Software Product Description

PRODUCT NAME: POLYCENTER Security Intrusion Detector for ULTRIX, Version 1.0 **SPD 43.07.00**

DESCRIPTION

POLYCENTER Security Intrusion Detector (ID) for ULTRIX is a real-time security monitoring application for the ULTRIX RISC 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 ULTRIX 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 and, therefore, ID will not kick legitimate users off the system or trigger false alarms.

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

POLYCENTER Security ID for ULTRIX

- Runs on every ULTRIX RISC system in a network to detect and take action on intruders—whether malicious hackers or inexperienced users – in real-time.
- 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 ULTRIX audit subsystem. The following is a list of these events:
  - access-control-event – A failed attempt to modify the protection of any file and the successful modification of the protection of a critical file
  - account-auth-event – A creation or modification of a user account, including a password change
  - audit-subsystem-event – A change to the audit subsystem including queries of the audit state, starting or stopping of auditing, changes to system and user audit levels
  - breakin-event – Successive login failures
  - database-auth-event – Access to an authorization database
  - file-transfer-event – An rcp-based 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 and 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, or using the su utility
  - process-id-change-event – A change in the audit-id of a process
  - process-termination-event – Logouts and any exiting of a monitored process
  - program-execution-event – Execution of a critical program that has been recently modified
- Has tailored automatic countermeasures that include:
  - sending mail to designated security officers
  - turning account auditing back on if it was turned off
  - 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, permits more frequent archiving of old data and ultimately means less disk space usage.

- 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.
- Allows security-relevant activity of several ULTRIX RISC nodes to be monitored from one designated Manager Interface node, giving the security manager the ability to monitor a larger number of machines with less people.

ADDITIONAL POLYCENTER SECURITY SOFTWARE

- POLYCENTER Security Intrusion Detector for OpenVMS (SPD 41.27.xx)
- POLYCENTER Security Intrusion Detector for SunOS™ (SPD 43.09.xx)
- POLYCENTER Security Compliance Manager for OpenVMS (SPD 26.N1.xx)
- POLYCENTER Security Compliance Manager for ULTRIX (SPD 41.26.xx)
- POLYCENTER Security Compliance Manager for SunOS (SPD 41.25.xx)
- POLYCENTER Security Compliance Manager for HP®-UX (SPD 46.12.xx)
- POLYCENTER Security Compliance Manager for AIX® (SPD 46.11.xx)
- 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 43.07.00-x).

SOFTWARE REQUIREMENTS

For Systems Using Terminals

ULTRIX Operating System

For Workstations

ULTRIX Worksystem Software

Refer to the System Support Addendum (SSA 43.07.00-x) for availability and required versions of prerequisite software.

ORDERING INFORMATION

Software Licenses: QL-NB7A9-AA
Software Media: QA-NB7AA-H*
Software Documentation: QA-NB7AA-GZ
Software Product Services: QT-NB7A*-**

* 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.

License Management Facility Support

This layered product supports the ULTRIX License Management Facility.

License units for this product are allocated on an Unlimited System Use basis.

For more information on the License Management Facility, refer to the ULTRIX Operating System Software Product Description (SPD 26.40.xx) or the *Guide to Software Licensing* in the ULTRIX Operating System documentation set.

SOFTWARE PRODUCT SERVICES

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

In addition to standard SPS remedial services, consulting services for planning, designing, and implementing a custom security system are also available. For more information, contact your local Digital office.

SOFTWARE WARRANTY

As with any security product, POLYCENTER Security ID for ULTRIX 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.

® AIX is a registered trademark of IBM.

® HP is a registered trademark of Hewlett-Packard Company, Inc.

™ SunOS is a trademark of Sun Microsystems, Inc.

™ The DIGITAL Logo, DEC, DECstation, DECsystem, Digital, OpenVMS, POLYCENTER, TK, ULTRIX, and are trademarks of Digital Equipment Corporation.

System Support Addendum

PRODUCT NAME: POLYCENTER Security Intrusion Detector for ULTRIX, Version 1.0 **SSA 43.07.00-A**

HARDWARE REQUIREMENTS

RISC-Based Processors Supported:

DECstation: DECstation 2100,
DECstation 3100,
DECstation 3100s

Personal DECstation 5000 Model 20/25 MX,
Personal DECstation 5000 Model 20/25 HX,
Personal DECstation 5000 Model 20/25 TX,
Personal DECstation 5000 Model 20/25 PXG+,
Personal DECstation 5000 Model 20/25 PXG Turbo+

DECstation 5000 Model 120/125/133 MX,
DECstation 5000 Model 120/125/133 CX,
DECstation 5000 Model 120/125/133 HX,
DECstation 5000 Model 120/125/133 PX,
DECstation 5000 Model 120/125/133 TX,
DECstation 5000 Model 120/125/133 PXG,
DECstation 5000 Model 120/125/133 PXG+,
DECstation 5000 Model 120/125/133 PXG Turbo,
DECstation 5000 Model 120/125/133 PXG Turbo+

DECstation 5000 Model 200 MX,
DECstation 5000 Model 200 CX,
DECstation 5000 Model 200 HX,
DECstation 5000 Model 200 PX,
DECstation 5000 Model 200 TX,
DECstation 5000 Model 200 PXG,
DECstation 5000 Model 200 PXG+,
DECstation 5000 Model 200 PXG Turbo,
DECstation 5000 Model 200 PXG Turbo+

DECstation 5000 Model 240 MX,
DECstation 5000 Model 240 HX,
DECstation 5000 Model 240 TX,
DECstation 5000 Model 240 PXG+,
DECstation 5000 Model 240 PXG Turbo+

DECsystem: DECsystem 3100,
DECsystem 5000 Model 25,
DECsystem 5000 Model 200,
DECsystem 5000 Model 240,
DECsystem 5100,
DECsystem 5400,
DECsystem 5500,
DECsystem 5810,
DECsystem 5820,
DECsystem 5830,
DECsystem 5840,
DECsystem 5900

Other Hardware Required:

To install POLYCENTER Security ID software, the system must support a CD-ROM reader or tape drives for either TK50 tapes or 9-track magnetic tape media.

Disk Space Requirements:

Disk space required for installation:	4,500 Kbytes
Disk space required for use (permanent):	4,500 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

For Systems Using Terminals

ULTRIX Operating System V4.0 - V4.3

For Workstations

ULTRIX Worksystem Software V4.0 - V4.3

ULTRIX Tailoring:

The ULTRIX Enhanced Security Features subset must be installed, however POLYCENTER Security ID for ULTRIX does not require that the user be running at the ULTRIX enhanced security level.

For more information on ULTRIX customization, refer to the ULTRIX Operating System Software Product Description (SPD 26.40.xx).

digital™

April 1993

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

9-track 1600 BPI Magtape, TK50 Streaming Tape

This product is also available as part of the ULTRIX Consolidated Software Distribution on CD-ROM.

The software documentation for this product is also available as part of the ULTRIX Online Documentation Library on CD-ROM.

ORDERING INFORMATION

Software License: QL-NB7A9-AA
Software Media: QA-NB7AA-H*
Software Documentation: QA-NB7AA-GZ
Software Product Services: QT-NB7A*-**

* 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.

® AIX is a registered trademark of IBM.

® HP is a registered trademark of Hewlett-Packard Company, Inc.

™ SunOS is a trademark of Sun Microsystems, Inc.

™ The DIGITAL Logo, DEC, DECstation, DECsystem, Digital, OpenVMS, POLYCENTER, TK, ULTRIX, and are trademarks of Digital Equipment Corporation.