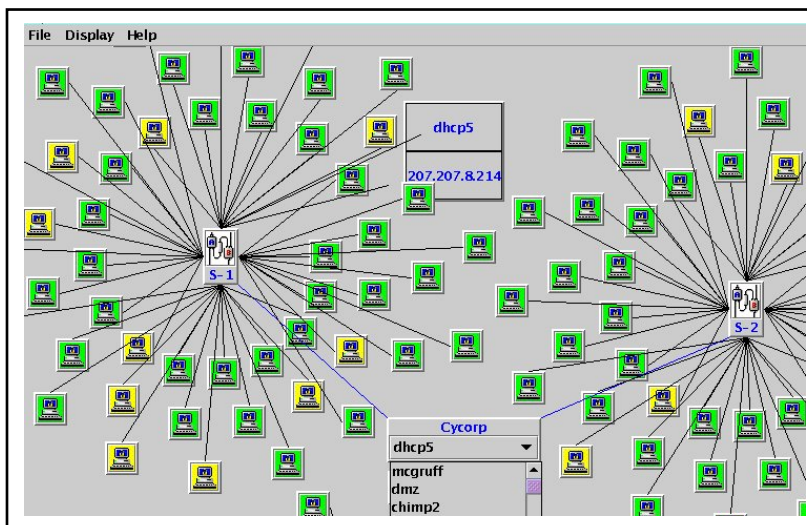


**CycSecure** predicts network attacks, recommends remediation and performs impact analysis in a safe simulation environment.

**CycSecure** complements network scanning services that merely provide perimeter scans and only identify individual vulnerabilities.

**CycSecure** locates compound vulnerabilities and reveals plans hackers could use to break into your seemingly secure network.



“The Internet will continue to get less and less secure as it gets more interesting, more useful, and more valuable.”

Bruce Schneir, in testimony before the US Senate

## Advantages

- High-fidelity semantic model enables a robust simulation.
- Declarative representation of attack rules keeps pace with new attack knowledge.
- Completely non-intrusive.
- Supports “What if?” analysis.
- Unlimited attack scenarios.
- No attack is too dangerous to simulate.

## Use Your Home Turf Advantage

Most vulnerability assessment scanners start by simply taking inventory of your network’s assets. But you know much more about your network, and so should your network guardian. The CycSecure Network Configuration Simulator™ relies on a detailed virtual model of your network containing all the data necessary for its vulnerability assessment, including: machine names and addresses, services running, programs installed and ports open.

## Know the Enemy

The CycSecure Knowledge Base contains an immense store of knowledge about computer vulnerabilities and their potential network impact, which is updated constantly with the latest vulnerability information. CycSecure applies its Knowledge Base to the virtual network model, thereby identifying your network’s vulnerabilities without the need to perform invasive scans or to consume bandwidth.

## Predict Their Next Move

The AttackPlan Analyzer™ employs a planning algorithm to identify novel sequences of actions which could result in a compromise of the network. The AttackPlan Analyzer plays the role of a hacker and performs a virtual attack on the the network model, exploiting multiple vulnerabilities it has discovered throughout the network to gain unauthorized access, steal critical files, deface a website, etc.

**Generate Attack Scenarios**

Most of the security diagnosis will occur through the creation of plans that could be used to attack the network.

**View Reports in Plain English**

In addition to the scenario, the planning engine returns a list of vulnerabilities that were exploited in each plan.

**Test the Fix**

Approve suggested fixes and the model will be updated, allowing you to repeat the simulation until you are satisfied with the results. Then, correct the real network with confidence.

Step 1. Hypothetical Hacker sends an email to workstation.testnet.com, inviting the user of workstation.testnet.com to a particular website.

Step 2. Hypothetical Hacker constructs a data string designed to overflow the memory buffer for Real Player Version 11.0 .

Step 3. Hypothetical Hacker sends the malicious data string to Real Player Version 11.0 running on workstation.testnet.com.

Step 4. Hypothetical Hacker overflows the memory buffer for Real Player Version 11.0 running on workstation.testnet.com.

Step 5. Hypothetical Hacker installs a sniffer program on workstation.testnet.com.

Step 6. Hypothetical Hacker waits for the user of workstation.testnet.com to enter the account password.

Step 7. Hypothetical Hacker uses sniffer program to sniff the login information for a user account on the Cycorp test LAN on workstation.testnet.com.

Step 8. Hypothetical Hacker uses remote hacking computer to send a valid username and password to workstation.testnet.com.

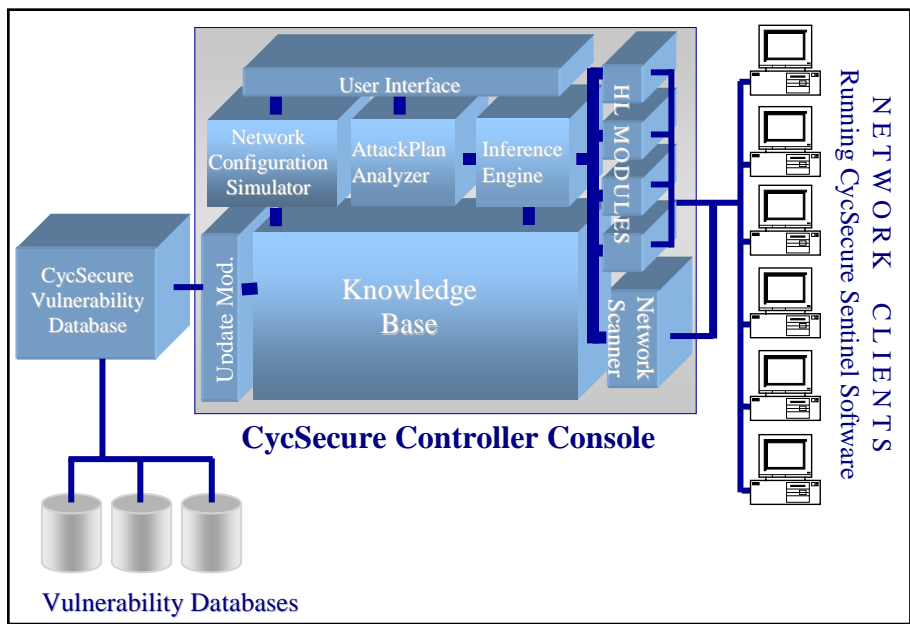
Step 9. Hypothetical Hacker uses remote hacking computer to login to workstation.testnet.com.

Step 10. Hypothetical Hacker downloads the MSIEXEC exploit program onto workstation.testnet.com.

Step 11. Hypothetical Hacker runs MSIEXEC to compromise workstation.testnet.com's operating system, Microsoft Windows NT.

Step 12. Hypothetical Hacker gets access to an account with SYSTEM privileges on workstation.testnet.com.

Step 13. Hypothetical Hacker can now read or write any files on workstation.testnet.com.



**Cycorp, Inc.**  
 7718 Wood Hollow Dr.  
 Austin, TX 78731 USA  
 (512) 342-4000  
 www.cyc.com  
 email: sales@cyc.com

Cyc is a registered trademark, Cycorp, CycSecure, Network Configuration Simulator, Attack Plan Analyzer and Scenario Generator are trademarks, and War Games for Networks is a service mark of Cycorp, Inc. Copyright 2005-2009 Cycorp, Inc. All rights reserved.