



IBM Software Group

“Solving the Linux Security Puzzle with Tivoli”

Security Management Solutions for Linux and the Enterprise

IBM Tivoli Access Manager

Tivoli. software

Shawn L. Young, Market Manager



May 15th | 2003

© 2003 IBM Corporation

Internal Threats are the Greatest Threats...

ajc.com The Atlanta Journal-Constitution

Wed • May 14, 2003
Current temp: 75
• Weather
• Traffic

HACKER MAY SIT IN NEXT CUBICLE
by BILL HUSTED

The computer hacker wasn't a devious competitor or some brainy teenager sitting at his home PC.

Instead, it was a Coca-Cola employee who slipped into the company's computer system without authorization and downloaded salary information and Social Security numbers of about 450 co-workers.

A recent computer scare at the world's largest soft-drink maker worried it enough to send an e-mail advising employees to check bank accounts and credit card balances...

Computer break-ins by insiders often do more damage than...remote hackers. "They know what to take; they know what is important." Gray said.

ajc.com
Nation / World ▶
Metro ▶
Business ▶
Sports ▶
Living ▶
Opinion ▶
Travel ▶
Health ▶
Your Money ▶
Buyer's Edge ▶
Jobs ▶
Cars ▶
Homes ▶
Classifieds ▶
AccessAtlanta
Entertainment ▶
Events ▶
Music ▶
Movies ▶
Theater & Arts ▶
Restaurants ▶
Recreation ▶
Personals ▶
ajc services
Archives

“The hacker who just stole your records is just as likely to be an insider as an outsider...”

“There's the notoriety, bad press and Wall Street doesn't like it,”

“Some computer systems simply allow users too much freedom to roam.”

And Identity Theft is Powerful Incentive

Case Study

Personalize Your Post
mywashingtonpost.com **washingtonpost.com** Subscribe | Print Edition
The Washington Post

Metro Weather News OnPolitics Entertainment Live Online Camera Works Marketplace Jobs

E-MAIL NEWSLETTERS | ARCHIVES SEARCH: News Search Options

News Home Page
Nation
World
Metro
Business
Portfolio
Market News
Economy
Policy
Product Safety
Communications
Disaster Aid
Energy
Trade
Highway Safety
Labor
Securities
Company Research
Mutual Funds
Personal Finance
Industries
Columnists
Special Reports
Live Online
Business Index
Technology
Sports
Style
Education
Travel
Health
Real Estate
Home & Garden
Food
Opinion
Weather
Weekly Sections
News Digest
Classifieds
Print Edition
Archives

Quick Quotes Get Quotes Look Up Tables | Portfolio | Index

Identity Theft More Often an Inside Job
Old Precautions Less Likely to Avert Costly Crime, Experts Say

By Brooke A. Masters and Caroline E. Mayer
Washington Post Staff Writers
Tuesday, December 3, 2002; Page A01

You can take all the steps you want to protect yourself against identity theft: Guard your wallet, shred your personal financial papers before throwing them in the trash, monitor your credit reports.

But no matter how careful you are, you may not be able to avoid having your identity assumed by someone who wants to go on a buying spree, using your credit card, bank account, Social Security number or other personal data.

That's because the nature of identity theft has changed and the threat today is more likely than ever to come from insiders -- employees with access to large financial databases who can loot personal accounts -- than from a thief stealing a wallet or pilfering your mail. Banks, companies that take credit cards and credit-rating bureaus themselves don't do enough to protect consumers, critics say.

"You can spend a lot of time and money trying to protect yourself," obtaining copies of your credit reports every three to six months, buying a credit-monitoring service to alert you when someone is making inquiries about your account or even buying identity-theft insurance, said Robert Gellman, a D.C. privacy consultant. "You can do as much as you can do, but it won't stop you from being a victim. There's nothing I'm aware of that will guarantee you not become a victim."

That fact was underscored last week when federal prosecutors announced that they had arrested and charged three people in connection with a scheme to steal the personal financial information of 30,000 Americans by downloading data from a computer and selling it to scam artists. The prosecutors said it was the largest case of identity fraud ever detected.

Understanding Regulatory Policy
Click Here for Interactive Primer

— Related FTC Articles —
* [FTC Sues Weight-Loss Firm Over Ads](#) (Associated Press, Dec 6, 2002)
* [FTC Finds Diet Ads Hard to Swallow](#) (The Washington Post, Dec 6, 2002)
* [Canada Telemarketers to Refund \\$1M to U.S.](#) (Associated Press, Dec 5, 2002)
* [More FTC News](#)
— About the FTC —
* [Mission](#)
* [Who's in Charge?](#)

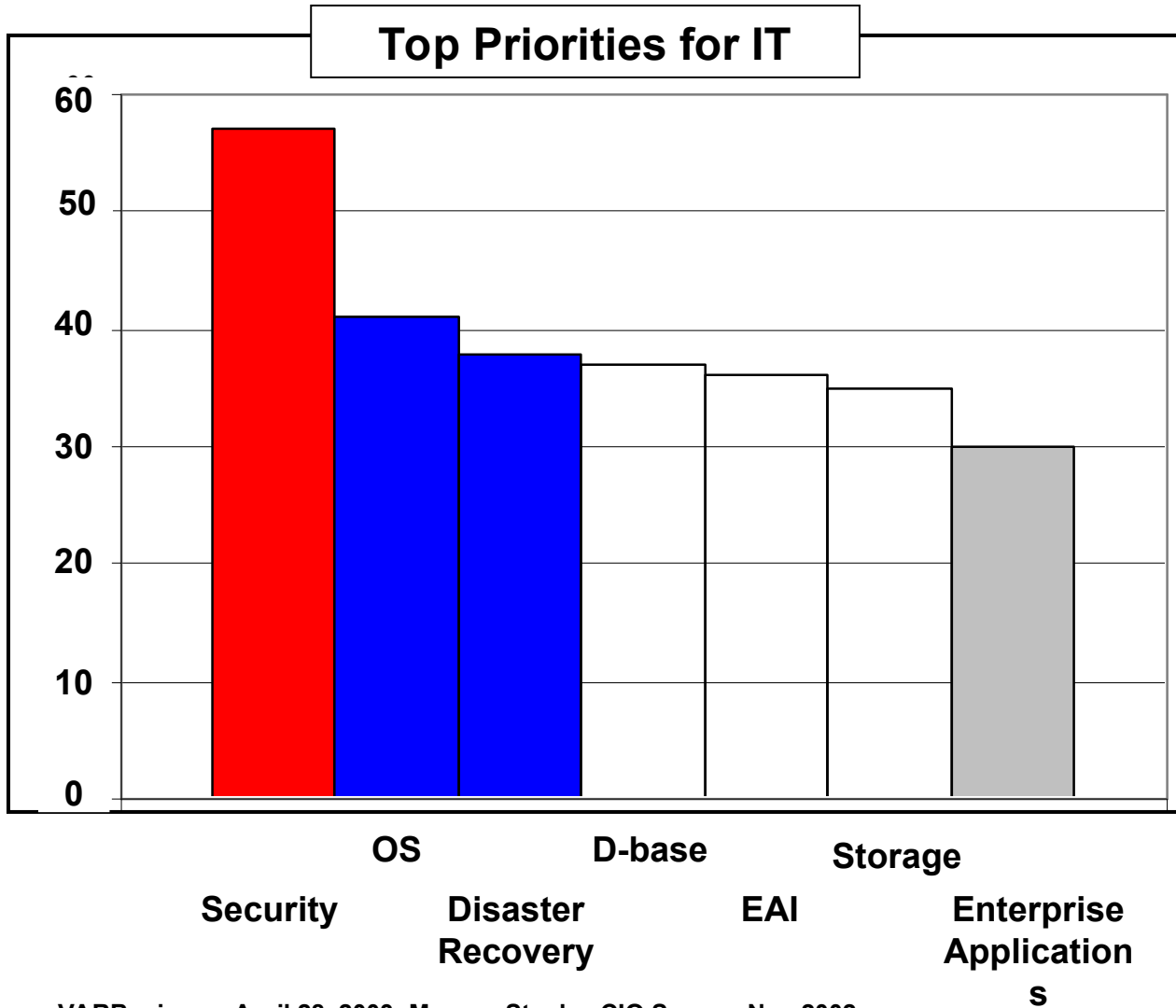
— Regulatory News By Agency —
Select an Agency

Identity Theft ring stole \$2.7M

- Employees received \$30 per report
- 30,000 reports were stolen over three years
- Identity Theft costs US \$5B and is growing at over 100% annually

“A lot of companies have gone to a lot of effort to protect themselves from being hacked, but it’s a lot harder to stop a rogue employee... We have the technology but we’re not using it.”

Security Remains Key Priority



Source: VARBusiness, April 28, 2003; Morgan Stanley CIO Survey, Nov 2002

Agenda

Linux and security

- **Common myth: “Linux security is inadequate”**

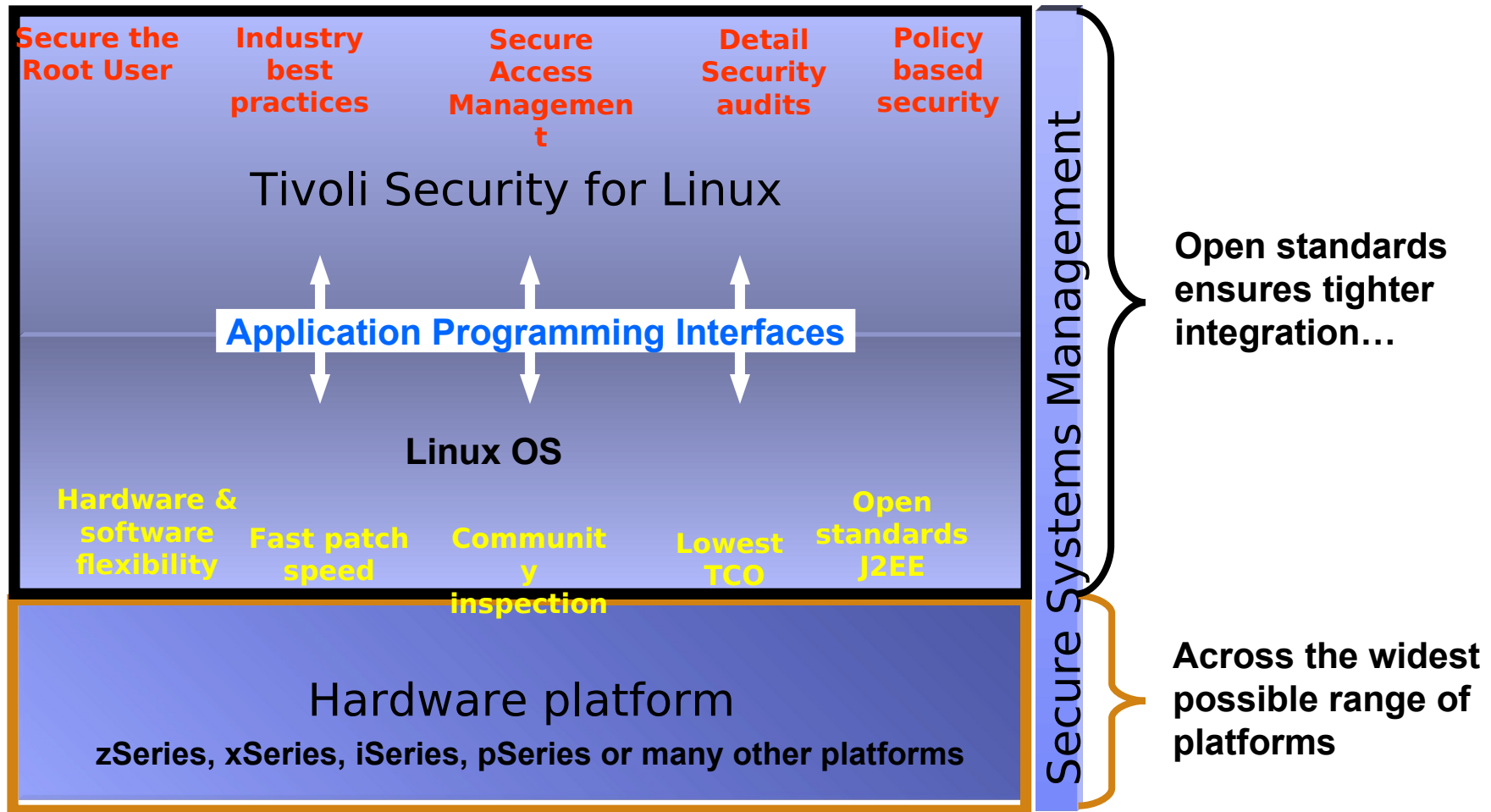
Ensuring full fledged security for your company

- **Common flaws**
- **Plugging holes**

Tivoli security management solutions

- **IBM Tivoli Access Manager for Operating Systems**
- **IBM Tivoli Access Manager for e-business**
- **IBM Directory Integrator**

Linux Enables Broad and Robust Security



Myth: Linux Security is Inadequate

Linux security compares favorably to other Operating Systems...

- **The same variety of security and cryptographic products are available**

While offering distinct advantages

- **Open source community ensures that weaknesses are known, reported and fixed**
- **Lack of vendor “lock in” allows customers to use Best in Breed products**
- **Open source allows security products to be built that are more tightly integrated with the OS**

A Wide Variety of Tools are Available for Linux

Readily Available Linux Tools

SNORT

LIDS

Firewalls

Port Sentry

Stack Guard

Protect Against a Wide Variety of Threats

Hackers

Stack Smashing

Buffer Overflows

Packet Sniffing

Parsing Errors

**Denial of Service
Attacks**

**Many of these tools are available
free or at low cost**

Myth: Linux Security is Inadequate

Linux security compares favorably to other Operating Systems...

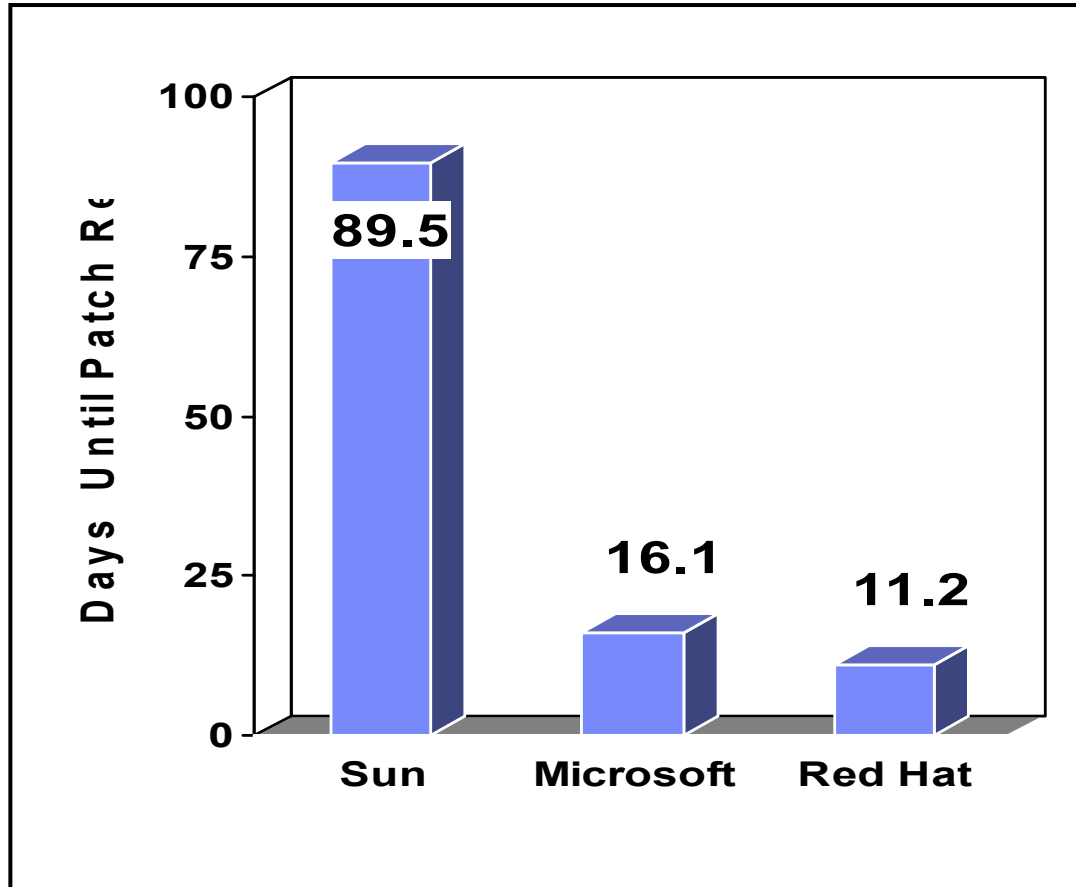
- The same variety of security and cryptographic products are available

While offering distinct advantages

- **Open source community ensures that weaknesses are known, reported and fixed**
- Lack of vendor “lock in” allows customers to use Best in Breed products
- Open source allows security products to be built that are more tightly integrated with the OS

Linux Community Patches Vulnerabilities Quickly

Average Security Event Response Time



- Open source functions like an academic community
- Built in monitoring and updating tools are available
—UP2DATE

Source: BugTrac Survey

Linux Community is Highly Responsive

Case Study

On April 4, 2001 a bug was found allowing a network time daemon to be exploited...

Time Elapsed

Activity

Time Elapsed	Activity
6 hours	<ul style="list-style-type: none"> Work around posted to Bugtrac
13 hours	<ul style="list-style-type: none"> Pointer to a FreeBSD patch posted
17 hours	<ul style="list-style-type: none"> FreeBSD releases a security advisory
2 days	<ul style="list-style-type: none"> Mandrake Linux releases advisory & updated patches
4 days	<ul style="list-style-type: none"> Red Hat posts advisory & pointer to patches
6 days	<ul style="list-style-type: none"> IBM releases advisory and temporary fix for AIX
28 days	<ul style="list-style-type: none"> Compaq releases advisory & patch for TRU 64
37 days	<ul style="list-style-type: none"> Sun has yet to release advisory despite Solaris' vulnerability

Source: BugTrac, Internal IBM analysis

Myth: Linux Security is Inadequate

Linux security compares favorably to other Operating Systems...

- The same variety of security and cryptographic products are available

While offering distinct advantages

- Open source community ensures that weaknesses are known, reported and fixed

- **Lack of vendor “lock in” allows customers to use Best in Breed products**

- Open source allows security products to be built that are more tightly integrated with the OS

Vendor “Lock In” Undermines Security

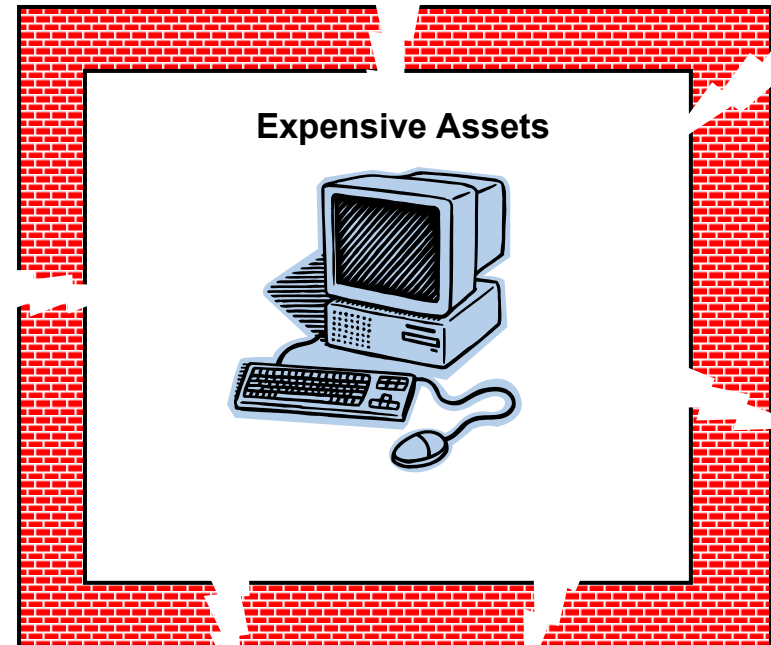
Best in Breed

“Locks out hackers”



2nd Rate

“Locks in gaps”



“Most hacks result from buggy software...”

--AT&T Research

Myth: Linux is not Secure

Linux security compares favorably to other Operating Systems...

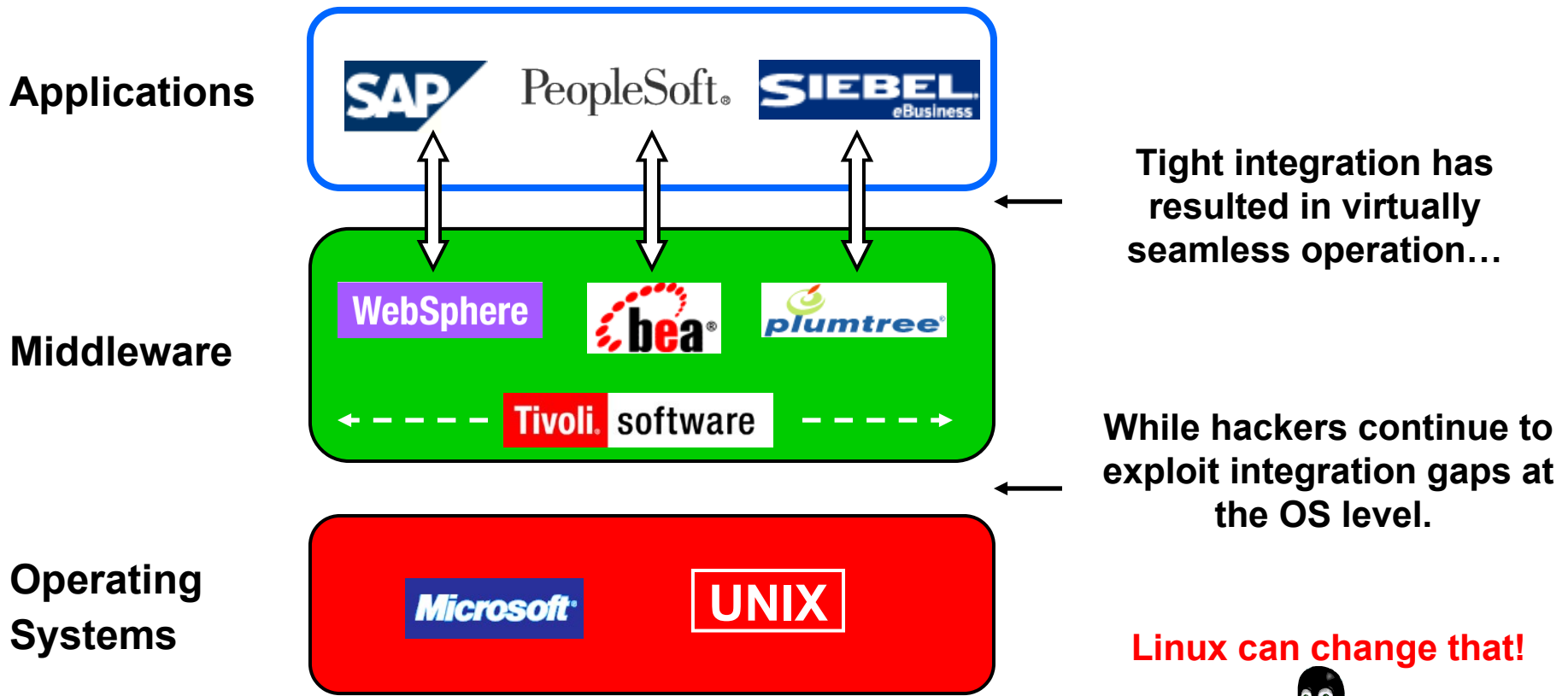
- The same variety of security and cryptographic products are available

While offering distinct advantages

- Open source community ensures that weaknesses are known, reported and fixed
- Lack of vendor “lock in” allows customers to use Best in Breed products

- **Open source allows security products to be built that are more tightly integrated with the OS**

Buggy Software Augments Integration Vulnerabilities



A Virtuous Circle of Value: Tivoli and Linux

Linux

- Linux lowers the cost of ownership
- Linux is moving to business critical applications
- Linux may not be the only platform in your business

Tivoli

- Tivoli lowers the cost of operations
- Tivoli secures business critical applications
- Tivoli provides consistent security across heterogeneous platforms

Agenda

Linux and security

- Common myths

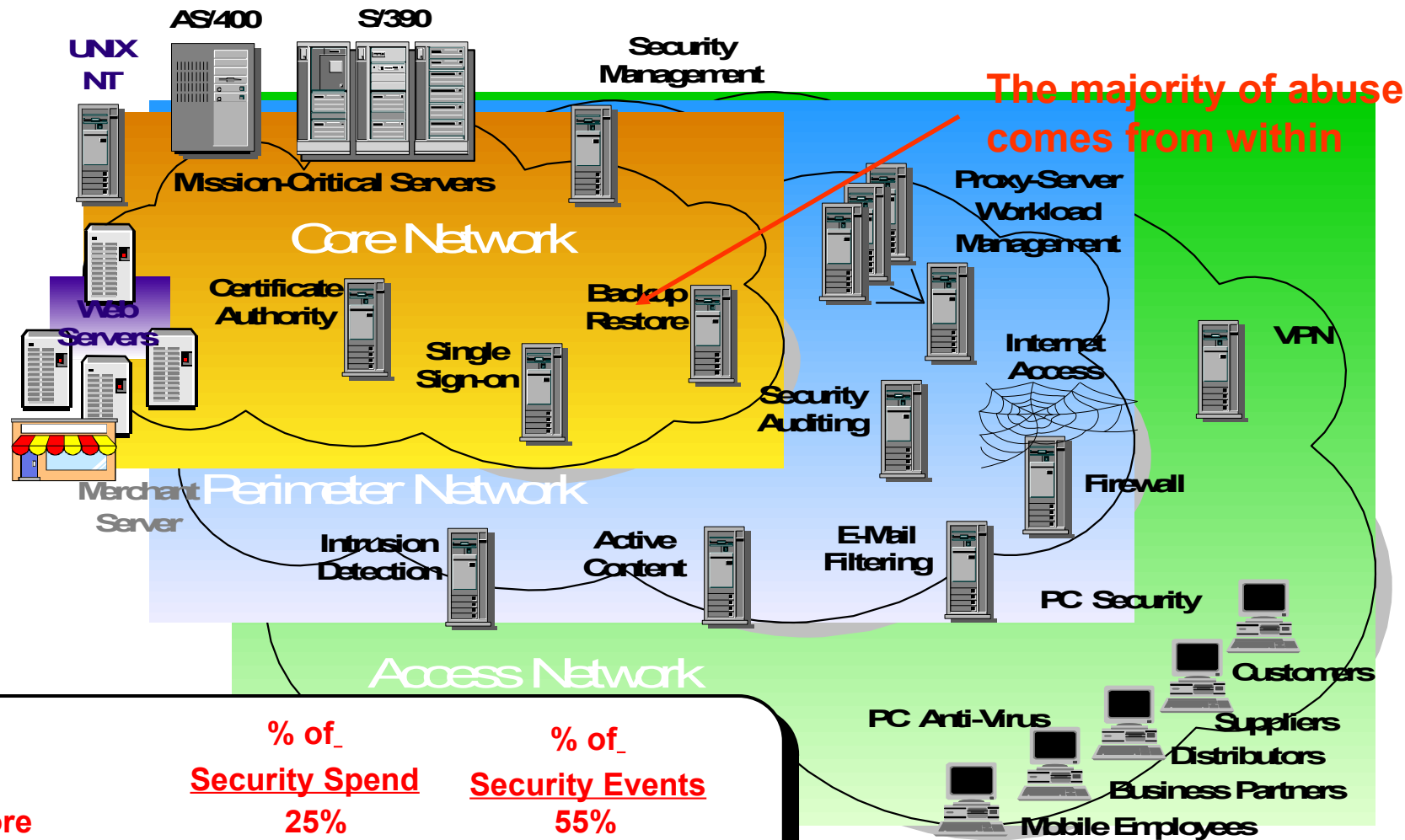
Ensuring full fledged security for your company

- **Common flaws**
- **Plugging holes**

Tivoli security management solutions

- IBM Tivoli Access Manager for Operating Systems
- IBM Tivoli Access Manager for e-business

The Total Security Map



	<u>% of Security Spend</u>	<u>% of Security Events</u>
Core	25%	55%
Perimeter	31%	} 45%
Access Network	44%	

Two Flaws Cause Security Vulnerabilities

Investment

General Server Vulnerabilities

Threats

Software Bugs

Misconfiguration

External
Vulnerability

Internal
Vulnerability

Best in Breed software

Simple policy installation

Frequent update policy

Easy to understand policy

Broad array of security products

Policies that cannot be subverted

Protection

Security Begins (and Ends) with Security Policy

Security Threats

Software bugs

Misconfiguration

Robust Security Policy

Policy Enforcement

- Frequently patch vulnerabilities

- Variety of 3rd party vendors & organizations

- Authenticate all users and programs
- Authorize all security sensitive kernel operations
- Protect the “Trusted Computing Base” from modification

- IBM Tivoli Access Manager

Agenda

Linux and security

- Common myths

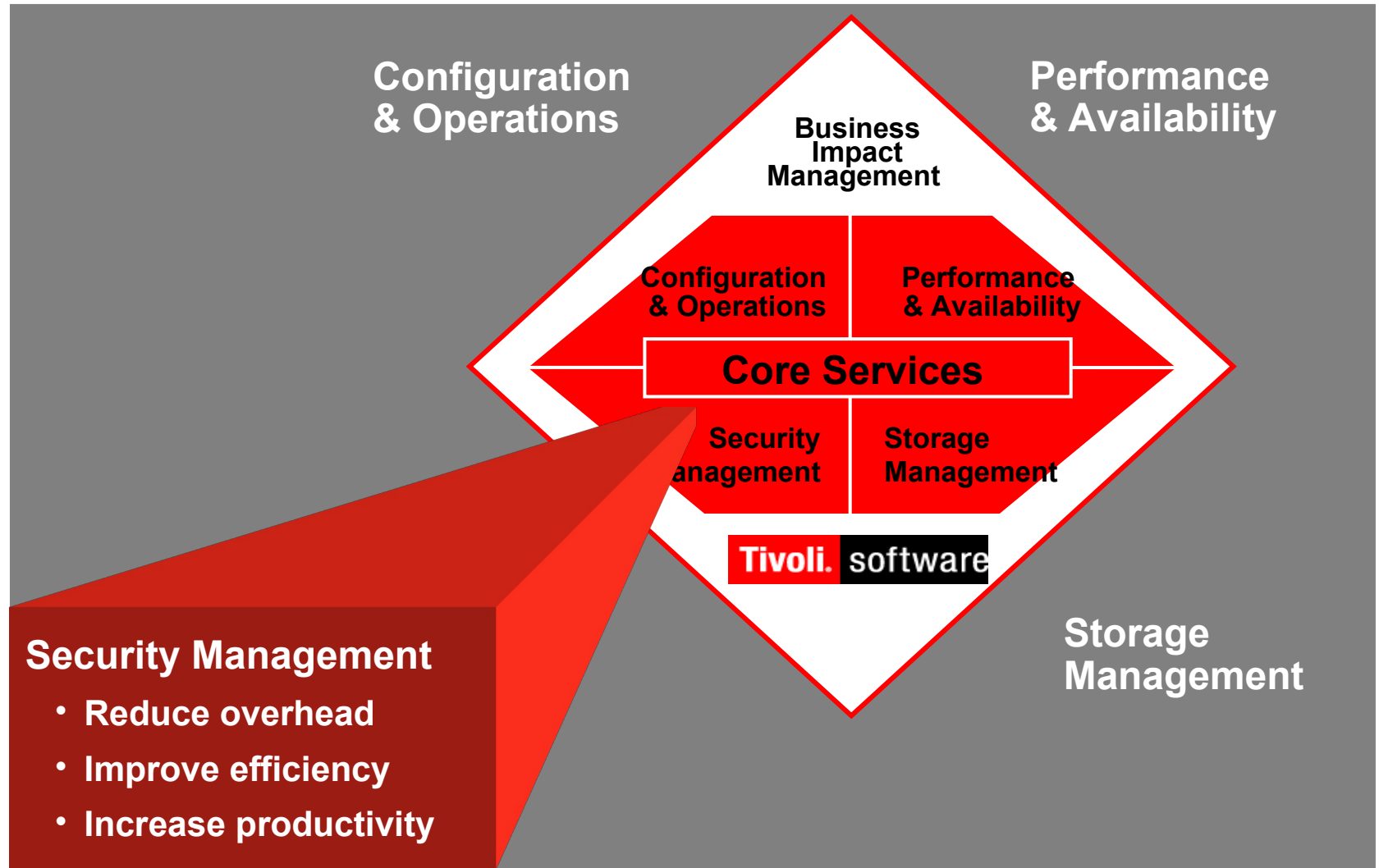
Ensuring full fledged security for your company

- Common flaws
- Plugging holes

Tivoli security management solutions

- **IBM Tivoli Access Manager for Operating Systems**
- **IBM Tivoli Access Manager for e-business**

IBM Tivoli Software Portfolio

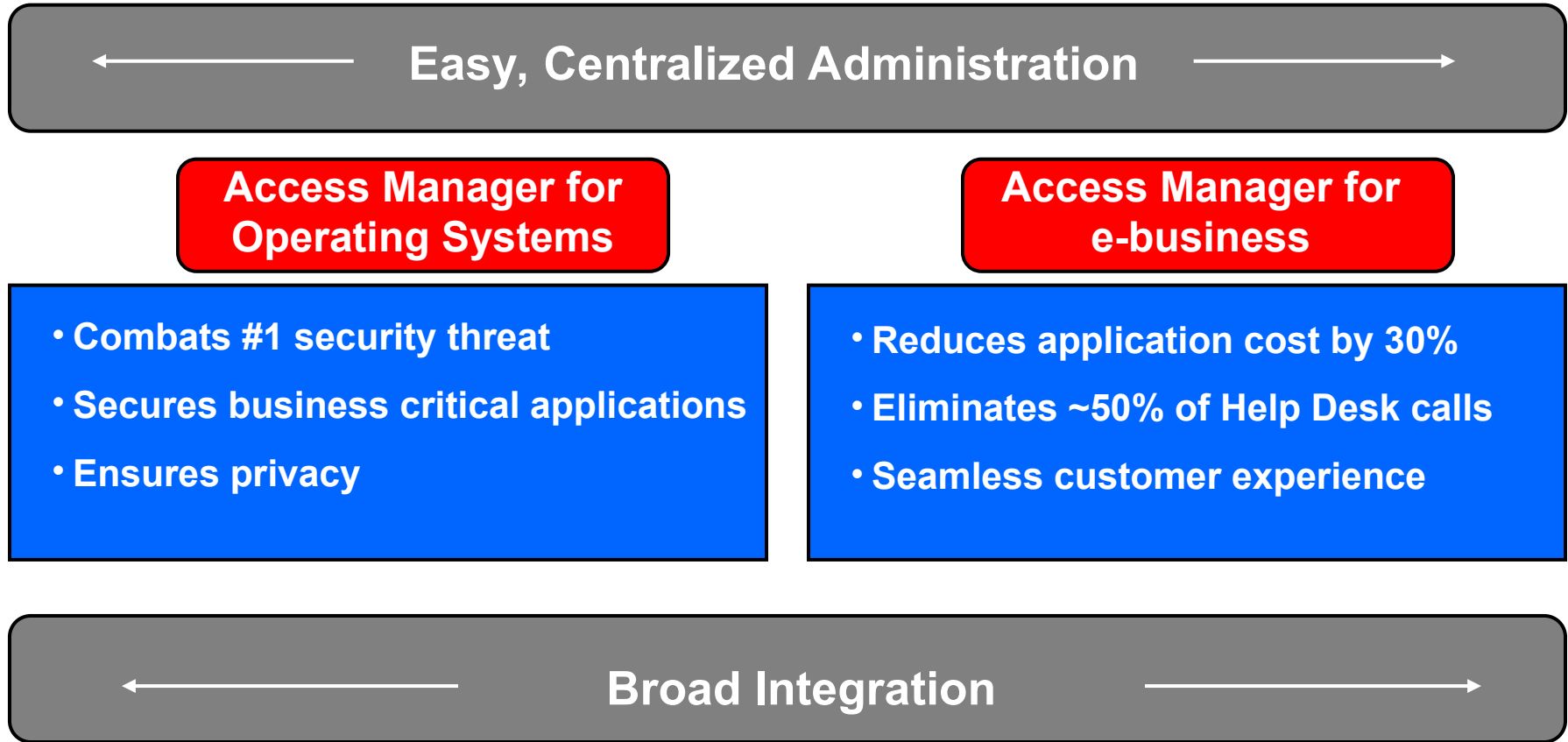


Customers Plagued by Multiple Security Challenges

<p>Provisioning Users</p>	<ul style="list-style-type: none"> • “45% of accounts are invalid”
<p>Managing Access Control</p>	<ul style="list-style-type: none"> • # 1 security threat results from inadequate controls on employees
<p>Protecting Privacy</p>	<ul style="list-style-type: none"> • “No systemic method of complying with customers’ privacy concerns”
<p>Synchronizing Information</p>	<ul style="list-style-type: none"> • “Large amounts of redundant, inaccurate, data clogs infrastructure”

Easy to Use, Integrated Tools for Rapid ROI

Foundational tools of secure environments



AMOS: Assurance for Key Relationships

Linux Security Challenges

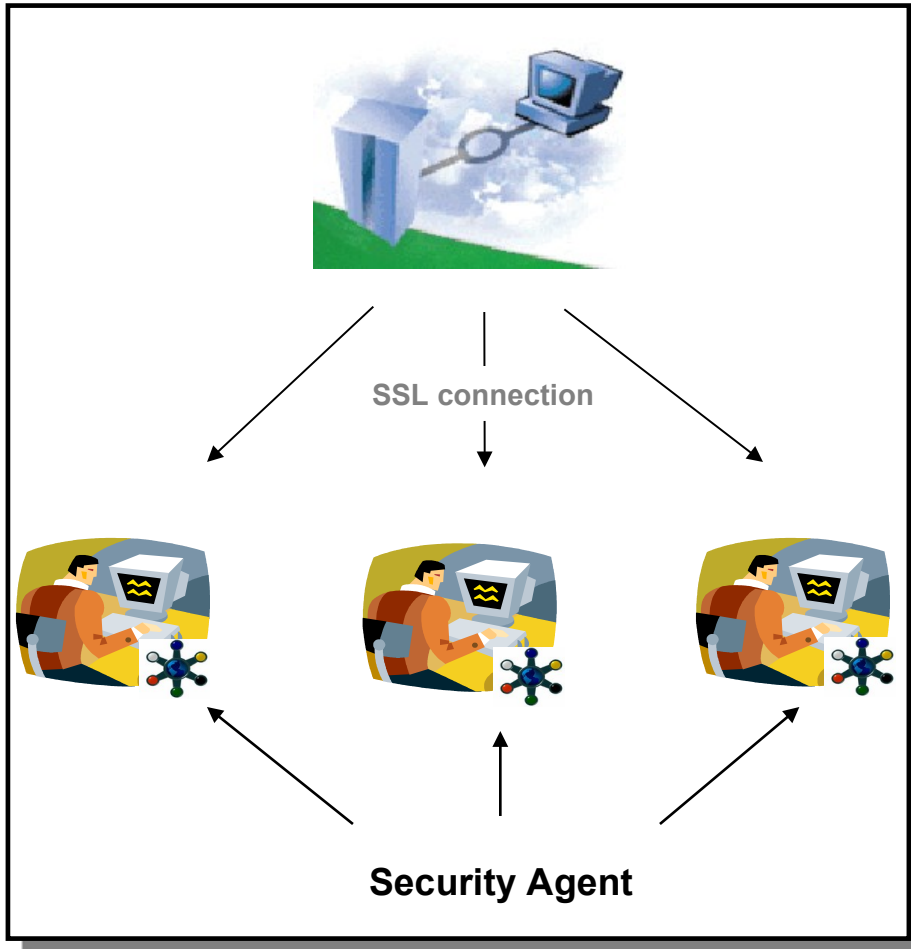
- **Application security is vulnerable, exposing private consumer and partner information**
- **Root users...**
 - **Have unlimited access**
 - **Can compromise audit data**
 - **Reduce accountability**
 - **Are common target for hacking**

Tivoli Response

- **Locks down applications at OS level**
- **Access Manager for Operating Systems**
 - **Limits access**
 - **Creates audit trail**
 - **Provides accountability**
 - **Presents poor target for hacking**

**Recently expanded
Linux coverage**

AMOS Relies on Simple Architecture



Access Manager Management Server
Centralized server contains

- Policy database
- User IDs

Management Server maintains policy
Security Agent enforces policy

Security Agent
Erects security perimeter

- Intercepts system call
- Make access decision
- Writes audit record

General Scenario: Joe Administrator

Action In UNIX In AMOS



Joe logs in • UID 1032 • joe UID 1032



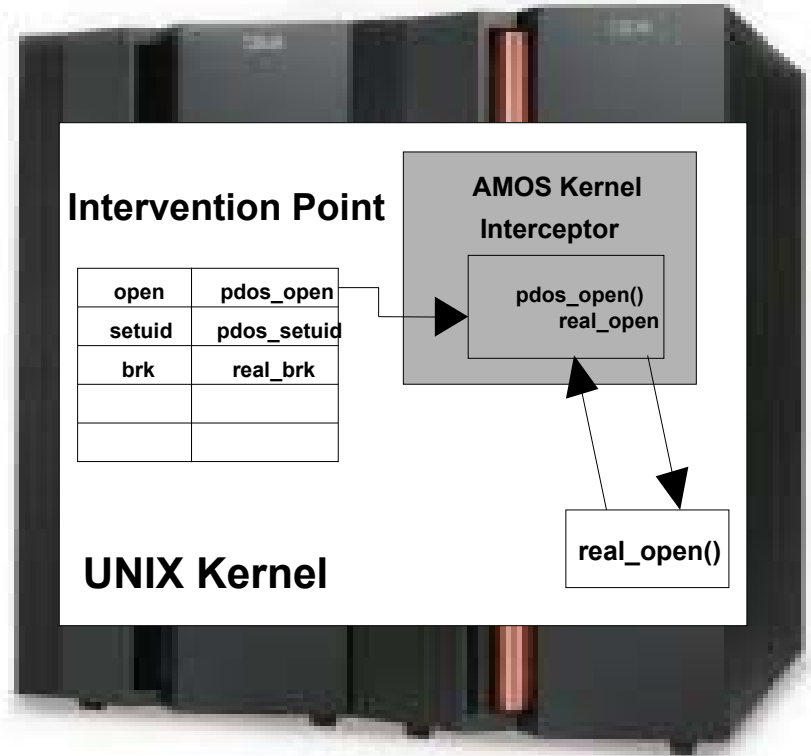
su to root • root UID 0 • joe UID 1032
 • Writes to audit log



INTERCEPTED!!!

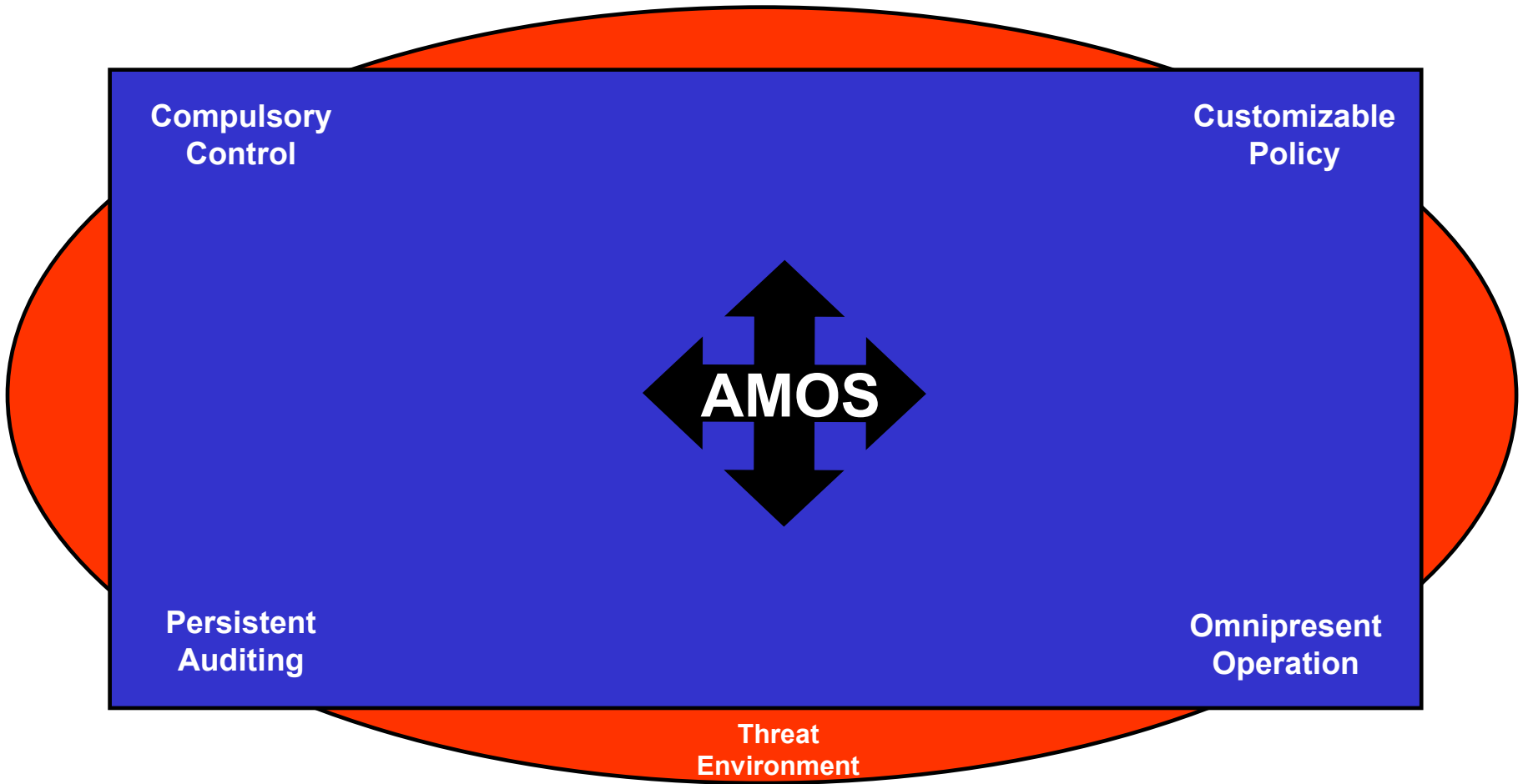
- Access = R, W
- Resource = /etc/passwd
- joe UID 1032

• Writes to audit log



- Tracks original login ID
- Audits at all times
- Applies control to each

AMOS Security Policy is Robust



Tivoli Access Manager for e-business

Multi-purpose security environment

- ***Centralized administration***
- ***Integrates with industry's leading solutions***
- ***Supports a secure e-business On-Demand infrastructure***

Access Manager for e-business

Web/URL

- URLs
- CGI Programs
- HTML files
- Java servlets
- Java class files

Web Servers

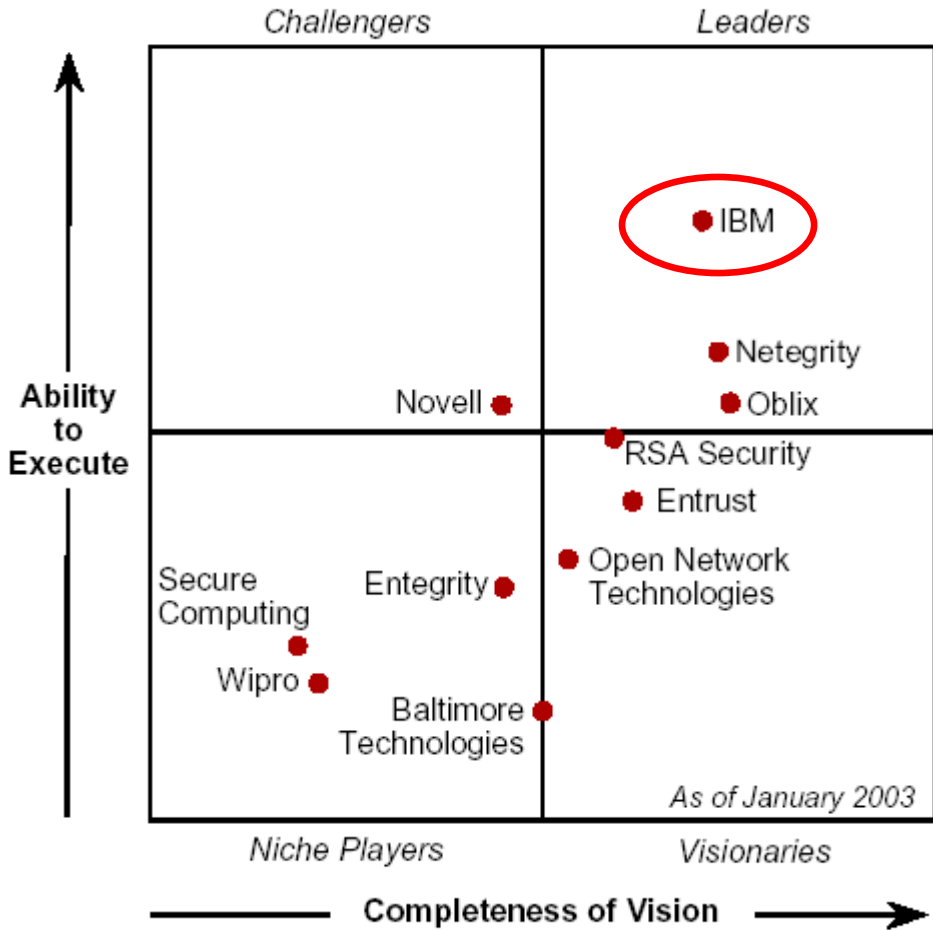
- IBM WebSphere
- BEA WebLogic
- *Any other via J2EE, JAAS, and/or API*

Portal / Web Solutions

- Plumtree
- WebSphere Portal Server
- BroadVision
- Vignette
- mySAP
- Lotus Domino
- and more . . .

Access Manager for e-business is Clear Leader

Extranet Access Management 2H02 Magic Quadrant



Ability to execute

- Robust technology
- Highly scalable
- Broad integration for comprehensive protection
 - Web pages
 - Web application servers
 - Portals

Complete Vision

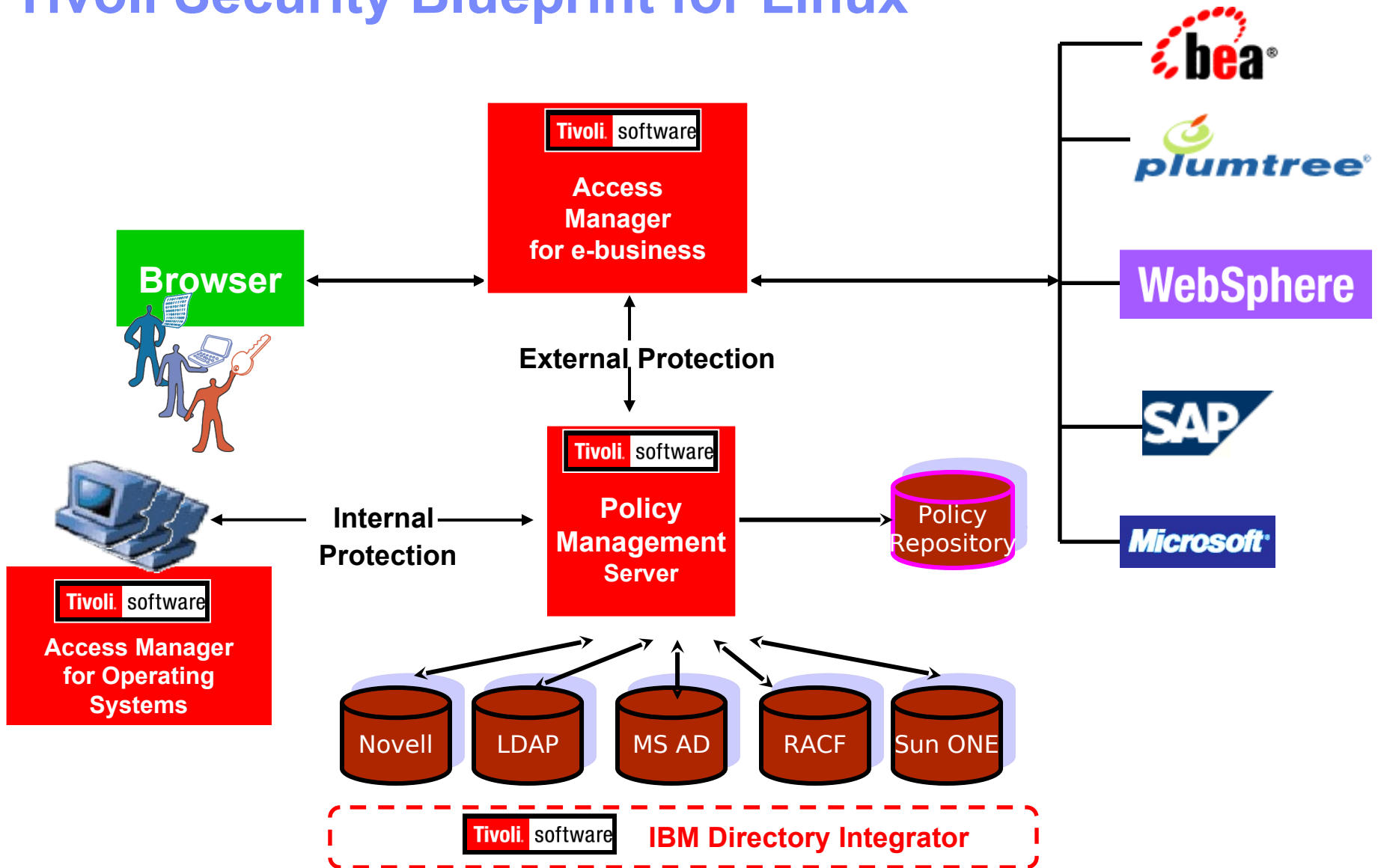
- Single sign on
- Cost reduction
- Identity management
- Federated identity
- Web services

Source: Gartner Research

January 8, 2003 Research Note "Extranet Access Management 2H02 Magic Quadrant" by John Pescatore and Ray Wagner

The magic quadrant is copyrighted January 2003 by Gartner, Inc. And is reused with permission. Gartner's permission to print or reference its magic quadrant should not be deemed to be an endorsement of any company or product depicted in the quadrant. The magic quadrant is Gartner's opinion and is an analytical representation of a marketplace at and for a specific time period. It measures vendors against Gartner-defined criteria for a marketplace. The positioning of vendors within a magic quadrant is based on the complex interplay of many factors. Gartner does not advise enterprises to select only those firms in the leaders segment. In some situations, firms in the visionary, challenger, or niche player segments may be the right match for an enterprise's requirements. Well-informed vendor selection decisions should rely on more than a magic quadrant. Gartner research is intended to be one of many information sources and the reader should not rely solely on the magic quadrant for decision-making. Gartner expressly disclaims all warranties, express or implied of fitness of this research for a particular purpose.

Tivoli Security Blueprint for Linux



Administration is Centralized and Easy

IBM Tivoli Access Manager

Task List

Browse Object Space

Refresh Tree Prune Tree

Path	ACL	POP
/	default-root	
+ BEA		
+ CRM		
+ IBM Solutions	default-IBM_Solutions	
+ Management	default-management	
+ OSSEAL		
+ PDMQ		
+ Portlets		
+ WebSEAL	default-webseal	
+ WebSphere		

Signed On User: sec_master [Sign Off](#) TIVOLI

Administration conducted through a Web GUI

- **Centralized administration with distributed access**

Delegated, hierarchical administration

- **Maximizes productivity**
- **Minimizes abuse**

Other Tivoli Products Support Linux

Tivoli Identity Manager

- Provides method of automating the provisioning of resources, privileges and rights to users
- Fully integrated with other Tivoli products
- Provides for substantial ROI in a short period of time
 - From 40-55% of Help Desk calls are for password related
 - Each call costs ~\$20
- Enhances security—up to 30-60% of customer accounts are invalid

Tivoli Privacy Manager

- Provides an automated method for companies to address consumers' privacy concerns
- Provides an automated method of complying with HIPAA
- Tags consumer data with “Business Use” profile, specifying ways in which consumer data can be used

IBM Tivoli Strongly Supports Open Security Standards

Web Services Security

- **WS-Security (OASIS)**
- **WS-Trust, WS-SecureConversation, WS-Policy**
- **XML Digital Signatures; XML Encryption; XKMS**

Federated Identity Management

- **Open standards**
- **Security Assertions Markup Language: SAML (OASIS)**
- **Kerberos**
- **Open interface to connect to Microsoft Trustbridge and Liberty Alliance technology**

Open or proposed open Java/Middleware Standards

- **J2SE (Java 2 Security Edition)**
- **JAAS (Java Authentication and Authorization Service) Programming Model**
- **JSSE (Java Secure Socket Extension)**
- **JCA (Java Cryptography Architecture)**
- **JCE (Java Cryptography Extension)**
- **CSIV2 (Common Security Interoperability)**
- **JSR115 for pluggable J2EE Container authorization**
- **Java 2 and JAAS**
- **aznAPI**

General Security Information

CERT for advisories on viruses, worms and vulnerabilities

- **<http://www.cert.org>**

SANS for general information on IT security

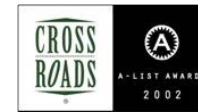
- **<http://www.sans.org>**

Industry recognition for Access Manager

- Finalist, Best in Show, LinuxWorld '03
- Winner, Mindcraft Extranet Performance Benchmark
- Winner, Gartner Leadership Quadrant
- Winner, 2002 Crossroads A-List Award
- Winner, Information Security Excellence Award
- Winner, Frost & Sullivan Market Excellence Award
- Winner, VARBusiness Annual Report Card
- Commended, SC Magazine 2002 Best Security Management



Gartner



Integration and partnerships

