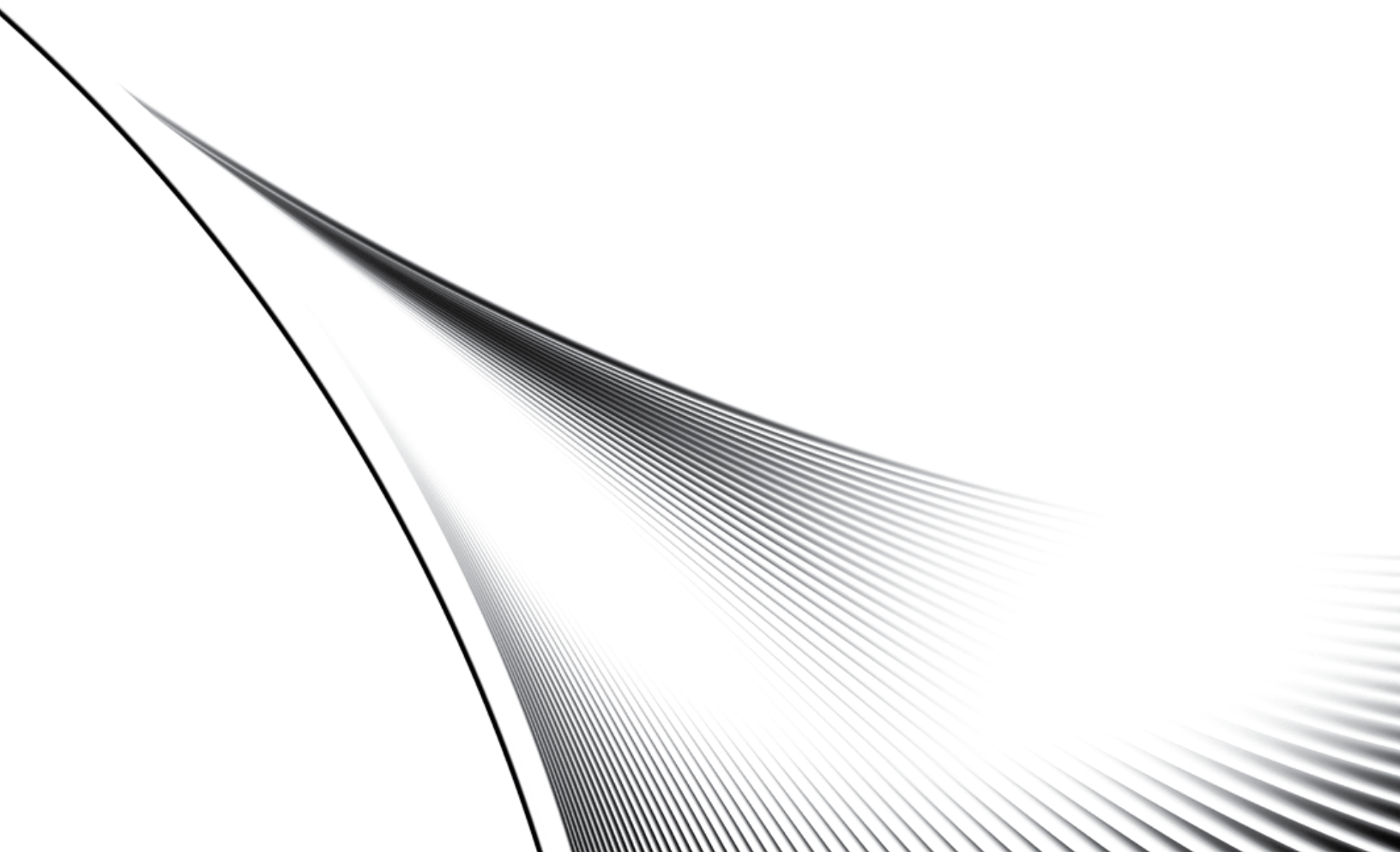




# CounterACT Edge<sup>TM</sup>

## Threat Prevention

Datasheet



# CounterACT Edge delivers an entirely unique approach to preventing network intrusions: Stop attackers based on their “proven intent” to attack.

## How It Works

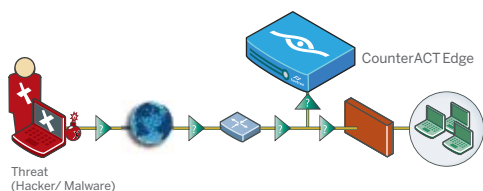
Users or self-propagating threats must gather information on the network’s configuration and vulnerabilities to initiate an attack.

ForeScout’s Active Response™ technology detects this reconnaissance and responds with counterfeit or “marked” information. Any subsequent attempt to use this marked information is proof of malicious intent.

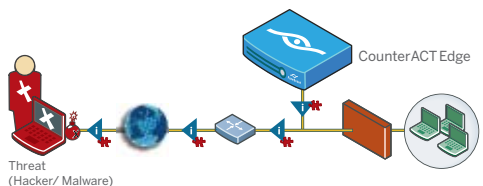
By focusing on proving attacker intent, CounterACT Edge can block attackers before they gain access to the network – without the need for signatures, deep-packet inspection or manual intervention.

Figure 1: Active Response Three-Step Process.

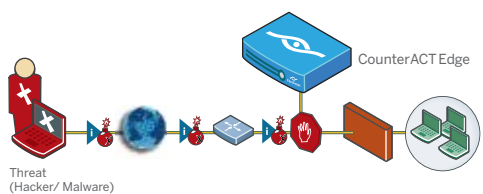
### Step 1 - Monitor for Reconnaissance Activity



### Step 2 - Interact with Reconnaissance Activity



### Step 3 - Prove the Intent of the Attacker and Block the Attack



## Benefits

**Pinpoint Accuracy.** CounterACT Edge stops even the most sophisticated and intelligent attackers. It even identifies “low and slow” scans with long time lags occurring between each scan step, tracks attackers who change IP addresses, and detects attackers who attempt to launch mass attacks at multiple targets.

**Automated Response to Zero-Day Threats.** CounterACT Edge provides an automatic and unparalleled level of protection against “zero-day” threats. Since the CounterACT Edge appliance is not in-line with the switch, there is zero latency and zero points of failure.

**Alerting & Reporting.** CounterACT Edge provides flexible, intuitive alerting and reporting options to ensure that security managers get the information they need, when they need it:

- Geographical Maps. CounterACT Edge features a world map with geographical locations of monitored and/or blocked sources, and offers history reports for any specific point in time or time range.
- Complete Event Documentation and Reporting. CounterACT Edge records all detected malicious activity, enabling security personnel to thoroughly investigate incidents. Comprehensive reports feature current and historical data of CounterACT Edge activity.
- Trend Analysis. CounterACT Edge maintains a historical database of reconnaissance and malicious activity, enabling security managers to pinpoint trends and take the appropriate action.
- E-mail Alerts. Event information is sent based on user-defined parameters.

**Blocking Options.** Blocking behavior can be customized to support corporate security policies (addressing specific attack categories with configurable action duration and alerts).

**Firewall-based Blocking.** CounterACT Edge seamlessly integrates with firewalls to enable immediate containment of active threats in real time. In addition to using its own blocking technique, CounterACT Edge can dynamically configure the firewall by creating rules in real-time.

**Advanced TCP Session Reset.** Unlike conventional TCP resets,

**CounterACT Edge** maintains business continuity during sophisticated attacks and outbreaks of self-propagating malware by detecting and blocking threats before they reach the network.

which are sensitive to timing subtleties, CounterACT Edge TCP resets are activated during the initiation of the TCP session, providing more efficient blocking.

**Exclusion and Inclusion Lists.** CounterACT Edge allows security managers to manually override its identification and blocking mechanisms, in order to exclude pre-defined IPs and/or to permit access from business-critical addresses.

**SNMP Traps & Management.** CounterACT Edge can send SNMP traps about specific attack and operational events to authorized SNMP management stations and supports read-only SNMP-based management. Various communities can be defined, allowing read-only access to different parts of the CounterACT Edge management information database.

**Whols.** CounterACT Edge sends Whols service information on suspected attackers to security staff, including their geographic location, corporate affiliation and contact information.

**Easy Installation.** CounterACT Edge and its Enterprise Manager are easy to install and require little user interaction. Configuration usually takes less than an hour.

**Administration & Granular User Privileges.** The CounterACT Edge Site and Enterprise Managers enable authorized users to configure and control the appliance from authorized locations. Individual users can be authorized to access specific functions, as needed.

**Configurable Detection Settings.** The CounterACT Edge default detection settings can be optionally fine-tuned to reflect the unique characteristics of the network and its surrounding environment

**Monitor/Block Mode Toggle.** CounterACT Edge supports both a Monitor-mode and a Block-mode, allowing the security manager to switch between observation and blocking of malicious traffic.

**Security.** CounterACT Edge provides robust security to ensure that it is well protected against compromise by potential attackers.

Security features include:

- Hardened Linux-based operating system
- Encrypted and authenticated communications between components
- Strictly enforced access control mechanism
- Highly granular user privileges
- Stealth mode operation
- Built-in anti-tampering mechanisms

**Total Cost of Ownership.** CounterACT Edge operates without human intervention or manual updates, which significantly reduces the total cost of ownership.

Figure 2: CounterACT Edge Site and Enterprise Managers display aggregated attack data from around the world.



## CounterACT Edge - Two Configurations

**Site Solution.** The Site solution consists of one CounterACT Edge appliance and protects networks with a single point of connectivity to the Internet.

**Enterprise Solution.** The Enterprise solution consists of multiple CounterACT Edge appliances and the Enterprise Manager and protects networks with multiple points of Internet connectivity.

## CounterACT Edge Enterprise-Only Features

**Enterprise Manager.** CounterACT Edge's Enterprise Manager provides one-to-many communications across CounterACT Edge appliances. It offers a visual overview of CounterACT Edge threat prevention activity, including a geographical representation of the location of potential and actual attackers, their IP addresses, their activities, and the preventive steps that were taken against them. It manages appliance activity and policies, and collects threat information, such as attempts, identification, and prevention. It can also receive threat alerts from an appliance and distribute it to all CounterACT Edge appliances in the enterprise, creating an effective, uniform layer of security at all network entry points.

**Enterprise Alert Hub.** When an attacking source is identified, the Enterprise Manager immediately alerts all CounterACT Edge appliances in the enterprise, providing a high and consistent level of defense across the enterprise's perimeter. Each CounterACT Edge in the enterprise then acts upon the alert according to policy.

**Aggregated Threat Information.** Event information from geographically dispersed CounterACT Edge appliances is consolidated into a single view on the Enterprise Manager. The information includes attacker IP addresses, types of reconnaissance utilized, and the exact time and date of attacks is readily available.

Table 1: CounterACT Edge Platform Specifications.

NOTE: All devices comply with FCC Part 15 of the FCC Rules, Class A; CANADA/USA: CSA 60950 and UL 60950 (Safety); ROHS.

CounterACT Edge 100		CounterACT Edge 1000
Bandwidth	100 Mbps	1 Gbps
VLAN Support	Unlimited	Unlimited
Network Ports	Three copper 10/100/1000Mbps (RJ45)	Three copper 10/100/1000Mbps (RJ45)
I/O Ports	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (RJ45) PS/2 keyboard and mouse port
USB Ports	Three, USB 2.0-compliant	3, USB 2.0-compliant
VGA	1 (DB15)	1 (DB15)
CD-ROM	1	1
Hard Drives	1 HDD	2 HDD (RAID-1)
Power Supply	1 @ up to 400W, 100-240VAC	2 @ up to 650W, 100-240VAC
Temperature		
Operating	+10°C to +35°C (fluctuation not to exceed 10°C per hour)	-10°C to 35°C , derated 0.5°C for every 1000 ft (10,000 ft. max)
Storage	-40°C to +70°C	-40°C to 70°C
Humidity	90%, non-condensing at 35°C	90%, non-condensing at 30°C
Chassis	1U 19" rack mount	1U 19" rack mount
Dimensions	Height: 43.25mm (1.703 inches) Width: 430mm (16.93 inches) Depth: 692mm (27.25 inches)	Height: 43.2mm (1.7 inches) Width: 430mm (16.93 inches) Depth: 654.4mm (25.76 inches)
Shipment	Size: 10 inches x 28 inches x 36 inches Weight: 37 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 54 pounds



ForeScout

10001 N. De Anza Boulevard, Suite 220 . Cupertino, CA 95014  
Tel: 1.866.377.8771 . Fax: 1.408.213.2283 . www.forescout.com

© 2008 ForeScout Technologies, Inc. Products protected by US Patent #6,363,489, March 2002. All rights reserved. ForeScout Technologies, the ForeScout logo, CounterACT, CounterACT Edge and Active Response are trademarks of ForeScout Technologies, Inc. All other trademarks are the property of their respective owners. CE -DS-V001-1108