

# CycSecure<sup>ä</sup>

**An Intelligent Automated Network Security Risk Analysis Tool**

---



## Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
Overview .....	3
The CycSecure Advantages.....	4
<b>PROBLEMS AND SOLUTIONS.....</b>	<b>6</b>
Significant Losses and Costs to Industry .....	6
Vulnerability Assessment .....	7
Increased Spending in the Internet Security Category.....	8
<b>TECHNOLOGY OVERVIEW .....</b>	<b>9</b>
CycSecure Functionality .....	9
Overview .....	9
Network Analysis Process.....	11
<b>VALUE PROPOSITION.....</b>	<b>14</b>
Vulnerability Assessment .....	14
Summary of CycSecure advantages .....	14
Time & Cost Savings .....	14
Added Security .....	15
Reduction in Total Cost of Ownership .....	15
Policy Enforcement .....	15

## **CycSecureä, An Intelligent Automated Network Security Risk Analysis Tool**

*This document is designed to provide the reader with an overview of CycSecureÖ, a new and intelligent automated network security risk analysis tool currently under development. Cycorp began beta testing CycSecure with commercial enterprises during the third and fourth quarters of 2001. CycSecure goes many steps further than current tools, and will provide the network security professional with both a strategic and operational analysis of an organization's network and its vulnerabilities.*

## **EXECUTIVE SUMMARY**

### **Overview**

Cycorp is a Delaware Corporation, based in Austin, Texas and incorporated in 1994. The business was founded by computer science pioneer and Stanford professor Douglas B. Lenat. Ten years prior to incorporation, Lenat went on leave from Stanford to serve as Principal Scientist of the first computer-related consortium in the United States: MCC (The Microelectronics and Computer Technology Corporation). It successfully carried out its 10-year mission, which was to counter the threat of the Japanese Fifth Generation initiative (a MITI-funded attempt to install Japan as the world leader in computing technology). Under the Research and Development umbrella provided by the dozens of corporate members of MCC, Lenat began work in 1984 on a high-risk high-payoff long-term project he called Cyc. In late 1994 Lenat left MCC to form Cycorp, Inc. Cycorp has remained self-funded and profitable and has steadily grown from a dozen to over 70 full-time employees.

The Cyc project's objective was to codify, in machine-usable form, the millions of pieces of knowledge that comprise human common sense. Such a **common sense knowledge base**, and its associated **reasoning system**, is now being used to enable the development of knowledge-intensive applications.

The first Cyc application to be rolled out by Cycorp's Commercial Products Division is CycSecure. CycSecure is an intelligent automated network security risk analysis tool that provides the network security professional with both a *strategic* and *operational* analysis of an organization's network vulnerabilities.

CycSecure was developed to address the dramatic increase in security breaches and network vulnerabilities worldwide and to capitalize on a market that is expected to grow from \$5.7 billion to \$19.7 billion in the coming three years.<sup>1</sup>

CycSecure is a software application that utilizes the intelligent and common-sense technology known as Cyc®. This unique and patented technology allows CycSecure to provide an organization with a virtual representation of its networks that will allow attacks and simulated modeling to occur without risking any damage to the real network. It provides the network security team levels of information that afford complete, concise and actionable risk analysis. The result is mission critical problem-prevention and preemption.

The Cyc technology and software have been used by the United States Department of Defense, DARPA, NSA, and CIA among others. It has a 17-year legacy of developing, deploying and managing sensitive data and information. Cycorp has already been retained to develop and deploy CycSecure by DARPA to protect portions of the Department of Defense's network infrastructure.

---

<sup>1</sup> Source: Forrester Research

## The CycSecure Advantages

The CycSecure process begins by scanning and aggregating information describing the state of the network. This is the same kind of information that is collected by traditional vulnerability assessment scanners. This is the **only** area where there is a similarity between CycSecure and existing vulnerability assessment scanners.

CycSecure then builds up a formal model of the network, analyzes the low-level vulnerabilities in that model, and assembles plans capable of attacking the network. Its users can then try out proposed remedies on CycSecure's model of their network (e.g., to see what new vulnerabilities would be introduced by such changes), and can pose additional hypothetical questions, before making changes on the actual network itself.

The Cyc Knowledge Base ("KB") and Inference Engine provide the analytical backbone for CycSecure.

CycSecure's unique features and benefits include:

- **Compound vulnerability analysis:** Discovers compromises that otherwise go undetected because they involve attack plans with a large number of steps, often exploiting several different "minor" vulnerabilities present on several different machines to enable an attack that is far from minor in its seriousness. Other tools either lack this capability entirely, or else are able to do so only by running canned exploit "scripts" of past attacks which have already been tried by hackers and have become well known, meaning that hackers can succeed with *any* novel attack against your network.
- **Identifying the most critical vulnerabilities that must be corrected.** As was just mentioned, these are not always the ones which *in isolation* appear to be the most serious, but rather those which can be exploited as steps and sub-steps in attack plans having the most serious overall consequences.
- **Reporting the actual sequences of actions that can compromise your network.** This enables the user to decide how and where to modify their network, to thwart these attack plans. Instead of just making those changes to their networks, however, they can use the following capability at this stage:
- **"What-if..." analysis:** CycSecure users can see the effects of any planned changes to the network configuration, network security policies, etc. (by editing CycSecure's model of their network and rerunning CycSecure's analysis module on that edited model) before committing to costly, time-consuming implementation decisions which might even introduce new vulnerabilities that turn out to be worse than the ones they corrected.
- **Non-invasive and Continuous:** Since the attacks, and the processing, are happening on a simulation of the network instead of the real network, CycSecure mitigates risk of system damage, downtime, and bandwidth consumption. Other current state-of-the-art vulnerability assessment tools operate by an *invasive* technique – actually running known exploits against your network – which disrupts network functionality. Since those tools are so intrusive, their users only run them very infrequently. CycSecure is non-invasive, both in scanning and in analysis, so it can be run continuously, 24x7.

CycSecure is designed for

- Support of multiple platforms (machines, operating systems, etc.),
- Scalability (to networks with hundreds of thousands of nodes), and
- Interoperability with an organization's existing risk analysis and security tools.
- Future expansion drawing on the entire Cyc KB, including for example vulnerabilities involving real-world policies, business and financial models, physical layout, human motivations and capabilities.

By taking advantage of these powerful analytic capabilities and of the proprietary Cyc KB, organizations can achieve qualitative improvement in their network security.

## The Cyc-Secure Process

**1. SCAN THE NETWORK.** As much as 50% of the total time of traditional security audits is spent gathering information. CycSecure streamlines this process using a non-invasive information gathering and then uses that information to build a security status model (or representation) of that network. This model is then declaratively stored in the Cyc Knowledge Base (KB).

**2. IDENTIFY LOCAL VULNERABILITIES.** The network representation includes facts about installed software, running programs, user configurations, connectivity and inter-machine “trust” relationships, etc. From this model of the network, CycSecure first deduces low-level types of “local” vulnerabilities, given its extensive knowledge base of known bugs and exploits in existing operating systems, hardware, and applications software. Similar vulnerabilities (e.g., on a large class of workstations on the network which are all running the same known-vulnerable version of the same piece of code) are aggregated together, into a clear and concise report for the system administrators.

**3. PLAN MULTI-STEP ATTACKS.** CycSecure then performs a risk analysis using a combination of proprietary and public information within the Cyc KB, and a combination of public and proprietary planning and inference technology. The analysis is broken down into attacks which a particular sort of individual could execute, (e.g. disgruntled employee, a customer or any outside hacker) could execute.

**4. WHAT-IF ANALYSIS OF SUGGESTED FIXES.** CycSecure then assists the user in analyzing the data and recommending fixes that can be applied to thwart various plans – to correct security conditions. The network security administrator can pose “what if” questions or create “what if” scenarios by editing the model of the network. Steps 2 and 3 can then be run again, on the modified model, to see if the problems would be fixed, and to see what new problems would be introduced.

**5. REPEAT.** Steps 1-3 can be repeated continuously and automatically, re-scanning the network for new vulnerabilities that may be introduced when a new piece of software is installed on a machine, or when a new bug or vulnerability is reported with a certain piece of software on a certain OS/HW configuration, etc. Step 4 can be redone whenever Steps 1-3 turn up new attack scenarios that should be precluded. Step 4 can also be redone whenever a proposed change is about to be made to the network, to see the negative effects such a change would have.

## PROBLEMS AND SOLUTIONS

During the past several years, there has been a fundamental shift in technology spending habits. The majority of technology projects today involve using the Internet to increase revenue opportunities, reduce costs and improve operating efficiencies. Initiatives, ranging from setting up a simple Web presence to the deployment of complex B2B e-commerce applications, all necessitate the opening up of previously internal IT systems to the public Internet. The Internet, combined with intranets for employees and extranets for customers and partners, effectively creates networks that extend beyond the enterprise. This fact creates significant new security concerns and opportunity for expanded security applications. The following chart illustrates the quantum increases in attacks.



\*January to September. Source: Computer Emergency Response Team, September 2000

Figure 1. Incidence of attacks.

### Significant Losses and Costs to Industry

A study conducted by the Computer Security Institute and the FBI found that 70 percent of the companies surveyed reported a serious cyber attack such as theft of proprietary information or a denial-of-service attack. The survey results show that 74 percent of companies reported a financial loss due to a security breach in 1999, which collectively was more than double the aggregate loss reported in the prior four years. High-profile security breaches regularly appear in the mainstream media, compounded by an increase in the number of high-profile software and hardware vulnerabilities. On July 16, 2001, in testimony before the U.S. Senate on the security of the Internet, Bruce Schneier of Counterpane said:

“I believe that the Internet will never be totally secure. In fact, I believe that the Internet will continue to get less and less secure as it gets more interesting, more useful, and more valuable. And the processes of detection and response, risk management and insurance, and forensics and prosecution will serve the Internet world just as they serve the real world.”

## Vulnerability Assessment

The following chart illustrates the rise in reported vulnerabilities.

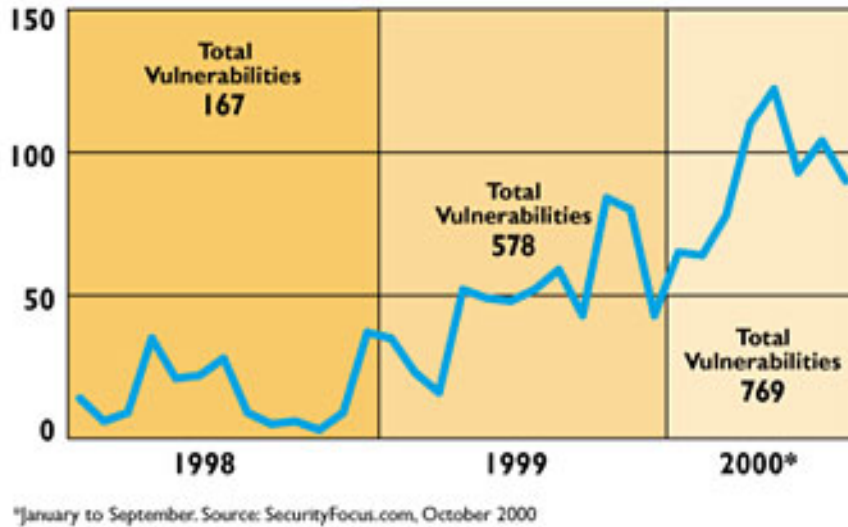


Figure 2. Reported vulnerabilities.

While information security includes a wide range of individual technologies, risk management and assessment presents one of the largest and most profitable opportunities. Prior to the introduction of vulnerability assessment scanners, there were no tools available that allowed the collection of necessary information. Vulnerability assessment scanners represented a giant leap forward from the time when no information about a network's weaknesses was available. Today, we are in an environment where security administrators are deluged with more information than they can make use of. As explained in the overview, CycSecure's first product release will provide functionality that will create an entirely new level of network risk management and analysis.

### Protection from Viruses Before they Exist

The Nimda virus, like most other Internet worms, takes advantage of known vulnerabilities with known fixes. The reason these viruses and worms are so successful is because few people either take or have the time to keep up-to-date on these problems. CycSecure makes it easy to identify and correct these vulnerabilities. So while other companies incur the profound costs scrambling to respond to the crisis of a newly released virus, companies using CycSecure continue to conduct business as usual.

## Increased Spending in the Internet Security Category

According to *PC Data*, the Internet security category continues to follow a “meteoric growth” curve:

“To put this into perspective, 1Q 2000 saw greater than a 205 percent increase in unit volume compared to the same quarter in 1999. Even more remarkable, the category saw more than 100,000 units of Internet security products shipped in 1Q 2000 alone, almost totaling the entire category sales in 1999.”

In October 2000, Wit SoundView surveyed attendees at the lead security session at Gartner’s annual Symposium. Representatives of large commercial enterprises and government agencies indicated that their spending in this area would increase sharply in the coming year (measured by an average score of +86 on a scale from –100 to +100). Consistent with the results from this survey, companies continue to prefer “best of breed” products to product suites by a ratio of 4:1. This reflects a climate in which innovative technology is embraced.

Forrester Research estimates spending on security products will grow from \$5.7B in 2000 to \$19.7B by 2004:

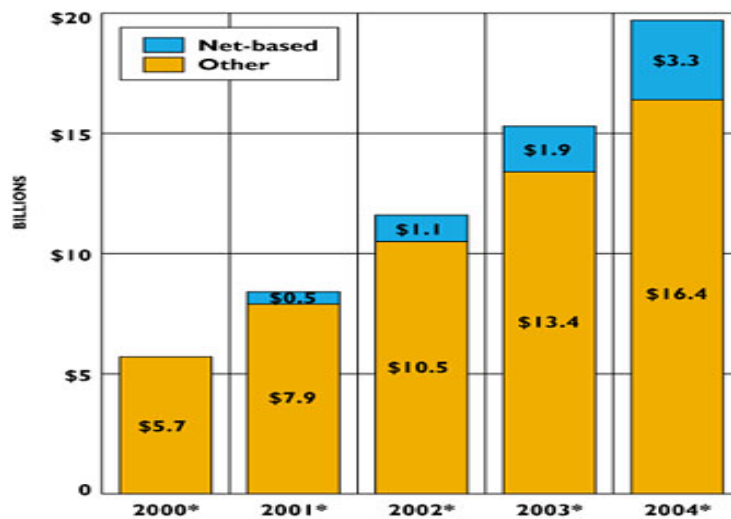


Figure 3. Estimated spending on security products.

These factors – increases in attacks over the Internet; increases in known vulnerabilities; increases in spending; openness of industry to accept security innovations; and the lack of capability in existing technology – highlight the need for a tool that has the power of CycSecure.

# TECHNOLOGY OVERVIEW

## CycSecure Functionality

### Overview

The CycSecure process involves scanning, collecting, collating and analyzing information describing the state of the network.

It begins by gathering information about the network and then uses that information to build a security status model (or representation) of that network. This model is then stored in the Cyc Knowledge Base (“Cyc KB”). This network representation includes facts about installed software, running programs, user configurations and deduced vulnerabilities. A risk analysis is performed using a combination of proprietary and public information within the Cyc KB. The analysis, including discovery, deduction, reasoning and logic will provide the following, all without doing any harm to the real network and at minimal bandwidth:

- It will deduce and report network vulnerabilities based on Cyc KB representations of all reported bugs and vulnerabilities.
- It will use the Cyc KB to find plans by which different kinds of attackers (hacker, disgruntled employee or customer) could successfully attack the network.
- It will enable a network administrator to pose “what if” questions or create “what if” scenarios by editing the model of the network.
- It will evaluate the impact of proposed fixes and proposed policy changes.
- It will continuously scan the network for changes, which may lead to the introduction of new vulnerabilities.

These are accomplished by the following:

- An interactive interface through which network administrators can explore the state of their network, focusing on the aspects of greatest interest at the moment, and through which they can perform many of the recommended fixes.
- An inference engine that intelligently reasons about the network and automatically reports vulnerabilities to the network administrator. Through inference, CycSecure is able to discover compound vulnerabilities that are not seen when viewed independently.
- A planning engine that generates hypothetical attacks against the network and enumerates the specific vulnerabilities that would enable them to succeed.
- A simulation engine that allows administrators to test alternate configurations of their network before actually making the changes.

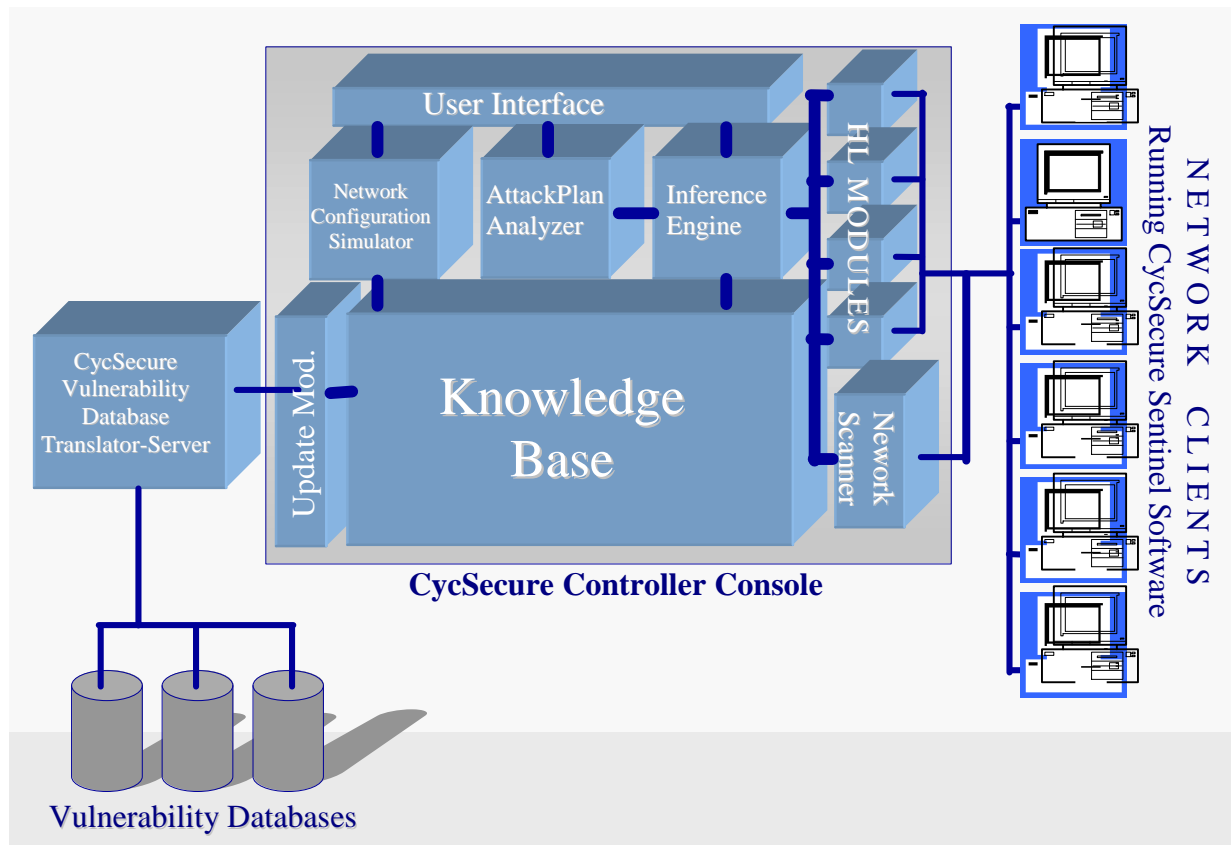


Figure 4. CycSecure architecture.

The CycSecure risk analysis process begins with the installation of CycSecure Sentinels and controller console(s). First, a Sentinel (an unobtrusive software program that runs continuously in the background, gathering information) is installed on every machine in the network. The Sentinel, when polled or queried by the controller, gathers information from its host machine.

The controller console, built around the Cyc KB, has a detailed understanding of computer networks, including how computers and other network devices can be connected to each other, how they communicate and what programs they can run. The knowledge base also contains details about ways a network can be at risk of compromises to its availability, confidentiality and integrity. Where multiple controller consoles are employed, a custom controller matrix will be developed to manage global filtering and communication requirements of the organization.

The information gathered into the Cyc KB is collated with additional facts and data to build a functional model of the network. This process consists of two steps:

1. Gathering the information.
2. Analyzing the network model.

## Network Analysis Process

1. **Answering questions:** CycSecure allows network administrators to ask questions about the configuration of their networks in order to diagnose potential problems. Questions may be as straightforward as “Which computers on the network are running Linux?” or more complicated: “Which buffer overflow vulnerabilities exist on the network and which machines have them?”. This allows the network administrator to get information as it is needed, structured in the most usable manner possible.

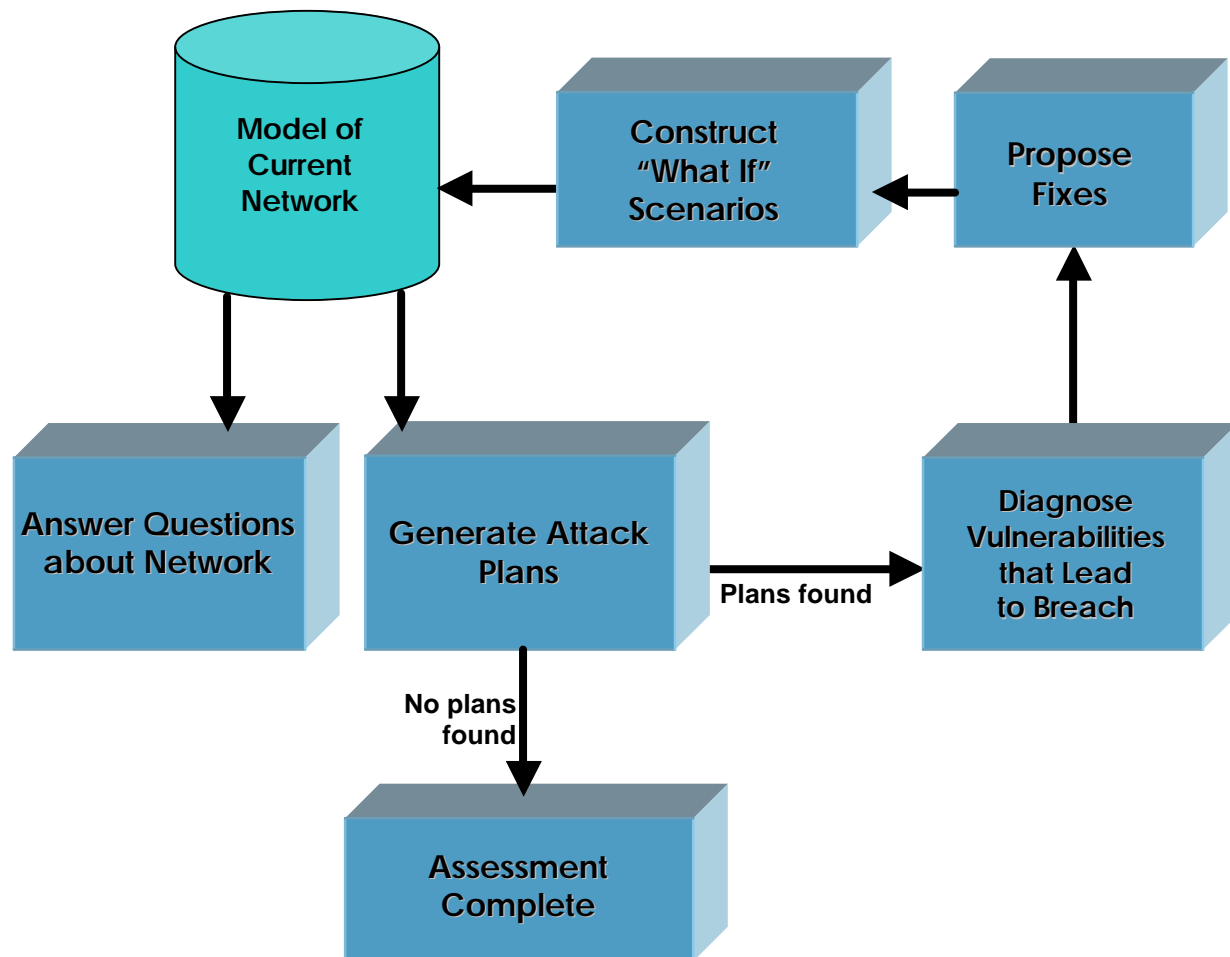


Figure 5. CycSecure network analysis process.

**Generating attack plans:** Most of the security diagnosis will occur through the creation of plans that could be used to attack the network. These scenarios are constructed to achieve specified goals that the network administrator is interested in monitoring. Here is an example of one such attack plan:

Plan1:

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

Step 2. Hypothetical Hacker constructs a data string designed to overflow the memory buffer for Real Player Version 7.0 .

Step 3. Hypothetical Hacker sends the malicious data string to Real Player Version 7.0 running on workstation.cyc.com.

Step 4. Hypothetical Hacker overflows the memory buffer for Real Player Version 7.0 running on workstation.cyc.com.

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

Step 6. Hypothetical Hacker waits for the user of workstation.cyc.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 LAN on workstation.cyc.com.

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

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

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

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

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

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

**a remote unauthorized access exploit on Cycorp's internal network.**

*Figure 6. Example attack plan scenario.*

2. **Diagnosing vulnerabilities:** In addition to the step-by-step description of attack plans which could be used to target the network, the planning engine also returns a list of the vulnerabilities which were exploited in each plan. This information can be reviewed by the network administrator to determine which problems need to be addressed.

3. **Proposing fixes:** Once the network administrator has decided which vulnerabilities need addressing, CycSecure can be asked for suggested fixes that can be applied to correct the problem in question. Where such a fix exists CycSecure will direct the network administrator to it, either allowing the fix to be made directly through the CycSecure interface or directing the network administrator to some other resource.
4. **Constructing “what if” scenarios:** When a fix or set of fixes has been decided on, the network administrator is able to create another network model in the Cyc KB reflecting these proposed changes. Then, prior to implementing the actual fixes, the same tests can be performed once again on this simulated network, repeating until the network administrator is satisfied with the security and functionality provided.
5. **Completing the assessment and altering the physical network:** Once the above diagnostics have been completed the network administrator can make any desired changes to the physical network.

CycSecure provides a global picture of the network that interacts with knowledge in the Cyc Knowledge Base to provide a much richer picture of the network and network security in general. By taking advantage of this knowledge and by applying a variety of analytic techniques CycSecure can provide a great deal of help to the security administrator trying to discover, diagnose and fix the holes in their network security.

## VALUE PROPOSITION

CycSecure is designed for support of multiple platforms, scalability and interoperability with an organization's existing risk analysis and security tools. The analytical backbone for CycSecure is provided by the Cyc Knowledge Base and Inference Engine. This enables CycSecure to discover and link seemingly unrelated data to identify compound vulnerabilities in a way no other tool can replicate.

By taking advantage of these powerful analytic capabilities, organizations can achieve qualitative improvement in their network security. By using the Attack Plan Generator, network administrators are able to make a far more realistic assessment of the dangers to their network, allowing them to react to potential attacks before those attacks occur. CycSecure also provides support for forensic analysis of attacks that are discovered after the fact, enabling network administrators to make better decisions in order to prevent similar occurrences in the future.

## Vulnerability Assessment

Vulnerability assessment scanners have been the dominant tools in the security professional's toolkit for years. These scanners allow a great deal of information about the security status of a single computer to be gathered automatically and rapidly. This information is collected in reports which are returned to the user. The user can then perform an analysis of the security of the network as a whole, though this is a laborious process that involves wading through reams of data produced by the scanner and then manually analyzing the data.

Because these scanners operate by an **invasive** security scan which disrupts network functionality, these scans are not performed frequently. They are often performed during off-hours in order to avoid the negative consequences they might bring about. Assessing the security conditions of the network in this way is incomplete and limiting. These tools have other limitations which are discussed in detail in the question and answer section.

## Summary of CycSecure advantages

CycSecure gathers the same kind of information that is collected by traditional vulnerability assessment scanners. This is the only area where there is a similarity between CycSecure and vulnerability assessment scanners.

CycSecure uses this information to build a representation of the network in the knowledge base. The information is then indexed to enable rapid access by users in the most convenient form possible.

CycSecure provides more powerful analytic capability by generating attack plans in which the network could be successfully threatened by a knowledgeable attacker. This allows a very rapid and accurate assessment of the impact of vulnerabilities detected on the network. CycSecure also helps the user analyze the data and recommends fixes that can be applied to correct security conditions.

In addition, CycSecure employs a **non-invasive** information-gathering process that when combined with the power of the knowledge base enables the network administrator to access this information at a moment's notice rather than waiting for the next quarterly scan.

## *Time & Cost Savings*

Because CycSecure's information is constantly available in this manner, it can be rapidly analyzed. This eliminates the time currently spent gathering information about the network in more labor-intensive ways, resulting in substantial time savings on most network maintenance and testing activities. For example, keeping up to date on vendor-supplied security patches requires more time as the number of reported

vulnerabilities continues to increase. Rapid pinpoint detection and the automatic updates provided by CycSecure minimize the amount of time that this requires. **No other product can do this.**

Security audits are another area in which a great deal of time and money is invested. Most large organizations have security audits performed both by internal staff and by external consultants. As much as 50% of the total time of these audits is spent gathering information. By eliminating this time and skipping straight to the analysis, organizations can reduce the manpower requirements of internal audits and the cost of external audits substantially.

Even ordinary maintenance requires a great deal of monitoring and information collection on the part of the network administrators. Great increases in productivity, in many cases on the order of 100 to 1, can be achieved by allowing the network administrator to focus their attention on the decisions that need to be made in order to keep the network running and secure.

All of the investment in time described above translates into costs to the company, whether it is through external consulting fees, loss of productivity and increase in staff size, or inadequate security leading to potential damage to the organization. **CycSecure dramatically reduces these costs** while at the same time providing a higher level of risk assessment.

### ***Added Security***

By taking advantage of the powerful analytic capabilities built into CycSecure, organizations can achieve a qualitative improvement in their network security. Significant reduction in analysis time (as explained above) results in the most current information being applied to security fixes or patches which can reduce the risk of breaches or other network threats.

### ***Reduction in Total Cost of Ownership***

CycSecure can help decrease the total cost of technology ownership by optimizing the purchase and maintenance of per-seat software licenses. Very often, companies estimate the maximum number of users for a particular piece of software, pay for that number and neglect to keep track of actual usage. There are some system management software packages on the market that track usage (such as those from Tivoli and Hewlett-Packard), but they are an added expense that many companies choose to avoid. CycSecure, with the help of its Sentinel software, provides a system management capability that can track all application usage, identify underutilized licenses and help calculate the optimal number of licenses to purchase for a new software acquisition. Money that is not spent on unnecessary licenses goes straight to the bottom line.

### ***Policy Enforcement***

The network model maintained by CycSecure can be used to monitor compliance with corporate policy and rapidly detect alterations in network configuration. This enables greater centralized control of organizational infrastructure.



Cycorp, Incorporated ♦ 3721 Executive Center Drive ♦ Suite 100 ♦ Austin, Texas 78731-1615

[www.cyc.com](http://www.cyc.com) ♦ 512-514-2961