

# Software Product Description

**Product Name: POLYCENTER Security Compliance Manager  
for NetWare, Version 1.0**

**SPD 62.80.00**

## DESCRIPTION

POLYCENTER™ Security CM for NetWare® is a software tool that a security or system manager uses to establish a custom security analysis and reporting system. With this tool, the security manager can implement and maintain a security standard for the NetWare file servers in a distributed computing environment that is consistent with corporate security policy.

Customers can purchase security consulting services that help them to design and implement a security analysis and reporting system, which balances business needs with security requirements. Local Digital™ offices can help customers to determine the appropriate services for their requirements.

POLYCENTER Security CM does the following:

- Checks compliance to a security standard
- After a simple installation, runs unattended on the NetWare server
- Generates reports that help the system manager develop system compliance

Security managers define tests to examine the settings of operating system parameters that are relevant to the security of the system. These tests ensure that the operating system parameters comply with the organization's security policy. Using POLYCENTER Security CM's command line interface, these tests are grouped into inspectors, which are run regularly to test for compliance with the security policy.

POLYCENTER Security CM provides tests to examine the following categories of system settings:

- File and directory protections
- Accounts
- Passwords
- Intrusion detection

- Network

Inspectors arrange tests hierarchically into subsystems, test collections, and tests. The system settings that POLYCENTER Security CM tests are defined as parameters for the tests within the inspector. When POLYCENTER Security CM executes inspectors, it generates the following:

- Reports — POLYCENTER Security CM generates reports, summarizing the results of the inspection, for each inspector.
- Lockdown scripts — POLYCENTER Security CM generates lockdown scripts that can help you to reset parameters that do not comply with the requirements of the inspector.
- Unlockdown scripts — POLYCENTER Security CM generates unlockdown scripts that can help you to reverse the operation of the corresponding lockdown file. POLYCENTER Security CM generates a corresponding unlockdown script every time it generates a lockdown script.
- Tokens — POLYCENTER Security CM generates tokens after executing a special type of inspector. This inspector is called the Required Inspector and is described in the following paragraph. Tokens contain summaries of the results of the Required Inspector. POLYCENTER Security CM transmits these tokens to a POLYCENTER Security Reporting Facility (POLYCENTER SRF) node. POLYCENTER SRF extracts the data from the tokens and stores it in a relational database. Designated users can access this information to monitor the security compliance of all the servers in a network.

There are two types of inspectors: the Required Inspector and customized inspectors.

The Required Inspector is the inspector that POLYCENTER Security CM uses to test the compliance of the system with the security baseline in force. It defines the basic security settings that are required for compliance with an organization's baseline security standard. The POLYCENTER Security CM database contains at most one Required Inspector on each NetWare server. The database may also contain several customized inspectors.

Customized inspectors do not generate tokens, but the local system manager uses them for specialized testing.

The following list describes some situations in which customized inspectors may be useful:

- Before executing the Required Inspector — If the Required Inspector is copied to a customized inspector, the system's security compliance can be tested without sending tokens to the POLYCENTER SRF node. Users can correct security weaknesses before POLYCENTER Security CM performs an inspection using the Required Inspector.
- After installing or upgrading the operating system.
- When inexplicable modifications to file protections are discovered.
- When security compromises are suspected — Inspect the system using a customized inspector if daily audit reports reveal suspicious security events.

While POLYCENTER Security CM is effective when used alone in small distributed systems, managing the security of a large number of nodes is difficult. POLYCENTER Security CM software, used with POLYCENTER SRF software, can solve this problem. POLYCENTER SRF software is designed to run on one or more nodes to support the centralized collection and management of compliance information from POLYCENTER Security CM installations. It provides centralized management for distributed POLYCENTER Security CM client nodes. POLYCENTER SRF extracts data from tokens sent by servers running POLYCENTER Security CM and maintains this data in a relational database for management reporting. For more information about managing network security, see the POLYCENTER SRF Software Product Description (SPD 26.N2.xx).

#### *Additional Security Products*

The following is a list of related security products:

- 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 AIX (SPD 46.11.xx)
- POLYCENTER Security Compliance Manager for HP-UX (SPD 46.12.xx)
- POLYCENTER Security Compliance Manager for SunOS (SPD 41.25.xx)
- POLYCENTER Security Compliance Manager for Solaris 2 (SPD 55.87.xx)
- POLYCENTER Security Compliance Manager for DEC OSF/1 AXP (SPD 55.86.xx)
- POLYCENTER Security Reporting Facility for OpenVMS (SPD 26.N2.xx)
- POLYCENTER Security Intrusion Detector for OpenVMS (SPD 41.27.xx)
- POLYCENTER Security Intrusion Detector for ULTRIX (SPD 43.07.xx)
- POLYCENTER Security Intrusion Detector for DEC OSF/1 (SPD 43.08.xx)
- POLYCENTER Security Intrusion Detector for SunOS (SPD 43.09.xx)

#### **HARDWARE REQUIREMENTS**

The systems, components and peripherals specified are supported.

#### *Minimum Supported Configuration*

- An Intel™ 80386-, 80486- or Pentium based personal computer, IBM® or compatible.
- 1.5 MB of free hard disk space.
- In a PC local area network, at least one DOS workstation must have one diskette drive capable of reading 3.5 inch diskettes to load the distribution media.

#### **Disk Space Requirements**

The following are the disk space requirements:

*Disk Space Required for Installation* 1.5M Bytes

*Disk Space Required for Use (Permanent)* 1.5M Bytes

**SOFTWARE REQUIREMENTS**

POLYCENTER Security Compliance Manager for NetWare requires software on both the PC client and the NetWare server.

*For the PC client:*

MS-DOS® V5.0 or higher.

*For NetWare server:*

NetWare Operating System Version 3.11 or 3.12.  
NetWare C NLM Runtime Library V3.12h or higher

**GROWTH CONSIDERATIONS**

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

**DISTRIBUTION MEDIA**

POLYCENTER Security Compliance Manager for NetWare is supplied on a high density 3.5 inch diskette.

**ORDERING INFORMATION**

The software license, media, and documentation are combined in a single shrinkwrap package. The software license is available separately.

License only: QM-34BAA-AA

Package: QM-34BAA-SA

\* For additional information on available licenses, services, and media, see 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.

**SOFTWARE LICENSING**

This software is furnished under the licensing provisions contained in the licensing agreement QM-34BAA-AA. For more information about Digital's licensing terms and policies, contact your local Digital office.

Possession, use, or copying of the software described in this publication is authorised only pursuant to a valid written licence from Digital or an authorised sublicensee.

**SOFTWARE PRODUCT SERVICES**

A variety of service options are available from Digital. In addition to standard SPS remedial services, consulting services to help plan, design, and implement a custom security analysis and reporting system with the POLYCENTER Security CM and POLYCENTER SRF tools are also available. For more information, contact your local Digital office.

**SOFTWARE WARRANTY**

Warranty for this software product is provided by Digital with the purchase of a license for the product as defined in the licensing agreement QM-34BAA-AA.

- ® AIX and IBM are registered trademarks of International Business Machines Corporation.
- ® HP is a registered trademark of Hewlett-Packard Company.
- ® MS-DOS is a registered trademark of Microsoft Corporation.
- ® NFS, Solaris and SunOS are registered trademarks of Sun Microsystems, Inc.
- ® NetWare is a registered trademark of Novell, Inc.
- ® OSF and OSF/1 are registered trademarks of the Open Software Foundation Inc.
- ™ RISC System/6000 is a trademark of International Business Machines Corporation.
- ™ The DIGITAL logo, AXP, DEC, Digital, OpenVMS, POLYCENTER, ULTRIX, and VMS are trademarks of Digital Equipment Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

©1993, 1994 Digital Equipment Corporation. All rights reserved.

