Software Product Description

PRODUCT NAME: POLYCENTER Security Intrusion Detector for SunOS, Version 1.0 **SPD 43.09.00**

DESCRIPTION

POLYCENTER Security Intrusion Detector (ID) for SunOS is a real-time security monitoring application for the SunOS operating system. It performs knowledge-based analysis of the output of the audit subsystem to recognize and respond to security-relevant activity. Violations such as attempted logins, unauthorized access to files, illegal setuid programs, and unauthorized audit modifications are automatically detected and acted upon. This frees the system or security manager to tackle more important end-user problems.

Most security breaches involve a series of actions. Instead of looking at each action individually, ID for SunOS looks at the whole picture. Using a case method modeled after criminal investigations, ID assigns an agent to monitor the suspect and file evidence to the case. By analyzing each security event within the context of a case, ID can distinguish between real threats and innocent behavior. So ID won't kick legitimate users off the system or trigger false alarms.

POLYCENTER Security ID for SunOS can be configured to take countermeasures against intruders without human intervention, and security managers can work from the Manager's Graphical User Interface or from the UNIX command line.

POLYCENTER Security ID for SunOS does the following:

- Runs on every SPARC Sun system in a network to detect and take action in real-time on intruders—whether malicious hackers or inadvertent users.
- Uses a built-in knowledge base to automatically interpret the audit log data.
- Notifies security managers about critical security events occurring on a system, as detected from the SunOS Audit Subsystem.

The following is a list of these events:

  - — Access-control-event — A failed attempt to modify the protection of any file or the successful modification of the protection of a critical file
  - — Account-auth-event — Successful and unsuccessful password changes to nonprivileged user accounts
  - — Audit-subsystem-event — The start or termination of the operating system's audit facility or changes to the system and user audit controls
  - — Breakin-event — Successive login failures
  - — File-transfer-event — A network file copy
  - — Logfail-event — A failed login
  - — Login-event — A successful login
  - — Obj-access-event — A failed attempt to access any file or device or the successful modification of a critical file
  - — Privileged-process-creation-event — Gaining privilege by running a SUID-to-root program that is not registered as a critical file
  - — Process-termination-event — Logouts and any exiting of a monitored process
  - — Program-execution-event — Execution of a program that has been recently modified
- Tailored automatic countermeasures, per a master configuration file which the security manager sets up at the time of product installation, can include:
  - — Sending mail to designated security managers
  - — Further monitoring the security-relevant actions of the offender
  - — Re-enabling of audit data generation
  - — Shutting down an offending process

- Filters a large volume of audit data, reducing it to a manageable set of relevant information for the system manager to review, permitting more frequent archiving of old data which ultimately means less disk space is used.
- Can be started and operated from Digital's POLYCENTER Framework for centralized system and network management.
- Produces daily or weekly summaries of security-relevant activity.
- Security-relevant activity of several SunOS and ULTRIX nodes can be monitored from one designated Manager Interface node, giving the security manager the ability to control a larger number of machines with less people.

Additional POLYCENTER Security Software

- POLYCENTER Security Intrusion Detector for OpenVMS (SPD 41.27.00)
- POLYCENTER Security Intrusion Detector for ULTRIX (SPD 43.07.00)
- POLYCENTER Security Compliance Manager for OpenVMS (SPD 26.N1.01)
- POLYCENTER Security Compliance Manager for ULTRIX (SPD 41.26.00)
- POLYCENTER Security Compliance Manager for SunOS (SPD 41.25.00)
- POLYCENTER Security Compliance Manager for HP-UX (SPD 46.12.00)
- POLYCENTER Security Compliance Manager for IBM AIX (SPD 46.11.00)
- POLYCENTER Security Reporting Facility for OpenVMS (SPD 26.N2.01)

HARDWARE REQUIREMENTS

Processor and/or hardware configurations as specified in the System Support Addendum (SSA 43.09.00-x).

SOFTWARE REQUIREMENTS

SunOS Operating System V4.1.1 or V4.1.2
Basic Security Module (BSM)
OpenWindows V2.0 or V3.0

Refer to the System Support Addendum (SSA 43.09.00-x) for availability and required versions of prerequisite /optional software.

ORDERING INFORMATION

Software Licenses: QL-NB8A*-**
Software Media: QA-NB8A*-**
Software Documentation: QA-NB8A*-GZ
Software Product Services: QT-NB8A*-**

* Denotes variant fields. For additional information on available licenses, services, and media, refer to the appropriate price book.

SOFTWARE LICENSING

This software is furnished under the licensing provisions of Digital Equipment Corporation's Standard Terms and Conditions. For more information about Digital's licensing terms and policies, contact your local Digital office.

SOFTWARE PRODUCT SERVICES

In addition to standard Software Product Support remedial services, consulting services for planning, designing, and implementing a custom security system are also available.

A variety of service options are available from Digital. For more information, contact your local Digital office.

SOFTWARE WARRANTY

As with any security product, POLYCENTER Security ID for SunOS software should be considered part of an overall security plan. Customers are encouraged to follow industry-recognized security practices and not rely on any single security product or service to provide complete protection.

Warranty for this software product is provided by Digital with the purchase of a license for the product as defined in the Software Warranty Addendum of this SPD.

System Support Addendum

PRODUCT NAME: POLYCENTER Security Intrusion Detector for SunOS, Version 1.0 **SSA 43.09.00-B**

HARDWARE REQUIREMENTS

Processors Supported:

Sun 4/110, 4/150, 4/260, 4/280
SPARCstation 2

The following processors have not been tested. However, as they support the SunOS Basic Security Module (BSM), it is expected that this product will run on these processors.

SPARCstation SLC,
SPARCstation IPC,
SPARCstation IPX,
SPARCstation 1,
SPARCstation 1+,
SPARCsystem 330,
SPARCsystem 470,
SPARCserver 390,
SPARCserver 490

Other Hardware Required:

To install POLYCENTER Security Intrusion Detector for SunOS software, the system must support a QIC tape drive.

Disk Space Requirements

Disk space required for installation:

Base Kit:	2,000 Kbytes
Manager Interface:	2,000 Kbytes
POLYCENTER Framework Kit:	50 Kbytes

Disk space required for use (permanent):

Manager Interface:	2,000 Kbytes
POLYCENTER Framework Kit:	50 Kbytes

These counts refer to the disk space required on the system disk. The sizes are approximate; actual sizes may vary depending on the user's system environment, configuration, and software options.

SOFTWARE REQUIREMENTS

SunOS Operating System V4.1.1 or V4.1.2
Basic Security Module (BSM)
OpenWindows V2.0 or V3.0

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the minimum requirements for the current version.

DISTRIBUTION MEDIA

18-track QIC 150 streaming tape
CD–ROM

ORDERING INFORMATION

Licenses: QL-NB8A*-**
Software Media: QA-NB8A*-**
Software Documentation: QA-NB8A*-GZ
Software Product Services: QT-NB8A*-**

* Denotes variant fields. For additional information on available licenses, services, and media, refer to the appropriate price book.

The above information is valid at time of release. Please contact your local Digital office for the most up-to-date information.