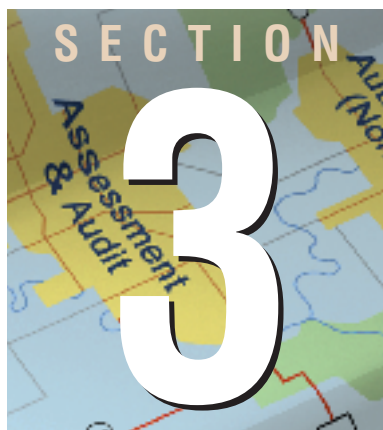


ASSESSMENT & AUDIT

3A IS AUDITING TOOLS



3A IS Auditing Tools

ERQ Audit

Advanced Software Products Group Inc. ERQ Audit allows the user to extract exactly the information requested, from one specific field (or portion of a field) up to entire SMF records. Retrieved information is stored in ISPF variables and tables that are easily accessed from any CLIST or REXX command procedure.

Price: Starts at \$7,500

Secure FTP

Advanced Software Products Group Inc. Secure FTP provides a full audit trail of all FTP commands that were executed or attempted and offers online monitoring of all active FTP sessions including the number of bytes being transferred. This solution secures an FTP command by utilizing user ID/password, originating IP address and target FTP server port.

Price: Contact vendor

Unused Account Ferret Anixis

Unused Account Ferret helps network admins quickly identify and remove unused user and computer accounts from a Windows domain. Unused Account Ferret can also delete the Microsoft Exchange mailboxes and home folders that are associated with the unused accounts.

Price: Starts at \$110/100-user domain

BizRights Approva

BizRights enables the management, analysis and monitoring of critical business transactions and processes within enterprise applications. It delivers operational visibility and continuous auditing, ensuring enterprise-wide adherence to internal business controls, resulting in

IN THIS SECTION	
3A	IS Auditing Tools 80
3B	Vulnerability Assessment Scanners 81
3C	Penetration Testing Tools 85
3D	Forensics Software 86
3E	Log Analysis Software 88
3F	Other Security Assessment Tools/Toolkits 89

compliance with business rules, regulations, policies and practices.

Price: Contact vendor

Firewall Informer Blade Software

Firewall Informer provides the ability to statefully send any network traffic protocol to and from any IP address via any ports bi-directionally. This enables complete testing and validation of a firewall rule set, to confirm exactly what traffic is allowed and blocked both ways through the firewall.

Price: Starts at \$4,800

IDS Informer Blade Software

IDS Informer is the first purpose-built solution designed to test the integrity and compliance of intrusion detection systems. IDS Informer helps configure all IDSes to ensure that they work efficiently and that false positives are reduced.

Price: Starts at \$5,000

LT Auditor+ Version 8.0 for Novell NetWare and Windows Blue Lance

LT Auditor+ ensures data privacy and protects against unauthorized access, theft of intellectual property and abuse of user privileges. Both NetWare and Windows versions feature 24/7 unobtrusive user and activity monitoring, powerful data filtering, real-time alerts, customizable reports, audit trail data protection and cross-platform consolidation.

Price: Subscription-based, contact vendor

Secure Shuttle Transport Boomerang Software

See entry under 2K

Consul/eAudit and MSM CONSUL Risk Management

Consul/eAudit automatically consolidates all network activity data in a central database, audits the data against active security policies and produces normalized reports that emphasize exceptions and attentions. Consul/MSM is an outsourcing of IT auditing mainly for small- to mid-sized organizations.

Price: Contact vendor

CoreNessus

Coresecure Inc.
See entry under 3B

Web-application Assessment Tools Deloitte & Touche Canada (Reseller)

See entry under 9B

Advanced NT Security Explorer ElcomSoft Co. Ltd.

See entry under 1E

eScan IntraWatch Emprise Technologies

See entry under 3B

Elkey

Global Technologies Group Inc.
See entry under 7E

GlobalAdmin Global Technologies Group Inc.

See entry under 2J

Information Security, Disaster Recovery Hart Systems

Hart Systems offers information security consulting, reviews physical and logical security and provides disaster recovery and business continuity plans after analysis, review, plan development and testing.

Price: Contact vendor

IBM Tivoli Privacy Manager for e-business IBM

See entry under 2I

AbsoluteTrack Inside the Box Inc.

AbsoluteTrack is a computer tracking and inventory management service that lets organizations simplify the management of software license compliance, computer leases, machine configuration, PC retirement, upgrades and device allocation.

Price: \$19.95/seat

NetIntelligence iomart

See entry under 6D

ASSESSMENT & AUDIT

Data Security Server (DSS)

IPLocks Inc.

See entry under 4B

I.C.U...OS/390

JANUS Associates Inc.

See entry under 3C

ScanDo

KaVaDo Inc.

See entry under 3B

McAfee Cybercop ASaP

Network Associates

CyberCop ASaP is an online vulnerability assessment service that remotely evaluates the security of network perimeter, DMZ and externally visible assets. CyberCop ASaP provides detailed reports to identify a network's security threats and proposes fixes that can be implemented by IT staff.

Price: Contact vendor

NGSSQLCrack

NGSSoftware Ltd.

Password auditing tool for Microsoft SQL Server standard logins. Performs dictionary, dictionary substitution and brute-force attacks to assess the strength of a user's password.

Price: \$295

NGSSQuirreL

NGSSoftware Ltd.

Security audit and management tool for Microsoft SQL Server. NGSSQuirreL generates lockdown scripts to help secure the server based upon the vulnerabilities found, easing the administrative burden and providing for a greater ROI. Supports detailed reporting, auditing of multiple hosts and intuitive GUI.

Price: Starts at \$755

StormFront

OKENA

See entry under 3D

Oracle Selective Audit

Oracle Corp.

Selective Audit is an Oracle consulting solution that provides capabilities to monitor user access to data within an Oracle database, including the ability to capture and play back SQL queries. Selective Audit provides security specialists with a means to manage and control auditing without involving the DBA. Available for Oracle8i/9i.

Price: Contact vendor

Intact

Pedestal Software

See entry under 5A

NTSEC

Pedestal Software

NTSEC is a set of command-line programs that allow system administrators to manage permissions on NTFS,

Registry, Share, Policies, Users and Groups. Administrators can control and view file and directory access control lists, registry security, and network printer and storage services.

Price: Contact vendor

PoliVec Scanner

PoliVec Inc.

PoliVec Scanner uses agentless technology to audit Windows NT/2000 systems for compliance with corporate security policy. Stays current with patches and hotfixes, remotely scans and changes system configurations, registry settings and services that are enabled. Manages NTFS and active directory servers.

Price: \$9,995/250 servers

PowerLock SecurityAudit

PowerTech Group

PowerLock SecurityAudit is software that allows you to set and manage a sound security policy within an iSeries environment. Internal and external auditors use PowerLock SecurityAudit to conduct comprehensive security analysis and obtain meaningful and accurate results.

Price: Contact vendor

Vulnerability Management Services

PricewaterhouseCoopers

See entry under 9E

Global Security

Pro-Defihse

See entry under 8B

Secure 4 Audit

S4Software Inc.

Some of the main features of Secure 4 Audit include ability to define multiple audit configuration files; use command-line interface with script files to perform any menu program function that can be run without operator intervention; hide the differences between Unix auditing variants; enable specific selection of audit events; consolidate audit information into standard reports; and archive audit files to remote systems.

Price: \$995-\$1,500

Risk Assessor for the iSeries 400

SafeStone Technologies Inc.

Risk Assessor enables external or internal auditing staff to perform accurate and in-depth auditing of the iSeries 400. It enables organizations to ensure all areas of the iSeries 400 are compliant with corporate, government and legislative security standards.

Price: Contact vendor

LANWatch

Sandstorm Enterprises Inc.

LANWatch is a customizable software-based network monitor and packet analyzer that displays network traffic in real time. It provides over 400 filters with which to isolate network traffic, and recognizes and decodes over 60 network

protocols.

Price: Starts at \$695

RedAlert

Savvydata Inc.

See entry under 4B

DetectIT

Secor

See entry under 2C

eTrust CA-Examine Auditing

Secure Logic LLC (Reseller)

See entry under 9B

ENVESTOnline

Security Automation Inc.

See entry under 8E

SilentRunner

SilentRunner Inc.

See entry under 3D

Vulnerability Assessment Reports

The Orkand Corp.

See entry under 3F

3B

Vulnerability Assessment Scanners

AppDetective

Application Security Inc.

AppDetective is a network-based, penetration testing/vulnerability assessment scanner that locates and assesses the security strength of databases within a network. AppDetective will locate, examine, report and help fix security holes and misconfigurations. Versions available for Microsoft SQL Server, Lotus Domino, Oracle and Sybase.

Price: Contact vendor

ISS Database Scanner

Best Internet Security (Reseller)

See entry under 9B

Automated Technical Vulnerability Assessment Services

Beyond Security Australia

Automated Technical Vulnerability Assessment Services are uniquely supported and operated from Australia by Beyond Security Australia. This service is suitable for assessing both external and internal computer networks. A comprehensive report is delivered within 24 hours, detailing existing technical (security) vulnerabilities with recommended solutions.

Price: Under \$200

3A/B
IS AUDITING
TOOLS/
VA SCANNERS

ASSESSMENT & AUDIT

External Network Security Monitoring

Catbird Networks
See entry under 3C

SecureReview

Digital Inc.

Cigital's SecureReview identifies specific risks in software code and suggests mitigation strategies that lead to increased levels of security and integrity.

Price: Contact vendor

eTrust Policy Compliance

Computer Associates

eTrust Policy Compliance is a vulnerability assessment tool that allows organizations to develop and enforce enterprise-wide security policies and provide appropriate audit-ready documentation.

Price: Starts at \$200

CoreNessus

Coresecure Inc.

CoreNessus is a Web-automated vulnerability scanning service.

Price: Starts at \$50/month

Enterprise Vulnerability Management Solutions

Critical Watch

See entry under 9A

DrawBridge

CyberNet Defense

DrawBridge is a vulnerability assessment technology that allows organizations of all sizes to mitigate the risk of exploitation from known security vulnerabilities. The DrawBridge Smart-Filter allows for elimination of false positives and recurring variables in the reporting process, while providing a detailed summary of each vulnerability and multiple mitigation options.

Price: Monthly subscription, contact vendor

Vulnerability Assessment Scanners

Deloitte & Touche Canada (Reseller)

See entry under 9B

ipLegion

E*Maze Networks

ipLegion is a vulnerability assessment tool with a Web-command interface, remote scanning, software expandability for intranet control, complete installation in customer data center for large network or particular need.

Price: Contact vendor

EdgeSecure Advanced Scan

Edgeos

Edgeos' EdgeSecure platform, tools for vulnerability assessment and initial penetration testing, is fully automated and functions remotely. Admins can log in to the EdgeSecure Web site and enter IP address(es) to analyze.

Price: \$25/IP address

Retina Enterprise

eEye Digital Security

Retina Enterprise was developed as an enterprise-class network security scanning solution with centrally managing event logs. Retina Enterprise consists of an event management server and a help desk application.

Price: Contact vendor

Retina Network Security Scanner

eEye Digital Security

Retina is a network security scanner that can scan every machine on a network, including a variety of OSes, networked devices and third-party or custom applications.

Price: Starts at \$995

eScan IntraWatch

Emprise Technologies

eScan IntraWatch is an appliance that provides continuous, on-demand network vulnerability assessment. A GUI allows customers to initiate scheduled or ad hoc scans of the internal or external network. Detailed reports indicate vulnerabilities discovered, risk levels and suggested resolutions.

Price: Starts at \$10,000/annual subscription

FoundScan Enterprise Vulnerability Management System

Foundstone Inc.

See entry under 4A

GFI LANguard Network Security Scanner

GFI Software Ltd.

This security scanner checks the network for all potential methods that a hacker might use to attack. It analyzes the OS and applications running on the network and determines all the possible security holes.

Price: Starts at \$249/up to 50 IPs

Everguard System

Gibraltar Software Inc.

See entry under 4C

Harris STAT Scanner

Guardian Technologies LLC

Harris STAT Scanner performs a complete security assessment of Windows NT/2000/XP and Unix/Linux resources. With a mouse click, STAT Scanner performs a complete analysis of a single machine or an entire domain.

Price: Starts under \$1,000

STAT Analyzer

Harris Corp.

STAT Analyzer is a network risk assessment solution that automates and correlates multiple network modeling/scanning tools to perform an assessment of a network's security risk, providing a single, accurate and repeatable output. STAT Analyzer generates exportable reports

ranging from high-level summaries to detailed descriptions of vulnerabilities and suggestions for fixes.

Price: Contact vendor

STAT Scanner

Harris Corp.

STAT Scanner Professional Edition is a vulnerability assessment solution that detects more than 2,000 vulnerabilities and enables analysis, reporting and correction of found vulnerabilities for Windows NT/95/98/ME/2000/XP, Sun Solaris Unix and Red Hat/Mandrake Linux environments.

Price: Contact vendor

HSC TSAR

Hervé Schauer Consultants

TSAR is a vulnerability assessment service based on Nessus and Babelweb. Each test is monitored by a security consultant, who provides advice and support to an organization's management.

Price: Starts at \$490

Database Scanner

Internet Security Systems

The Database Scanner application assesses online business risks by identifying security exposures in leading database applications. Database Scanner offers security policy generation and reporting functionality, which measures policy compliance and automates the process of securing critical online business data.

Price: Starts at \$3,995

Internet Scanner

Internet Security Systems

The Internet Scanner application provides network vulnerability assessment for measuring online security risks. Internet Scanner performs scheduled and selective probes of communication services, operating systems, applications and routers to uncover and report systems vulnerabilities that might be open to attack.

Price: Starts at \$650/subscriber license for 10 IPs

System Scanner

Internet Security Systems

The System Scanner application ensures policy compliance and detects vulnerabilities that leave servers open to compromise. System Scanner measures, manages and enforces security policies across a wide range of operating systems.

Price: Starts at \$695

Wireless Scanner

Internet Security Systems

See entry under 5D

ActiveSentry

Intranode Software Technologies

ActiveSentry helps companies determine if their systems are adequately equipped to cope with the latest types of attacks.

Price: Contact vendor

3B VULNERABILITY ASSESSMENT SCANNERS

ASSESSMENT & AUDIT

3B VULNERABILITY ASSESSMENT SCANNERS

ScanDo KaVaDo Inc.

ScanDo is a comprehensive scanner that audits the Web application environments (Web servers, application servers, business logic, etc.) to uncover known and unknown vulnerabilities. Its AutoPolicy technology sends this information directly to KaVaDo's Web Application Protection product, InterDo, to automate the process of creating or updating security configuration.

Price: Contact vendor

StillSecure Server VAM Latis Networks Inc.

Server VAM offers a multitude of vulnerability scans at customizable intervals, providing an accurate view of a dynamically changing infrastructure down to the OS level. Its built-in workflow environment allows tracking and assignment of security vulnerabilities from identification to repair. The reporting engine delivers customizable reports appropriate to specific audiences.

Price: Contact vendor

Vulnerability Assessment Scanning mwr InfoSecurity

mwr InfoSecurity's best-of-breed vulnerability scanners are tailored to individual client needs. mwr InfoSecurity can customize scanners and reports in parallel to reflect sensitive criteria.

Price: Contact vendor

N-Stealth HTTP Security Scanner N-Stalke Inc.

N-Stealth is a Web vulnerability assessment tool that performs more than 19,000 security checks. It features Cyclops Web Log Analyser, N-Stealth Miner (for custom Web applications), false positive filters, CVE-compatible e-mail report launcher, SANS/FBI Top 20 and online database update.

Price: Starts at \$250/server

nCircle IP360 Network Exposure Management System nCircle Network Security

See entry under 5B

iNETPATROL

Network Security Systems

iNETPATROL is an Internet-based system for testing the vulnerability of external computer networks to unauthorized entry. This Web-based managed service ensures that users are running the most up-to-date test suite without having to download or install additional software.

Price: Starts at \$995

LANPATROL

Network Security Systems

LANPATROL is a rackmounted and notebook security appliance for testing the vulnerability of internal computer networks to unauthorized entry. This hardware/software appliance installs

quickly anywhere on the network, allowing vulnerability assessments and penetration testing in a matter of minutes.

Price: Starts at \$9,995

DominoScan NGSSoftware Ltd.

Comprehensive Application Security Assessment Scanner (iASAS) for auditing Lotus Domino Web servers. Understands and assesses custom Domino applications for security holes, areas that traditional VA tools can't cover. Uses a technique developed by NGSSoftware to remotely enumerate each database's structure to find all security issues. Detailed reporting and analysis.

Price: Starts at \$1,500

NGSSquirrel NGSSoftware Ltd.

See entry under 3A

OraScan NGSSoftware Ltd.

Application Security Assessment Scanner (iASAS) for auditing Oracle Web servers. Understands and assesses custom PL/SQL and JSP applications for security holes, areas that traditional VA tools can't cover. Works by cataloging the site and searches for vulnerabilities such as SQL Injection, source code access and Oracle specific issues.

Price: Starts at \$755

Typhon II NGSSoftware Ltd.

Traditional host-based vulnerability assessment scanner. Ideal for security baselining remote hosts and searching for common vulnerabilities in service software. Scan modules include Web, MS SQL, Oracle, FTP, SMTP, SNMP, NetBIOS, LDAP, SSH and DNS. Supports scanning of multiple hosts and HTML reporting.

Price: Starts at \$1,500

VigilEnt Security Manager

PentaSafe Security Technologies Inc.

See entry under 4A

VigilEnt Security Agent

PentaSafe Security Technologies, Inc. VigilEnt Security Agent automates and consolidates auditing and security management across one or more databases. The Agent provides powerful security auditing, user management, password management and reporting that is otherwise impossible or extremely time-consuming with native database security tools. Agents available for databases (Oracle, SQL and Sybase), FireWall-1, iSeries, NetWare, Unix, Web servers and Windows.

Price: Varies

Vulnerability Assessment

Primexus Inc. (Reseller)

See entry under 9B

QualysGuard Qualys

QualysGuard is a Web-based service that delivers automated, scalable security auditing and risk assessment of global networks, inside and outside firewalls. QualysGuard reduces security admins' time researching, scanning and fixing network exposures and enables companies to proactively eliminate network vulnerabilities before they can be exploited.

Price: \$15,000-\$45,000

QualysGuard Intranet Scanner Qualys

The QualysGuard Intranet Scanner is a vulnerability assessment appliance that gives admins automated, Web-based security audit capabilities for internal networks. The Intranet Scanner provides the inside perspective visible to internal hackers and malcontents behind the firewall.

Price: \$2,995

SAINT 4.0 SAINT Corp.

SAINT 4.0 is an all-inclusive vulnerability assessment tool that features comprehensive reports, automatic updates and flexible scanning capabilities.

Price: Contact vendor

AppScan 3.5 Sanctum Inc.

AppScan Web application security testing and vulnerability assessment tool explores applications, automatically creates and customizes tests and provides comprehensive actionable results through detailed and custom reports. AppScan delivers application life cycle security to help improve application development ROI and reduce business risk.

Price: Contact vendor

PhoneSweep and PhoneSweep Gold Sandstorm Enterprises Inc.

See entry under 3C

ScanAlert ScanAlert

See entry under 3F

Penetration Testing and Vulnerability Assessment Secor

See entry under 9F

SITI Secure Computing

SITI is an assessment tool that detects vulnerabilities within a company's network. A detailed report gives an overview of the vulnerabilities and offers step-by-step instructions for prioritizing and eliminating security risks. SITI tests for more than 3,000 vulnerabilities.

Price: \$650/IP address

ASSESSMENT & AUDIT

Retina Network Security Scanner
Skyhawk Consulting Inc. (Reseller)
See entry under 9B

eV3TM
Solutionary Inc.
See entry under 9A

SonicWALL Vulnerability Scanning Service
SonicWALL

SonicWALL Vulnerability Scanning Service is a Web-based subscription service that provides assessment of over 730 security threats by testing networks from the hacker's view. Scans can be scheduled on a regular basis or triggered on demand.

**Price: \$104/NFR 10-pack;
\$3,995/distributed enterprise pack**

SpectraSecure
Spectracomm Inc.

Network security evaluation service gives organizations a clear picture of current IT security vulnerability and alerts them to potential intrusions. Security tool also provides the foundation for implementing security remedies.

Price: \$5,000

WebInspect
SPI Dynamics

WebInspect dynamically scans standard and proprietary Web applications to identify all vulnerabilities, regardless of environment.

**Price: \$4,995/server
perpetual licensing**

System Security Services
SYTEX Inc.

See entry under 9D

Detective
Tech Assist Inc.
See entry under 3D

Cyberscope Scanner
Venus Info Tech Inc.

Cyberscope Scanner is a vulnerability assessment system that can be integrated with Cybervision IDS and managed by Cybervision IDS console.

Price: \$1,000-\$20,000

SecureScan NX
VIGILANTe

SecureScan NX's architecture implements a centralized console to manage remote test engines and probes, making it easy for admins to quickly and repeatedly scan and report vulnerabilities in distributed networks from a single location.

Price: Contact vendor

SecureScan Perimeter
VIGILANTe

The SecureScan Perimeter service beats hackers to the punch by vigilantly probing Internet-connected systems for vulnerabil-

ities before they find them. It identifies holes in an Internet infrastructure, scanning beyond the firewall to any device with an IP address.

Price: Contact vendor

SecureScan SP
VIGILANTe

SecureScan SP users can enjoy an unprecedented level of managed security through the ongoing testing of internal and public-facing IP addresses. SecureScan SP enables organizations to provide users or customers with an ongoing assessment service, allowing them to be tested as frequently as they find suitable to meet the requirements of their security policy.

Price: Starts at \$100,000

3C

Penetration Testing Tools

AppDetective
Application Security Inc.
See entry under 3B

External Network Security Monitoring
Catbird Networks

Catbird monitors a network's outer edge, Web site, e-transactions for security vulnerabilities (e.g., firewall and port vulnerabilities and SSL) and performance. No software or hardware is required, as Catbird monitors from outside the network.

Price: Contact vendor

CORE IMPACT

Core Security Technologies
CORE IMPACT is an infosec risk assessment product that streamlines the penetration testing process.

Price: Contact vendor

ipLegion
E*Maze Networks

See entry under 3B

EdgeSecure Advanced Scan
Edgeos

See entry under 3B

IBM Intrusion Detection Services
IBM

IBM's managed security services monitor networks 24/7, using intrusion detection tools from Axent, Cisco and ISS.

Price: \$37,000/year

I.C.U...OS/390

JANUS Associates Inc.
I.C.U...OS/390 is a penetration assessment tool for mainframes, working in conjunction with the OS/390 operating system and RACF.

Price: Contact vendor

Penetration Testing
mwr InfoSecurity
See entry under 9F

INETPATROL
Network Security Systems
See entry under 3B

LANPATROL
Network Security Systems
See entry under 3B

DominoScan
NGSSoftware Ltd.
See entry under 3B

OraScan
NGSSoftware Ltd.
See entry under 3B

Typhon II
NGSSoftware Ltd.
See entry under 3B

ProCheckNet
ProCheckUp Ltd.

ProCheckNet is a managed security service that helps organizations identify their business exposure to threats from the Internet. ProCheckNet utilizes AI-based attack technology to perform a comprehensive penetration test on a company's Internet gateways, firewalls, IDSes and Web servers.

Price: Contact vendor

PhoneSweep and PhoneSweep Gold
Sandstorm Enterprises Inc.

PhoneSweep was the world's first commercial telephone scanner (also known as a war dialer). It can identify more than 470 kinds of remote access systems. With PhoneSweep, users can find security leaks in corporate modem pools and find unauthorized modems.

**Price: Starts at
\$1,176/PhoneSweep;
\$1,750/PhoneSweep Gold**

SITI
Secure Computing
See entry under 3B

Active Network Monitor
SmartLine Inc.
See entry under 3D

WebInspect
SPI Dynamics
See entry under 3B

Superior Healthcare Security Solutions
Superior Consultant Co.

A suite of health care security solutions services that include assessment/strategy components, security penetration and vulnerability testing; HIPAA/best practices security assessments; security strategy and road map formulation and disaster recovery/business continuity.

3B/C
VA SCANNERS/
PENETRATION
TESTING TOOLS

ASSESSMENT & AUDIT

Includes best-of-breed solutions, awareness training; SSL server certificates; health care digital certificates; compliance management; health care identity management; disciplinary status and network monitoring.

Price: Contact vendor

TigerSuite
TigerTools.net Inc.
See entry under 3F

3D Forensics Software

eTrust Audit
Computer Associates
See entry under 3E

Advanced Archive Password Recovery

ElcomSoft Co. Ltd.

This software recovers lost or forgotten passwords for ZIP, ARJ, RAR and ACE archives. It supports the customizable brute-force attack, effectively optimized for speed (up to 15 million passwords per second on Pentium III); dictionary-based attack; and known plaintext attack. For most WinZip archives, guaranteed decryption is available.

Price: \$60

Advanced Lotus Password Recovery

ElcomSoft Co. Ltd.

This program recovers lost or forgotten passwords to files/documents created in IBM/Lotus applications (all versions): Organizer, WordPro, 1-2-3 and Approach. Multilingual passwords are supported.

Price: \$60

Advanced Office XP Password Recovery Pro

ElcomSoft Co. Ltd.

See entry under 1E

Advanced PDF Password Recovery Pro

ElcomSoft Co. Ltd.

See entry under 1E

Advanced WordPerfect Office Password Recovery

ElcomSoft Co. Ltd.

A program to recover lost or forgotten passwords to Corel WordPerfect Office documents for all versions up to 2002.

Price: \$30

NetWitness

Forensics Explorers, a division of CTX NetWitness is an integrated forensics solution providing comprehensive automated analysis that identifies violations of network usage, known and unknown, whether from a trusted insider or from an external source, so an organization

can effectively and quickly understand the source of violation and take action.

Price: \$7,500-\$60,000

Forensic IT Research

Fox-IT

Fox-IT gathers digital evidence on computers, networks and the Internet to solve digital crimes, including digital fraud. This includes analysis of data storage media and interception and analysis of network traffic. All work is performed according to forensic guidelines and results are suitable for use as evidence in a court.

Price: Contact vendor

DataLifter v2.0

Granite Communications Inc. DataLifter v2.0 Forensic Support Tools are a collection of useful programs for computer forensics. Tools include active reports, disk cataloging, file extraction, image linker, Internet cache and history agent, file signature generator, e-mail retrieve, recycle bin history, screen capture and disk-free space recovery tool.

Price: \$120

ICS Image MASter Solo 2 Forensic

Granite Communications Inc. The Solo 2 Forensic system is a handheld software duplication device made for computer disk drive data seizure. Image-capture operations can be performed from a suspect's drive to another hard drive with duplication speeds up to 1.8 GB/minute.

Price: \$1,450-\$2,750

ICS Link MASter

Granite Communications Inc. ICS Link MASter offers solutions to seize evidence from an unopened notebook or PC with USB, IEEE 1394 or CardBus port to an external hard drive. Boot suspect PC/notebook with included diskettes or CD-ROM. It's independent of suspect OS and is compatible with Forensic Tool Kit, EnCase and Unix-DD. It also prints an audit trail.

Price: Contact vendor

ICS Road MASter

Granite Communications Inc. ICS Road MASter is a portable computer forensic evidence seizure, preview and analysis system that supports any Windows-based forensic software package for field use.

Price: \$5,500

EnCase Enterprise Edition

Guidance Software

EnCase Enterprise Edition is an enterprise-wide incident response, information auditing and forensic discovery solution. Leveraging the functionality of Guidance Software's flagship product, EnCase Forensic Edition, the patent-pending technology enables clients to identify, preview, acquire and analyze digital

media anywhere on the network.

Price: Contact vendor

EnCase Forensic Edition

Guidance Software

The EnCase Forensic Edition allows law enforcement and IT professionals to conduct powerful, yet completely noninvasive computer forensic investigations. Validated by the courts, the EnCase Forensic Edition features can view all relevant files, including deleted files, file slack and unallocated space.

Price: Contact vendor

FacTracker

Kroll Ontrack Inc.

With Kroll Ontrack FacTracker, users take preliminary computer investigation into their own hands. FacTracker gives clients the power to investigate and discover electronically produced evidence related to legal matters.

Price: Starts at \$595

enVision Software

Network Intelligence Corp.

See entry under 3E

Private I Software

Network Intelligence Corp.

See entry under 3E

StormFront

OKENA

StormFront analyzes and helps to protect any business application by analyzing its actual operation. Using OKENA's StormWatch agent to intercept operating system calls made by an application, StormFront will identify undesired or malicious activity from that application. StormFront can create security policies for enforcement by the StormWatch agent, enabling incident remediation or application protection. Because this analysis is based on actual, observed behavior, it allows analysis and protection of any application.

Price: \$10/desktop; \$200/server

NetIntercept

Sandstorm Enterprises Inc.

Sandstorm's NetIntercept is a network forensics analysis tool that captures and archives network traffic, reassembles TCP streams into sessions, and drills down through multiple layers of encryption, compression and transfer encoding. NetIntercept parses over 80 types of data streams, including common productivity software and multimedia file formats. Discovers employee abuse, monitors network use, detects anomalies and assesses network risks.

Price: Starts at \$7,500

SilentRunner

SilentRunner Inc.

SilentRunner is a network security analysis solution that helps organizations track and investigate the movement of data

3D
FORENSICS
SOFTWARE

3D FORENSICS SOFTWARE/ LOG ANALYSIS

across networks. Used to investigate theft and abuse of critical information assets at more than 150 Fortune 1000 companies and government entities worldwide.

Price: Starts at \$25,000

Active Network Monitor SmartLine Inc.

Active Network Monitor is a NT/2000/XP tool for the day-to-day monitoring of computers in the network that allows systems administrators to gather information from all the computers in the network without installing server-side applications on these computers.

Price: \$30

Remote Task Manager SmartLine Inc.

Remote Task Manager is a systems control interface that can be run from any remote Windows NT/2000/XP computer. This enables a systems administrator to control most aspects of a remote environment.

Price: \$40

Computer Forensics Training—Online Southeast Cybercrime Institute

See entry under 8C

Byte Back Tech Assist Inc.

This computer forensic and imaging tool clones any size drive of an operating system. Featuring MD5 hashing, it has risk-free data recovery utilities for automatic and manual boot, and partition repair and file recovery.

Price: \$599

Detective Tech Assist Inc.

This computer forensic tool reveals the past by scanning drives for keywords including deleted temporary Internet files and cache. Runs from floppy across a network or single machine.

**Price: \$199/single drive;
\$995/unlimited drives**

ProDiscover DFT Technology Pathways LLC

ProDiscover DFT offers forensics examiners an integrated Windows application for the collection, analysis, management and reporting of computer disk evidence. ProDiscover DFT was designed by experts to support all four phases of computer forensics and is an ideal tool for civil, criminal or corporate forensics.

Price: \$495

Contego TriGeo Network Security

See entry under 4B

NEXT Witness WetStone Technologies Inc.

Network EXpert Time (NEXT) Witness is a Web-based forensic data collection tool that captures, seals and time stamps Web

ASSESSMENT & AUDIT

site content. By creating these secure records, analysts and investigators can ensure their digital evidence will provide a complete audit trail of court-acceptable data.

Price: Contact vendor

SMART Extractor WetStone Technologies Inc.

SMART Extractor is a software tool that provides for the recovery of deleted i-nodes from Linux EXT2 file systems. It also collects and reports information regarding the recovered data to include deletion time stamps, file size, owner, type, group, creation, last accessed and last modified time stamps.

Price: Contact vendor

Stego Watch WetStone Technologies Inc.

Stego Watch is a computer forensics investigative tool used by analysts to detect steganography hidden in digital image files. Stego Watch is offered as either a monitoring/scanning service or a stand-alone software package.

Price: Contact vendor

3E Log Analysis Software

LT Auditor+ Version 8.0 for Novell NetWare and Windows

Blue Lance
See entry under 3A

eTrust Audit Computer Associates

eTrust Audit collects enterprise-wide security and system audit information without reduced performance and overwhelming network traffic. It consolidates data from Unix and Windows NT servers, as well as other eTrust products, and stores it in a central database.

Price: Starts at \$200

Point Secure for VMS Computer Communications Ltd.

See entry under 2E

Consul/eAudit and MSM CONSUL Risk Management

See entry under 3A

CoreIDS Coresecure Inc.

See entry under 5A

Log Analysis Software Deloitte & Touche Canada (Reseller)

See entry under 9B

Linux Log Analyzer Fly-By-Day Consulting Inc.

The Linux-based log file analyzer and alerter analyzes Linux systems' log files (firewalls, routers, servers) and generates e-mail and pager alerts as necessary so protective action may be taken.

Price: Starts at \$499

NetWitness Forensics Explorers, a division of CTX

See entry under 3D

GFI LANguard Security Event Log Monitor (S.E.L.M.) GFI Software Ltd.

See entry under 5A

NetCocoon Analyzer Matsushita Electric Works Ltd.

See entry under 3F

N-Stealth HTTP Security Scanner N-Stalke Inc.

See entry under 3B

enVision Software
Network Intelligence Corp.
enVision is a network event management solution tailored for enterprise networks. enVision leverages log data from network and security devices and delivers real-time warnings, reports and analysis of network activity, while offering the ease of Web-based user interfaces, multiuser features and role-based user management.

Price: Contact vendor

Network Intelligence Engine Network Intelligence Corp.

See entry under 4B

Private I Software
Network Intelligence Corp.
Private I software is tailored for the SMB. Private I leverages device log data from network and security devices and delivers real-time warnings, reports and analysis of network activity, while offering the ease of Web-based user interfaces, multiuser features and role-based user management.

Price: Contact vendor

VigilEnt Intrusion Manager/Log Analyzer PentaSafe Security Technologies Inc.

See entry under 4B

LogSentry
Psionic Technologies
LogSentry (formerly Logcheck) automatically monitors system logs and mail security violations to admins on a periodic basis. LogSentry is a clone of a program that ships with the TIS Gauntlet firewall, but has been changed to make it work for normal system auditing.

Price: Free

ASSESSMENT & AUDIT

**Guard Tower Security
Correlation Appliance**
Secure Commerce Systems
See entry under 4A

SecureScope
Secure Decisions
See entry under 4B

3F Other Security Assessment Tools/Toolkits

Secure FTP
Advanced Software Products Group Inc.
See entry under 3A

SecurITree
Amenaza Technologies Ltd.
See entry under 9E

Professional Security Services
ARC IAI Inc.
See entry under 9E

Firewall Informer
Blade Software
See entry under 3A

IDS Informer
Blade Software
See entry under 3A

Hailstorm
Cenzic Inc.
See entry under 4D

Cisco Catalyst 6500 Network Analysis Modules Cisco Systems

These security modules for the Catalyst 6500 Series modular chassis provide up to 1 Gbps performance capabilities and deliver integrated traffic monitoring for full visibility into applications, hosts, VOIP and QoS. This information is critical to better use resources, detect anomalies and isolate network problems.

Price: Starts at \$17,995

eTrust Policy Compliance
Computer Associates
See entry under 3B

ECM Security Update Manager
Configuresoft Inc.
See entry under 4C

Consul/zAdmin for RACF
CONSUL Risk Management
Consul/zAdmin for RACF enables security officers to automate many of the recurring functions of system administration by enhancing the native RACF authorization and delegation capabilities. Consul/zAdmin identifies problems in RACF such as missing or inconsistent definitions, and fixes or prevents mistakes before they become threats to security.

Price: Contact vendor

Consul/zAudit ACF2
CONSUL Risk Management
Consul/zAudit ACF2 provides auditors, operations analysts and system programmers with reporting and analysis functions that allow them to make certain the security of the system is sound. It shows the ACF2 Logon IDs and identifies questionable definitions, lists the Access Rules by rule or rule line, displays the global systems options and highlights dangerous settings.

Price: Contact vendor

3F OTHER SECURITY ASSESSMENT TOOLS/TOOLKITS

ASSESSMENT & AUDIT

Design-Level Security Assessment DYONYX

See entry under 9E

Iris Network Traffic Analyzer eEye Digital Security

Iris is a network traffic analyzer that allows users to examine the inner workings of their network. Iris takes network traffic such as e-mails, instant messages, Web pages and more, and returns it to its original format with the click of a button.

Price: \$995

DAG 3.5, 3.6D, 4.2, 4.2GE

Endace Measurement Systems

DAG 3.5, 3.6D, 4.2 and 4.2GE network monitoring and surveillance cards enable header-only or full-packet capture, at full line rate with no packet loss. Packets are time and date stamped to better than 100ns resolution through synchronization to CDMA or GPS.

Price: Contact vendor

Advisor

eSecurityOnline

Advisor, eSO's vulnerability management appliance, auto-discovers assets and performs auto-inventory of software. Advisor then correlates those assets and technologies with Ernst & Young's vulnerability knowledgebase to provide systems admins with an asset-specific task list prioritized by risk.

Price: \$32,500

Framework

eSecurityOnline

See entry under 4E

Forensic IT Research

Fox-IT

See entry under 3D

ICS Road MASter

Granite Communications Inc.

See entry under 3D

Managed Incident Response and Forensics

Guardent

Guardent's Incident Management and Response Services enable organizations to respond quickly to computer-related security incidents.

Price: Contact vendor

Managed Vulnerability Protection Service

Guardent

See entry under 9F

Harris STAT Scanner Guardian Technologies LLC

See entry under 3B

STAT Analyzer

Harris Corp.

See entry under 3B

IBM System Security Assessment IBM

IBM's System Security Assessment provides a review of the operating system security controls in place.

Price: \$10,000-\$30,000

Panache

InfoTek Security Consultants

Panache is a risk-assessment tool that uses the HMG Infosec Standard 1 methodology and a countermeasure library based on BS 7799 Part 1 and CRAMM. Standard, professional and enterprise versions are available.

Price: \$1,000

CRAMM

Insight Consulting Ltd.

CRAMM Version 4.1, the globally adopted Information Security Officers Toolkit, comprising: CRAMM Risk Assessment Tool; an updated and enhanced library of over 3,000 countermeasures; BS 7799 Tool; report wizards; contingency planning tool; and CRAMM 'Express' function for high-level assessments.

Price: Contact vendor

Database Scanner

Internet Security Systems

See entry under 3B

Internet Scanner

Internet Security Systems

See entry under 3B

System Scanner

Internet Security Systems

See entry under 3B

IAM

Itillious Inc.

See entry under 9E

Professional Services

Jefferson Wells Int'l

See entry under 9I

NetCocoon Analyzer

Matsushita Electric Works Ltd.

NetCocoon Analyzer is the verification tool of IPsec interoperability. This software can analyze the IPsec, ISAKMP, ARP, IP, ICMP, UDP, IPX, etc. With a known key, you can decrypt the encrypted messages.

Price: \$5,000

Application Assessment Tool

NETSEC

Consisting of an integrated suite of Web application security analysis procedures, NETSEC's application assessment tool is not only an integral part of Web application development, but also enables security auditors, application developers and quality assurance engineers to identify vulnerabilities and logic errors within applications.

Price: Contact vendor

Information and Network Security NetWorks Group

NetWorks Group provides information security and networking products and services to medium-sized businesses and Fortune 500 companies. It integrates best practices and skilled project management to deliver network security solutions.

Price: Contact vendor

DiskAmnesia Pro

Professional Help Computer

Services Inc.

See entry under 2K

Secure 4 Audit

S4Software Inc.

See entry under 3A

ScanAlert

ScanAlert

Verification of servers being hacker safe by conducting daily, remote security audit scans.

Price: \$79.95/month/server

Policy Expert

Secoda Risk Management

See entry under 4D

SonicWALL ViewPoint

SonicWALL

SonicWALL ViewPoint reporting software provides administrators instant insight into network security status and easy-to-understand historical reports on a comprehensive set of monitored functions. ViewPoint reporting software's Web-based interface simplifies deployment and maximizes productivity by turning any secure Internet connection into a monitoring and reporting console.

**Price: \$595/Appliance Upgrade;
\$895/GMS Entry Edition Upgrade**

Secure Copy

Sunbelt Software (Reseller)

See entry under 9B

Security Explorer

Sunbelt Software (Reseller)

See entry under 9B

Service Explorer

Sunbelt Software (Reseller)

See entry under 9B

Risk Assessment Tool

Symantec (China)

Tool can be used to assess the asset, threat and vulnerability quantitatively.

Price: Contact vendor

Byte Back

Tech Assist Inc.

See entry under 3D

weakPasswords

The Halonen Co.

See entry under 1E

3F
OTHER SECURITY
ASSESSMENT
TOOLS/TOOLKITS

ASSESSMENT & AUDIT

Vulnerability Assessment Reports

The Orkand Corp.

The Orkand Corp. utilizes top industry professionals to provide reports for technical assessments, including C&A work for GISRA, PDD-63, NIST, DITSCAP and NICAP. It uses a suite of proprietary and COTS tools.

Price: Contact vendor

TigerSuite

TigerTools.net Inc.

TigerSuite security audit tools are available for the PC platform and Pocket PC and Windows CE handhelds. The software includes modules for remote scanning, service detection and penetration testing. The suite is compatible with both wireless and LAN Internet and/or network connections.

Price: \$14.95-\$69

Xacta Commerce Trust

Xacta Corp.

See entry under 4A

ZixAuditor

Zix Corp.

An assessment service that examines and analyzes an organization's inbound and outbound e-mail communications to identify regulated, high-risk or proprietary content. ZixAuditor is built around a sophisticated lexicon that enables the identification of messages that contain legal, health, financial, human resources and other legally protected or valuable proprietary information.

Price: \$20,000

3F

OTHER SECURITY
ASSESSMENT
TOOLS/TOOLKITS