

ForeScout Technologies' ActiveScout: The unknown-attack solution for SmartDefense users

SmartDefense™ leverages Check Point's™ powerful Stateful Inspection technology to protect your network against a broad range of attacks, including IP- and DNS-based attacks, DOS, and Internet worms such as Nimda and Code Red. And now you can gain an added level of protection against the next wave of malicious, as-yet-undocumented exploits with ForeScout Technologies' OPSEC-certified ActiveScout.

ForeScout's ActiveScout offers SmartDefense users:

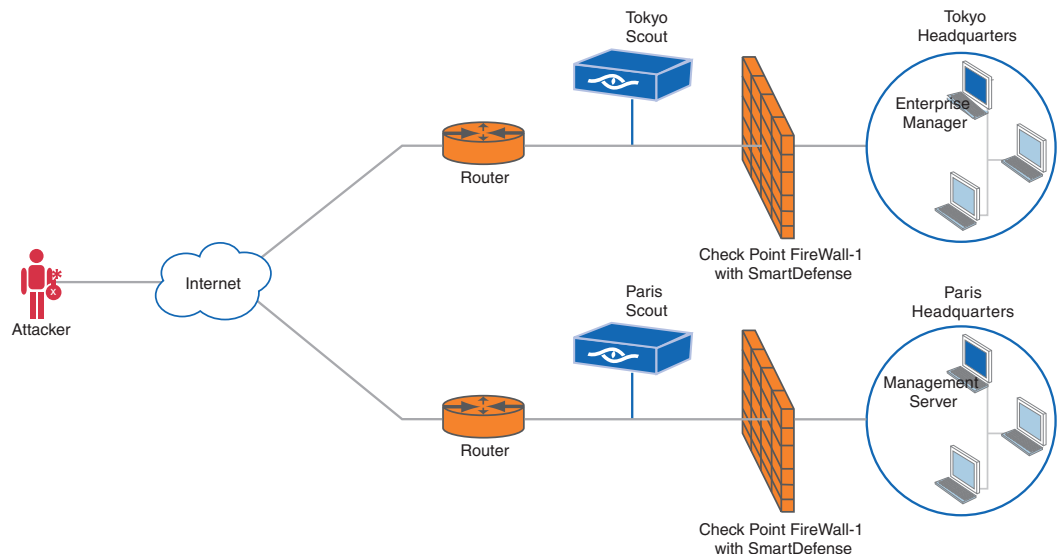
- Superior protection from new and unknown Internet threats
- Automatic, OPSEC-integrated defense mechanisms that free security professionals to perform other critical security-related tasks

ActiveScout delivers these benefits with a unique intrusion prevention technique that automatically neutralizes even the most virulent Internet attacks – even if the attacks haven't been effectively documented or

addressed by a SmartDefense signature file yet. With ActiveScout, you don't need any advance knowledge of an attack to prevent it. And the safety of your company doesn't depend on how quickly you respond to alerts or pager notifications. Instead, ActiveScout accurately identifies and automatically blocks both known and unknown attacks on your network in concert with SmartDefense.

Stopping attacks cold – without false alarms

ActiveScout automatically responds to reconnaissance activity with purposely deceptive data. This data “mark” identifies any subsequent traffic from a potential attacker, enabling ActiveScout to automatically detect and stop any ensuing attack in its tracks before the traffic reaches the Check Point firewall – whether or not the attack fits a known pattern or signature. ActiveScout thus perfectly complements your SmartDefense system by using attackers' own reconnaissance activities against them to block attacks before they reach the firewall.



ActiveScout Enterprise Manager enables central viewing of the prevention activity of all Scouts. ActiveScout works in concert with FireWall-1™ with SmartDefense to optionally block attacks.

Leverage your Check Point security investments

ActiveScout helps you get the most out of your existing investments in Check Point security solutions by making your firewall dynamic. It can automatically instruct your Check Point firewall to block any potentially malicious host – even if that host isn't the one that performed the original recon. That's because ActiveScout identifies malicious hosts by the phantom "mark" and not just by their IP address.

Because ActiveScout supports Check Point's Suspicious Activity Monitoring Protocol, it can also trigger firewall policy updates automatically and with great precision based on the types of potentially malicious activity it can uniquely discover. And its capabilities extend beyond TCP to additional protocols such as UDP – an important consideration in defending your network against a growing variety of threats.

Plus, by integrating its own logging with that of your Check Point firewall, ActiveScout ensures that your security team can enjoy the benefits of having a single, centralized repository for security event logging and analysis.

Greater security, less "housekeeping"

IT security teams face a two-fold challenge: 1) safeguarding their organizations from a growing range of security threats, and 2) making the most of the finite resources that those organizations can allocate to security management. ActiveScout's intrusion prevention technique enables you to fulfill both of these essential requirements with:

Zero false alarms

ActiveScout separates real threats from noise with 100% accuracy. This ensures your protection while eliminating false alarms and allows you to rely on the information to act upon it automatically.

Zero time to prevention

ActiveScout automatically renders any attack impotent – regardless of how quickly you can get to your alerts, reports or signature updates. So your security isn't totally contingent on the attention you and your staff can give to daily security "housekeeping" chores.

Multi-location synergy

ActiveScout effectively protects your entire enterprise, since the identification of an attacker at one location automatically triggers protection for every other location on the network.

Robust administrative and reporting functions

ActiveScout provides comprehensive information about suspicious activity, including historical trending, geographical maps, and on-the-fly WhoIs services. ActiveScout also provides streamlined, secure remote administration, making it an ideal solution for large, multi-location enterprises.



ForeScout Technologies, Inc.
2755 Campus Drive
Suite 115
San Mateo, CA 94403 USA

T 650.358.5580
F 650.358.5581



For more information on ForeScout Technologies' ActiveScout solution – including its patented ActiveResponse technique and advanced blocking mechanisms – please visit www.forescout.com or call ForeScout Technologies at 650.358.5580.