ForeScout CounterACT Edge

Threat Protection Made Simple

ForeScout CounterACT Edge is a high performance security appliance that protects your network perimeter against intrusion.

Unlike traditional IPS products, ForeScout CounterACT Edge is extremely easy to install and manage. It does not require frequent updates, tuning, or management overhead. It is powerful, and painless.

The Challenge of the Modern Attack

Despite advancements in security controls, organizations are increasingly affected by zero-day exploits, low-and-slow attacks, and targeted attacks (APTs).

Traditional network intrusion prevention systems (IPS) are primarily based on signatures, which are useless against zero-day attacks. Furthermore, most IPS systems are designed with traffic intensity thresholds, which causes them to miss low-and-slow attacks.

A second problem with traditional IPS systems is the fact that they are prone to false positives, in which legitimate business traffic is mistaken for an attack. This wastes valuable IT management time, as the devices need to be tuned and logs need to be constantly analyzed.

In an attempt to detect zero-day attacks, some IPS devices incorporate network behavioral analysis in addition to signatures. However, most network behavioral technologies are so prone to false positives that IT managers are reluctant to use them in blocking mode.

ForeScout CounterACT Edge

Rather than chase the latest threats and develop new signatures to address them, ForeScout offers an effective threat prevention technology called ActiveResponse™. ActiveResponse does not rely on signatures to detect zero-day threats. ActiveResponse does not produce false positives, nor does it require any tuning period or maintenance.

ForeScout CounterACT Edge is a high performance security appliance that uses ActiveResponse to protect your network against intrusion and attack. Unlike traditional IPS products, CounterACT Edge is extremely easy to install and requires approximately zero management overhead. CounterACT Edge is:

» **Accurate:** does not block legitimate traffic

» **Powerful:** stops intelligent attackers and zero-day attacks

» **Easy to install:** plug it in, configure and walk away.

» **Easy to maintain:** no signatures, tuning or maintenance.

ForeScout
Access ability.

Features

Preempt zero-day attacks. CounterACT Edge will detect and block any attack that goes over the network and relies on reconnaissance to identify possible targets (which almost all zero-day attacks do). CounterACT Edge blocked Zeus and Stuxnet on day-zero, before any security company anywhere had developed a signature for these attacks.

Suppress propagating worms. CounterACT Edge is effective against even hard-to-stop worms such as the infamous Conficker. Traditional IPS and antivirus systems had trouble blocking Conficker, but CounterACT Edge was able to block Conficker with extreme efficiency and accuracy.

Stop low-and-slow attacks. Unlike traditional IPS systems which have a time-out period built into their attack signatures, CounterACT Edge has no time-out period. It doesn't need one. And that allows it to be effective against the low-and-slow attacker—someone who is just looking for one folder, one credit card number, or one social security number.

ActiveResponse technology. ForeScout CounterACT Edge uses ForeScout's patented ActiveResponse technology to detect and stop attacks without any need for signatures, anomaly detection or pattern matching.

100% accuracy. ForeScout CounterACT Edge communicates with external entities during the reconnaissance phase of an attack. This allows CounterACT Edge to identify the subsequent attack with 100% accuracy—zero false positives. This fact allows you to comfortably put the product into blocking mode and walk away from it. It is truly "set and forget."

Multiple blocking modes. ForeScout CounterACT Edge provides multiple ways of blocking attacks. The primary blocking mode utilizes an advanced TCP session reset. Unlike conventional TCP resets, which are sensitive to timing subtleties, CounterACT Edge TCP resets are activated during the initiation of the TCP session, providing more efficient blocking. Other blocking modes include tarpit blocking, UDP blocking, and firewall ACL integration.

Firewall integration. CounterACT Edge seamlessly integrates with firewalls to enable immediate containment of active threats in real time.

Easy to install. You plug it in, configure it (usually in less than an hour), and walk away. ForeScout CounterACT Edge begins protecting your network immediately with 100% accuracy. No lengthy tuning period.

How ForeScout CounterACT Edge Works

ForeScout CounterACT Edge deploys outside your firewall to protect against incoming attacks. It is connected to a switch via a mirror port. It installs out of band, not in-line with traffic. There is no "bump in the wire", no latency, no single point of failure.

Use Cases #1: Primary IPS

ForeScout CounterACT Edge can be used as a primary IPS system in front of your existing network firewall. The amount of time that you will spend planning, installing, and managing your network defenses will be lower than with any other product combination. CounterACT Edge is effective against both human and automated attack patterns, including zero-day and "low and slow" attacks.

BEFORE   AFTER

CounterACT Edge

Typical IPS   20268   Typical IPS   00012

Events   Events

DMZ   DMZ
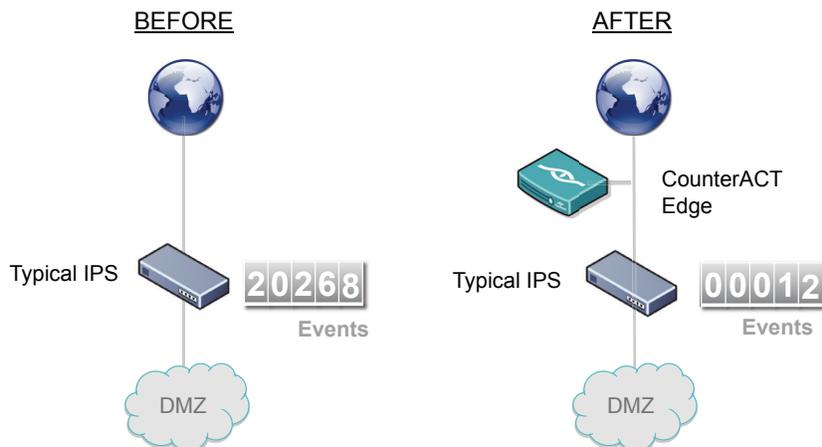
Use Cases #2: Secondary IPS

ForeScout CounterACT Edge can be used in front of your existing signature-based IPS to save you time and money. In this configuration, CounterACT Edge will greatly reduce the number of events that your signature-based IPS system needs to process; this can extend the life of your existing hardware if it is nearing its capacity limit. It will also reduce your administrative overhead because you will have fewer events that you need to monitor and analyze. CounterACT Edge operates with 100% accuracy, so the events (attacks) that CounterACT Edge blocks do not need to be reviewed by a human. CounterACT Edge filters out the noise, leaving traditional IPS devices to deal with a small number of other attacks.

The amount of time and money that you can save depends on many factors. Only a trial in your actual environment can tell you for sure what your savings will be. The figure below is for illustration purposes only.

How ActiveResponse Works

The first step of a network attack is almost always reconnaissance. In this step, an attacker (either human or automated) gathers information about the network's configuration and vulnerabilities. ForeScout ActiveResponse detects this reconnaissance.

CounterACT Edge

Threat
(Hacker/ Malware)
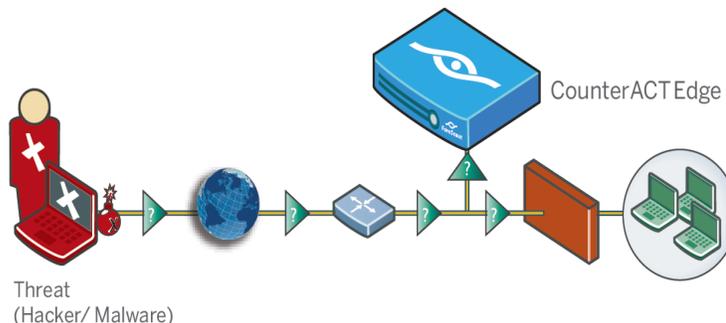
In step 2, ForeScout ActiveResponse responds with counterfeit or "marked" information. This response is not distinguishable from a network's legitimate response. It will look similar to what the source is expecting to receive from the real network.

Threat
(Hacker/ Malware)
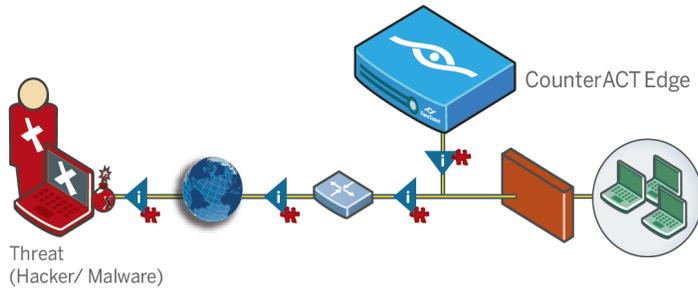
In step 3, the attacker tries to use the marked information to attack the network. This is proof of malicious intent. There is no legitimate reason for machines (or users) on the network to scan for resources, receive fake targets, and then try to access them.

Threat
(Hacker/ Malware)
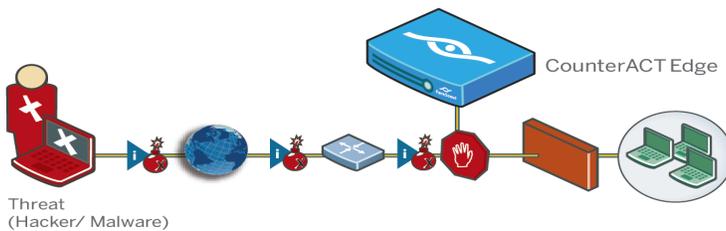
In this way, ActiveResponse can determine with confidence that this source has malicious intent and needs to be blocked. By focusing on attacker intent, ActiveResponse can block the attack without the need for signatures, deep-packet inspection or manual intervention. It's brilliant. And it's patented.

The ForeScout Difference

IT managers should evaluate network security products both in terms of their effectiveness (how accurate is it? does it block zero-day attacks?) as well as their management and operational costs.

Real-world experience and test results from independent labs show that signature-based and statistical anomaly-based IPS products on the market today do not deliver an attractive scorecard on either effectiveness or cost. Their weaknesses can leave organizations vulnerable to threats such as zero-day attacks, and severely challenged by problems such as false positives and high management costs. The cost of managing an IPS system that requires frequent tuning and signature updates can be multiple times the cost of procuring such a system.

ForeScout CounterACT Edge is an effective layer of network security which costs very little. CounterACT Edge blocks zero-day attacks without producing false positives. It is a true "set-and-forget" solution that does not require costly management and oversight.

CounterACT Edge Based on ActiveResponse™ Technology	Signature/Anomaly Detection Based on signature and heuristics
✔ Zero-Day prevention	✖ Delayed prevention
✔ Out-of-band	✖ Inline (point of failure and delay)
✔ Set and forget	✖ Significant management overhead
✔ Unprecedented accuracy	✖ False positives

Easy to maintain. CounterACT Edge needs no signatures, no updates, no tuning, no maintenance. Forever.

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.

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

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

Enterprise Manager. Organizations that require multilpe CounterACT Edge appliances can manage them all from one central consoule using ForeScout CounterACT Edge Enterprise Manager. This product provides 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. Event information from geographically dispersed CounterACT Edge appliances is consolidated into a single view on the Enterprise Manager.

Administration 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.

About ForeScout

ForeScout Technologies is a leading provider of automated security control solutions for Global 1000 enterprises and government organizations. With ForeScout, organizations can accelerate productivity and connectivity by enabling people to access corporate network resources where, how and when needed without compromising security.

ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. ForeScout CounterACT has been chosen by over 1300 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. The company delivers its solutions through its network of authorized partners worldwide

Scalable Models

ForeScout CounterACT Edge is sold as an appliance. Six models are available, as shown below.

MODEL	SC-2	SC-10	SC-50	SC-100	SC-200	SC-1000
Bandwidth	2 Mbps	10 Mbps	50 Mbps	100 Mbps	200 Mbps	1 Gpbs
Network Ports copper fiber	6 Available option (Up to 2 total)	6 Available option (Up to 2 total)	6 Available option (Up to 2 total)	6 Available option (Up to 2 total)	8 Available option (Up to 4 total)	8 Available option (Up to 4 total)
I/O Support	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (DB9); PS/2 keyboard and mouse port	1 serial port (DB9); PS/2 keyboard and mouse port
USB Ports	3, USB 2.0 compliant	3, USB 2.0 compliant	3, USB 2.0 compliant	3, USB 2.0 compliant	2, USB 2.0 compliant	2, USB 2.0 compliant
VGA	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)
CD-ROM	N/A	1	1	1	1	1
Hard Drives	3 HDD (RAID-1)	3 HDD (RAID-1)	3 HDD (RAID-1)	3 HDD (RAID-1)	3 HDD (RAID-1)	3 HDD (RAID-1)
Power Supply	1 @ up to 620W, 100-240VAC	1 @ up to 620W, 100-240VAC	1 @ up to 620W, 100-240VAC	1 @ up to 620W, 100-240VAC	2 @ up to 650W, 100-240VAC	2 @ up to 650W, 100-240VAC
Power Consumption	313W	313W	313W	313W	335W	335W
Temperature Operating Storage	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃	-10℃ to +35℃ (fluctuation not to exceed 10℃ per hour) -40℃ to +70℃
Humidity	90%, non-condensing at 35℃ (non-operating)	90%, non-condensing at 35℃ (non-operating)	90%, non-condensing at 35℃ (non-operating)	90%, non-condensing at 35℃ (non-operating)	90%, non-condensing at 35℃ (non-operating)	90%, non-condensing at 35℃ (non-operating)
Chassis	1U 19" rack mount	1U 19" rack mount	1U 19" rack mount	1U 19" rack mount	2U 19" rack mount	2U 19" rack mount
Dimensions	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 692mm (27.25 inches)	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 692mm (27.25 inches)	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 692mm (27.25 inches)	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 692mm (27.25 inches)	Height: 87.30mm (3.44 inches) Width: 430mm (16.93 inches) Depth: 704.8mm (25.75 inches	Height: 87.30mm (3.44 inches) Width: 430mm (16.93 inches) Depth: 704.8mm (25.75 inches
Shipment	Size: 10 inches x 28 inches x 36 inches Weight: 54 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 54 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 54 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 54 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 68 pounds	Size: 10 inches x 28 inches x 36 inches Weight: 68 pounds