

Securite™ Component Features

Secure DNS Resolution

- A Secure Service containing a list of whitelisted website domains and blacklisted phishing domains is used for securely resolving domain names requested for by Securite™ clients.
- Secure DNS resolution protects the user against DNS poisoning attacks and TCP packet hijacking by ensuring that all connections to a whitelisted domain is always resolved to the legitimate IP address and not redirected to a fake site.

Secure Site Verification

- Securite™ uses a fingerprint system to verify that the SSL certificate received from a whitelisted service provider such as a bank is valid and not spoofed.
- Secure Site Verification ensures that the certificate has not been compromised and the HTTPS session is being established with only the legitimate service provider.

Phishing Protection

- A service provider can immediately add newly discovered phishing sites to the blacklist, instantly protecting the rest of its Securite™ protected customers the moment a threat is detected.

Network Protection

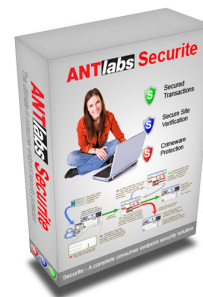
- During a Securite™ protected transaction all outbound traffic from the user's computer is tunneled via open standards to the service provider's router.
- Network Protection ensures that all traffic automatically gets to the legitimate destination without any user intervention and prevents man-in-the-middle attacks especially in rogue wireless networks.

Application Protection

- Securite™ enforces a policy-based application lockdown during a secure session which prevents any unauthorized applications from executing or reading and writing to disk on the user's computer.
- Securite's application protection thus protects the user from crimeware, preventing spyware such as keyloggers from being able to capture keystrokes and blocks crimeware that read the browser's cache in order to steal data.

Browser Protection

- During a Securite™ transaction, the user is warned of any unauthorized browser redirection out of the protected session, thus blocking cross-site scripting attacks.
- In addition, Securite™ will only allow user submitted data to be POSTed to legitimate URLs specified in the service provider's policy rules.



Requirements: End-User

→ Operating system platforms:

- Windows 2000
- Windows XP Home
- Windows XP Pro
- Windows Vista

→ Browsers supported:

- Internet Explorer 5
- Internet Explorer 6
- Internet Explorer 7
- Mozilla Firefox 2
- Mozilla Firefox 3

→ Free Disk Space: 10MB

Requirements: Service Provider

→ Routers supported:

- Cisco 800 series
- Cisco 1800 series
- Cisco 2800 series
- Cisco 3800 series
- GRE enabled Cisco routers

