs:** Prevents costly, widespread damage, greatly reducing investigation and clean-up costs.

**Decreases Administrative Burden:** Flexible automated responses and centralized, web-based management saves time and effort by dramatically reducing daily maintenance preparation and monitoring requirements.

**Reinforces Existing Security Infrastructures:** Integrates with and strengthens current network security investments, adding an additional layer of security to high-value and mission-critical information assets.

## COUNTERSTORM-1 FEATURES, CONTINUED

**Accurate Detection**

Combining behavioral attack recognition with a dynamic honeypot and packet and traffic flow anomaly detection, CounterStorm-1 accurately detects attacks for all IP-traffic (e.g., TCP, UDP, ICMP, etc.) without relying on signatures or patches.

**Real-Time Correlation**

CounterStorm-1's sophisticated correlation engine aggregates and validates all attack activity from multiple detection components in real-time, providing instant, accurate and actionable data without disrupting normal business functions.

**Multiple Automated and Manual Response Techniques**

In active mode, CounterStorm-1 stops attacks automatically, providing the fastest and most effective protection against expensive, widespread damage. In addition, CounterStorm-1 offers a flexible manual response mode that can be easily customized for any environment. Both response modes employ the following techniques:

- **Network Switch Integration:** CounterStorm-1 automatically locates the physical port of an infected machine and halts attack propagation by either disabling the port or placing it on a "remediation VLAN" where clean-up can occur without the risk of further damage.
- **Custom Response:** Provides a simple mechanism for creating customized responses to attacks, such as firewall and router ACL rules, and VPN user blocking.
- **Software Blocking:** CounterStorm-1 uses a combination of advanced packet-injection techniques to effectively neutralize attacks.

**WHEN EVERY SECOND COUNTS:**  
Most damage occurs within the first few hours after an attack.

**SECONDS**

vs.

**HOURS**

00:00:08

11:37:24

CounterStorm-1 stops attacks in seconds, preventing widespread infection and costly damage.

Other security products can take hours or days, allowing costly damage to spread throughout the enterprise.

- **Multiple Notification Options:** IT staff members are immediately notified of attack activity via SNMP, syslog, e-mail or pager.

**Easy To Install, Deploy and Manage**

CounterStorm-1 ensures enterprise-wide effectiveness and ease-of-use through a number of convenient, user-friendly features, including:

- **Centralized Enterprise Management:** The CounterStorm-1 Command Center manages a distributed deployment of CounterStorm-1 Sensors to provide an instant, enterprise-wide snapshot of attack and response activity.
- **Intuitive Graphical User Interface:** Easy-to-use, browser-based management interface allows for rapid configuration, real-time monitoring, and historical reporting of attack and response activity.
- **Plug-and-Play Installation:** Appliance installs easily with no network downtime and requires no host-based agents.

**THE PROBLEM BY THE NUMBERS:**

**\$18 billion:** Worldwide damage caused by worms and viruses in 2004, the costliest year on record.

**\$475,000:** Median corporate impact of the 2003 Blaster worm.

**\$130,000:** Average recovery cost per company in 2004 – up 30% from 2003.

**91%:** Organizations reporting that the threat from attacks is getting worse.

**50%:** Increase in attacks from 2003 to 2004.

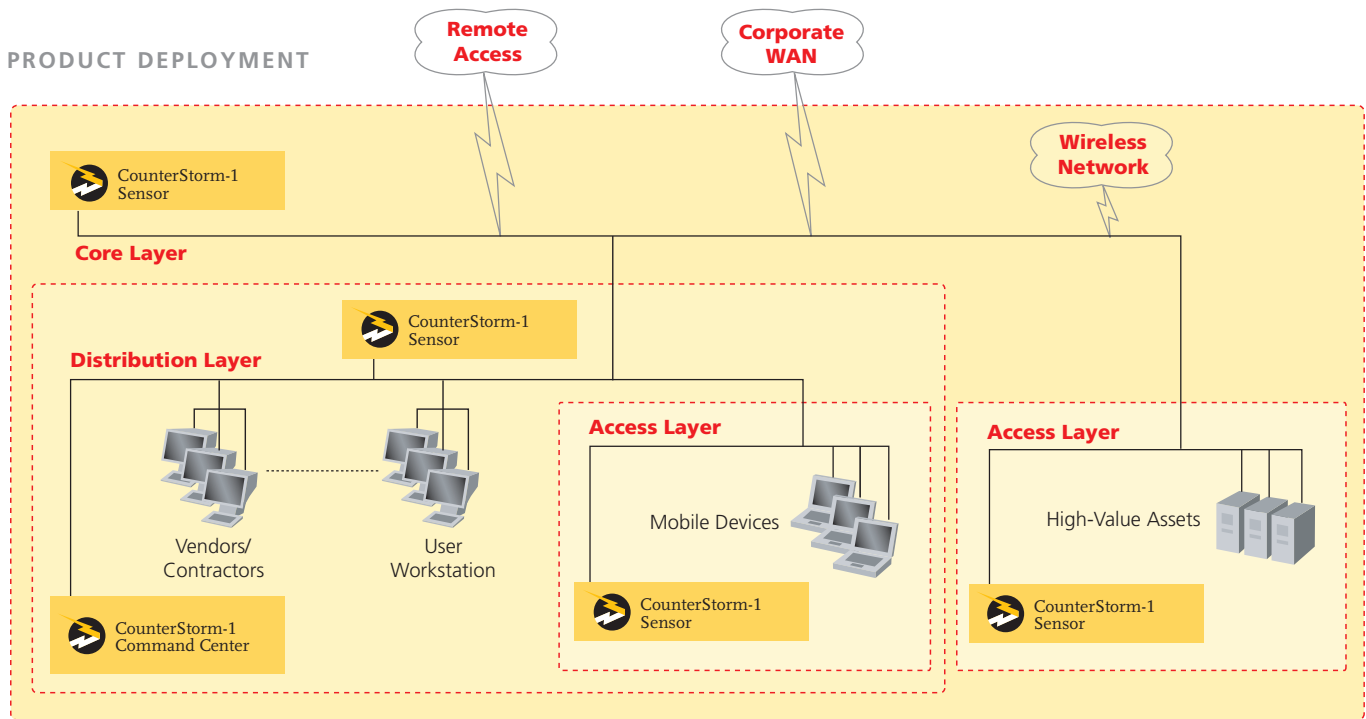
**31:** Average person-days required for full recovery in 2004 – a 30% increase from 2003.

**23 hours:** Average server downtime after an attack in 2004.

Sources: *Virus Prevalence Survey 2004*, ICSA Labs; *Impact of Malicious Code*, May 2005, Computer Economics.

**STOPPING ATTACKS INSTANTLY... ANYWHERE THEY ATTEMPT TO ENTER THE NETWORK**

Worms and other attacks are increasingly damaging networks from an assortment of internal sources, rendering traditional perimeter defenses useless. CounterStorm-1 can be deployed in the network areas where attacks typically occur.



**Protect Your Entire Network**

Organizations can deploy CounterStorm-1 at the core or distribution layers to provide comprehensive, enterprise-wide network protection.

**Internal LAN Segments**

Mobile workers who rely heavily on laptops can inadvertently introduce worms into the network. Vendors and contractors using specially designated network segments are often sources of internal attacks.

**Stop Attacks Originating in High-Risk Areas**

**Remote Access and VPN Users**

Authorized remote access users unwittingly pick up worms outside the corporate network and then release them inside its perimeter.

**Corporate WAN**

Modern enterprise networks are often comprised of disparate business units and peering points that may not have appropriate internal defenses to protect against costly, widespread damage.

**Wireless Network Segments**

The growing integration of wireless capabilities into traditional networks provides another avenue of attack for known, zero-day and targeted exploits.

**Fortify Your Defense of High-Value Assets**

CounterStorm-1 can be deployed to add an additional, focused layer of security to critical network segments, such as those housing important financial applications and sensitive customer data or those that have been targeted by hackers in the past.

**COUNTERSTORM-1: STOPPING KNOWN, ZERO-DAY AND TARGETED ATTACKS... NOW AND IN THE FUTURE**

CounterStorm, Inc. is a network security company that provides immediate defense against known, zero-day and targeted attacks. Based in New York City, CounterStorm has developed its advanced patent-pending technologies under research grants from the Defense Advanced Research Projects Agency (DARPA) and the U.S. Department of Homeland Security. Commercial, government and military installations worldwide rely on CounterStorm products.

To learn more about CounterStorm-1 or to arrange a demonstration, visit [www.counterstorm.com](http://www.counterstorm.com), email us at [info@counterstorm.com](mailto:info@counterstorm.com), or call 212.206.1900.

## WHY LEGACY NETWORK SECURITY TECHNOLOGIES CAN'T DEFEND AGAINST ZERO-DAY AND TARGETED ATTACKS

With worms and other cyber-attacks on the rise, organizations must protect their networks with multiple levels of security. However, even today's most sophisticated security products leave your network vulnerable to zero-day and targeted attacks. CounterStorm-1 reinforces existing network security efforts. By stopping known, zero-day and targeted attacks in seconds, CounterStorm-1 "closes the gaps" left by such security approaches as:

### Network Intrusion Prevention Systems (IPS)

Fundamentally an in-line perimeter defense, IPS cannot prevent or neutralize internal attacks. And because this methodology relies largely on vendor-supplied signatures, your network is defenseless for hours or days until updated signatures are released.

**CounterStorm-1 stops known, zero-day and targeted attacks in seconds without relying on signatures, protecting the network interior and bolstering IPS perimeter protection.**

### Host-Based Systems

Difficult installation, significant maintenance costs, and the need for a unique product for each OS and application within the network environment make host-based solutions expensive and impractical to deploy across an entire network.

**Easy to install and manage, CounterStorm-1 provides affordable network-wide protection and enhances host-based solutions by preventing misconfigured or unprotected hosts from causing widespread damage.**

### Network Behavior Anomaly Detection (NBAD)

By not offering fully automated responses due to a high level of false positives, and failing to recognize attack activity until significant damage has occurred, NBAD solutions leave a serious hole in your network security approach.

**Closing the wide gap left by NBAD solutions, CounterStorm-1's immediate and accurate detection and fully automated responses stop attacks in seconds, preventing costly damage.**

### Patch Management

While it is important to implement sound patch management practices, even the most up-to-date patches cannot protect against zero-day attacks, which, by definition, exploit security vulnerabilities for which patches do not currently exist. As with IPS solutions, your network is defenseless for hours or days until patches are developed, released and deployed.

**When every second counts, CounterStorm-1 stops zero-day and targeted attacks instantly, before widespread damage can occur.**

## TECHNICAL SPECS

CounterStorm-1's hardware platform consists of Sensor and Command Center appliances, both of which are powered by CounterStorm's customized, high-performance operating system that is hardened for security.

CounterStorm-1 Sensor



CounterStorm-1 Command Center



<b>Capacity</b>	100/1,000 Mbps	50 CounterStorm-1 Sensors
<b>Form Factor</b>	1U rack-mountable	2U rack-mountable
<b>Dimensions</b>	17"W x 26.5"D x 1.7"H 14 lbs 6 oz	17"W x 26"D x 3.5"H 19 lbs 11 oz
<b>Power Supply</b>	EPS 12V 400W output with PFC	EPS 12V 400W output with PFC
<b>Redundancy</b>		SCSI RAID5 Redundant power supply
<b>Certification</b>	FCC, UL, CE	FCC, UL, CE