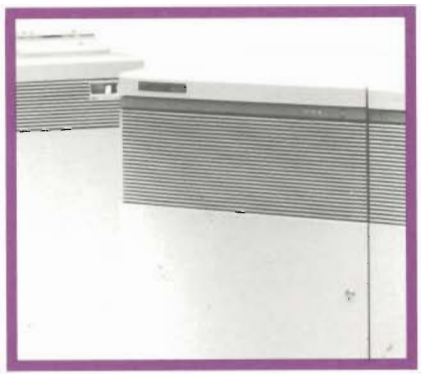
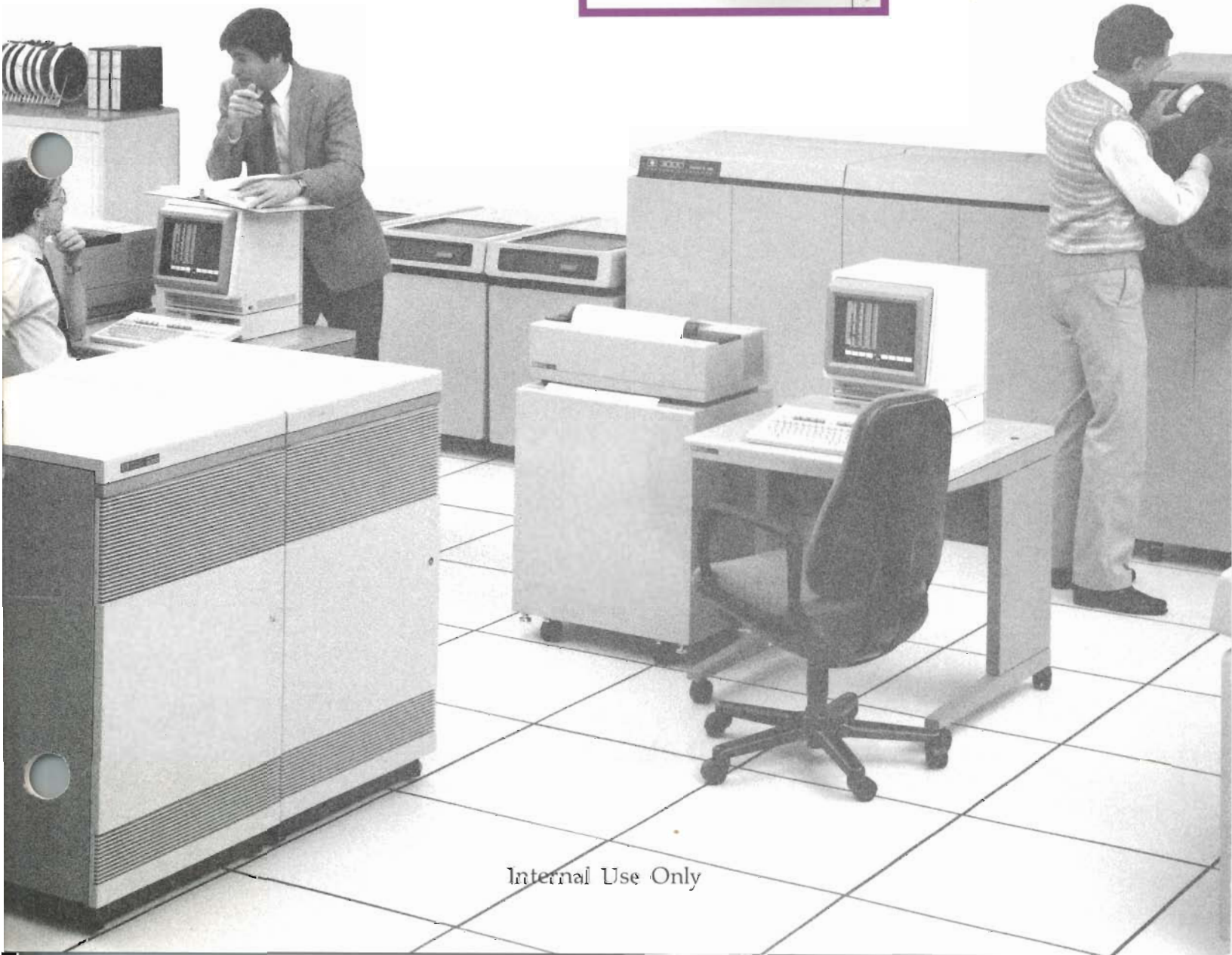
HEWLETT-PACKARD

HP Security Monitor

HP 3000

Sales Guide





Internal Use Only

HP Computer Museum
www.hpmuseum.net

For research and education purposes only.

HP Security Monitor/V

Introduction

Increased security for security conscious customers

HP Security Monitor/V is the new HP 3000 security product available on V-MIT, the latest version of the MPE V/E operating system. This Sales Guide explores the features and benefits of HP Security Monitor which substantially increases system security for your security conscious customers.

Improved Password Protection

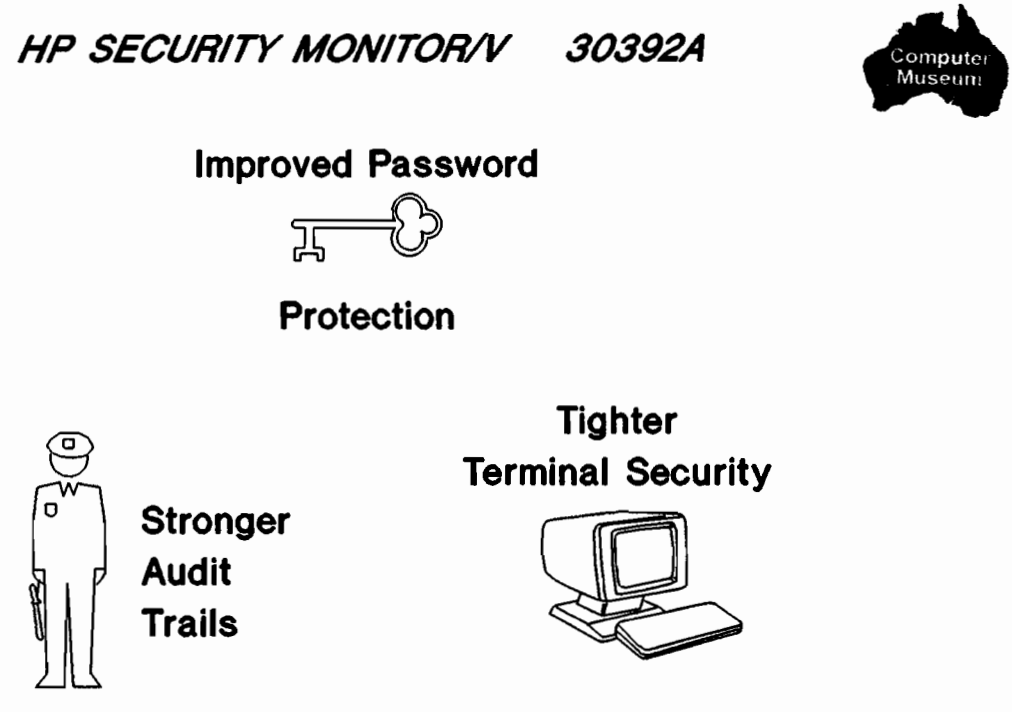
Passwords provide the first line of defense against unauthorized access to system resources and data. HP Security Monitor has improved password protection through a combination of methods including password encryption, password aging, and password length requirements. The Security Administrator can also require user passwords at either the account or system level. Finally, during interactive log-ons, the HP Security Monitor can reject embedded passwords, forcing the user to wait for the non-echoed password prompt.

Stronger Audit Trails

Audit trails allow security conscious customers to monitor and correct security breaches in the system. HP Security Monitor has improved audit trails by giving the Security Administrator the ability to log a wide variety of security relevant events. HP Security Monitor also allows the Security Administrator to selectively disable particular MPE commands.

Tighter Terminal Security

Terminal security allows customers to secure their systems against unauthorized bypassing of the log-on precautions. HP Security Monitor has substantially tightened terminal security: by limiting the number of invalid log-on attempts, by terminating idle sessions, and by passwording individual terminals. HP Security Monitor can also eliminate the log-on guidance that the system normally provides after an invalid log-on attempt.



Smooth Implementation

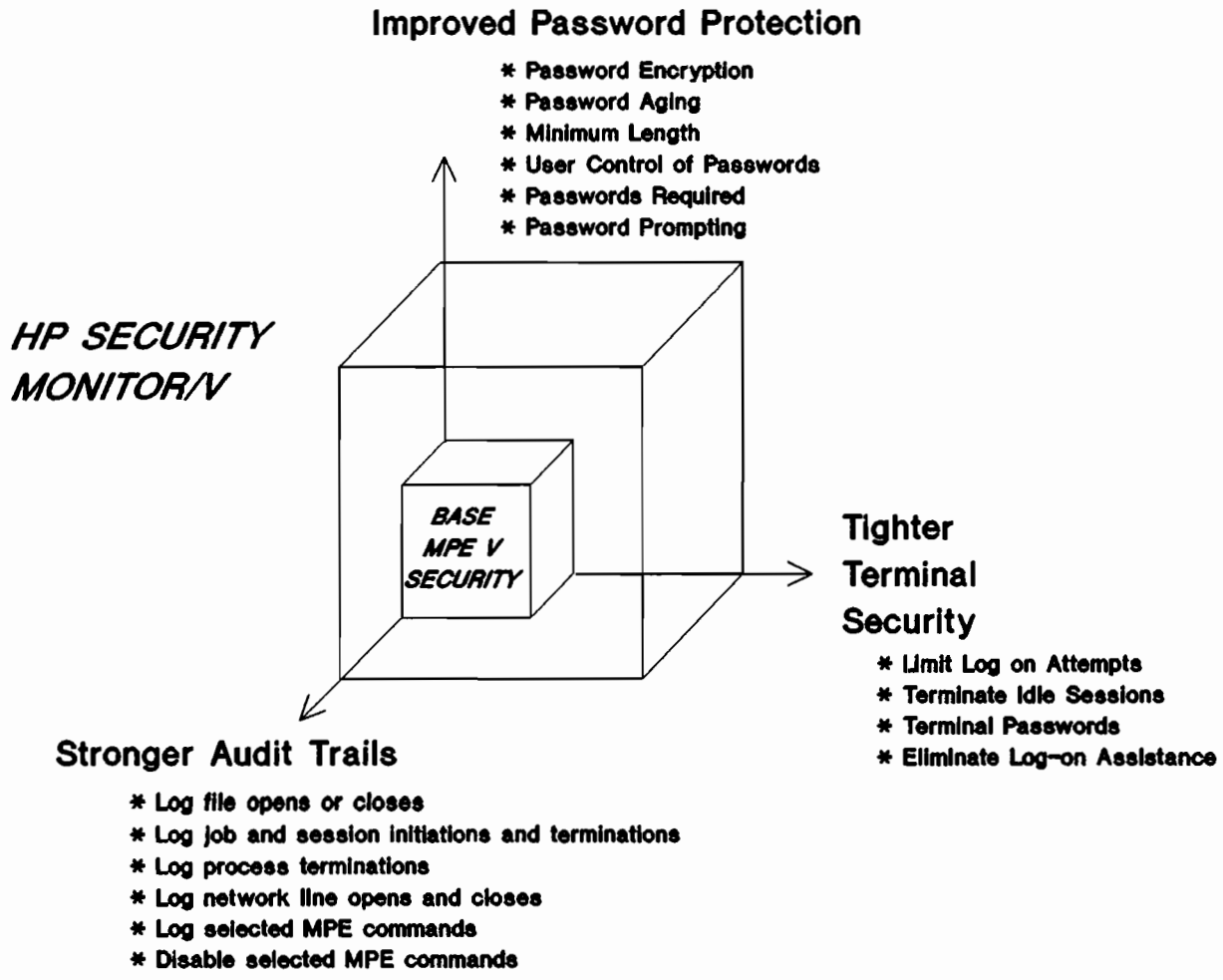
Optional features can be tailored to fit specific security needs

Builds on base HP 3000 Security

HP Security Monitor's security features are designed to complement the already strong security features of the base HP 3000. The base HP 3000 systems offer users, application managers, and system managers a flexible yet secure data processing environment. By combining the hardware architecture and the MPE operating system, the base HP 3000 system provides a set of features which allows preventive safeguards of system resources and user data. This environment also provides detection and audit mechanisms, which can be used to strengthen the "accountability factor" in security.

Smooth Implementation

Building on the security features of the base HP 3000, HP Security Monitor can be gracefully integrated on an as needed basis. All of its security features are optional, and each feature can be enabled individually. HP Security Monitor is also designed to "phase in" features, thereby easing the transition from the old to the new security practices on the system. This design gives customers wide latitude to tailor the security enhancements to fit their particular needs, while at the same time providing a smooth implementation.



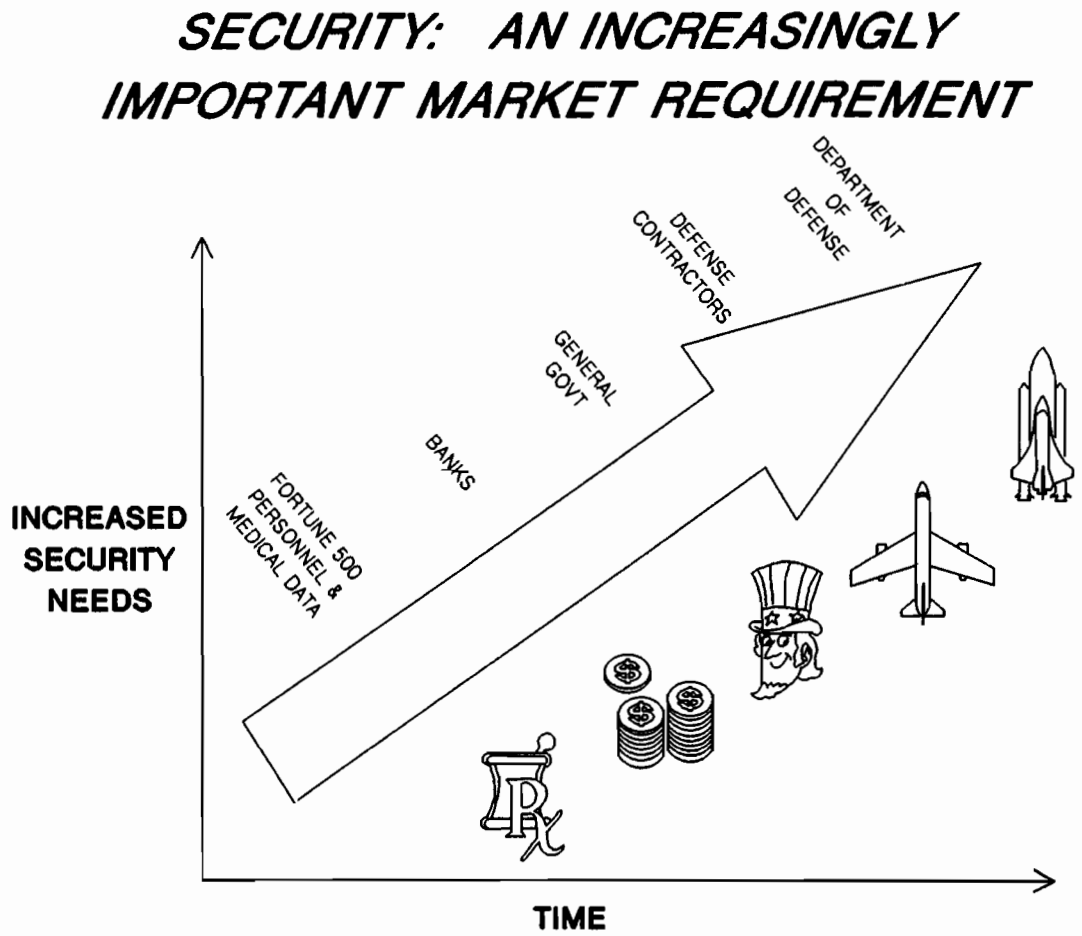
Security Trends

An increasingly important market requirement

As the HP 3000 family has grown in power, customers have been placing increasingly security sensitive applications on our high end systems. We have outgrown our traditionally "open" minicomputer roots, and have penetrated a number of different markets where system security is an increasingly important requirement.

Currently, our installed base includes a large proportion of defense contractors and government agencies. For these markets, the Department of Defense has established a set of computer standards called the Trusted Computer Base. An Executive Order has been issued which directs that these standards apply to all branches of the government and to all defense contractors and subcontractors. This Order envisions that 50% of the government installed base will be functioning at the C2 level of security by the end of 1987. While this goal is very aggressive and will probably not be met, the direction is clear.

Besides the government installed base, there are also other important market segments served by the HP 3000 which have security requirements. Among these, the financial sector has recently seen banking regulations which have significantly tightened the encryption and authentication requirements for electronic funds transfers. Also, various federal privacy laws have been passed which make organizations liable for the misuse of confidential data contained in their systems. This legal liability increases the need for system security for any Fortune 100 corporation which maintains personnel or medical data.



Sales Strategy

Don't Use Security to Sell Against DEC and IBM

Competition

In order to understand where the HP 3000 stands on security, it is important to understand what our primary commercial competitors, IBM and DEC, have done.

While both DEC VMS and IBM MVS (with ACF2) have been certified by the Department of Defense at the C2 level of security, HP Security Monitor will need to add two features to reach the C2 level. We plan to add these C2 features as well as other features appropriate for our target markets over the next 12 months. With the addition of these features, HP's security offering will be certified at C2.

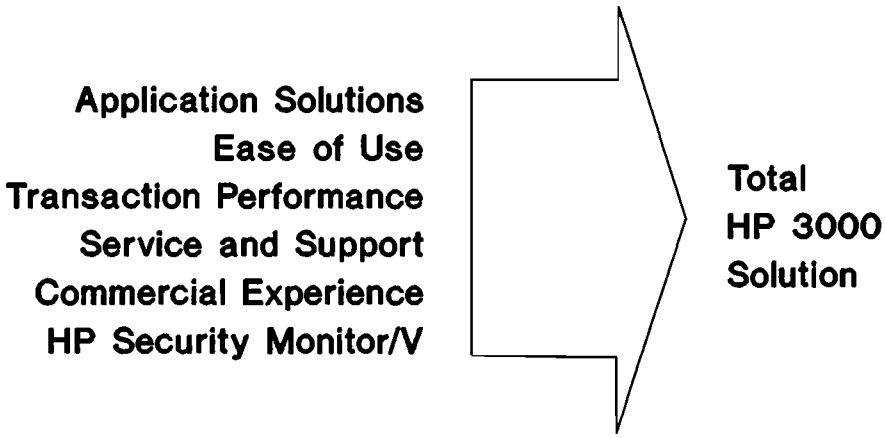
Even with these additional features, HP Security Monitor will not match the security offerings of DEC VMS and IBM MVS. Both systems offer a number of very sophisticated features which are targeted for markets which we are not pursuing with the HP 3000. These features are only required in extremely security sensitive environments such as the "mission critical" systems for defense contractors. Such environments are often prone to attacks by hackers, and they need extreme security, often sacrificing "ease of use" and performance in the process.

Sales Strategy

This means that HP's strategy on security is to meet customer needs in our existing target markets. Security is not an end in and of itself, but it is part of the overall system solution. For our target markets, security concerns must be weighed against ease of use and performance concerns.

HP should not go after new customers where security is the overriding issue. We should use HP Security Monitor in sales situations where moderate security concerns are inhibiting the sale of the total HP 3000 solution.

PUT SECURITY IN CONTEXT
WITH THE TOTAL HP 3000 SOLUTION



Pricing and Availability

Ordering Information

The right to use HP Security Monitor/V on an HP 3000 computer is available according to the terms and conditions of the standard Hewlett Packard Software Purchase Agreement. The list price is subject to the standard volume discounts and it is identical for all HP 3000 processors. HP Security Monitor/V can be ordered from the July CPL.

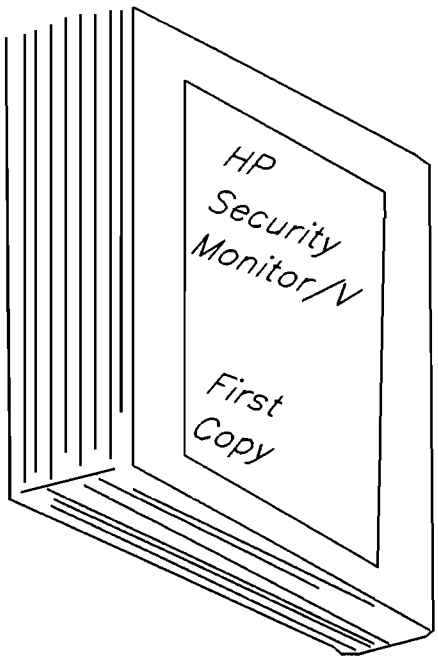
Product Number	Product Description	U.S. List Price
30392A	HP Security Monitor/V Provides Operating System Security	$ 3500
30392R	HP Security Monitor/V Right to Copy	$ 2450

Documentation

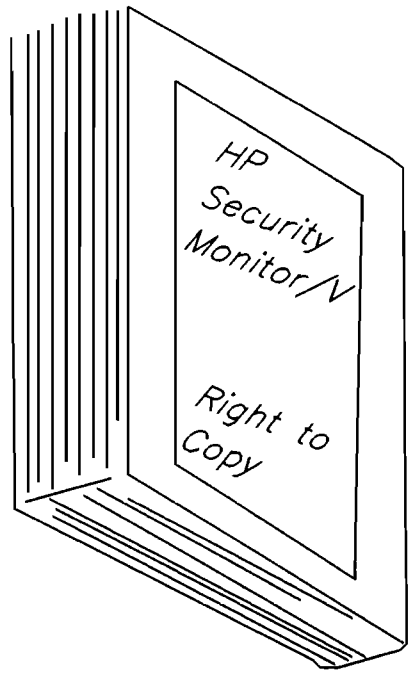
Part Number	Document Name
32033-90136	MPE V Account Structure and Security

Availability and System Environment

HP Security Monitor/V is supported on V-MIT and subsequent releases of MPE V/E. V-MIT will be available in early July.



30392A $ 3500



30392R $ 2450

Compatibility

Customers must carefully weigh the implications of a secure environment

By design, some of the higher security features of HP Security Monitor prevent execution of some of the ease of use features in HP, customer, and third party software.

For example, in a secure environment, customers may wish to require terminal passwords, thereby adding another layer of security on the system. In a less secure environment, however, customers may wish to use the automatic system log-on features available on some personal computer communication software packages. This automatic log-on feature bypasses the very authentication and verification steps which are necessary for a secure environment.

With these trade-offs between security and ease of use in mind, customers must carefully weigh the implications of adding various security features. While complementing the strong system security of the base HP 3000, the security features of HP Security Monitor can be gracefully integrated on an as needed basis. All of these features are optional, and each feature can be enabled individually.

HP Security Monitor is also designed to "phase in" features, thereby easing the transition from the old to the new security practices on the system. For instance, since any application software can be potentially affected by MPE command disabling, HP Security Monitor provides the ability to monitor the execution of MPE commands prior to disabling them. This identifies any application software which depends on the command to be disabled.

This flexible design gives customers wide latitude to tailor security enhancements to fit their particular needs, while at the same time providing a smooth implementation.

HP APPLICATION SOFTWARE: SUPPORTED WITH HP SECURITY MONITOR/V

SUPPORTED		*PARTIALLY SUPPORTED*
HPWORD	*EDIT/V*	*HPDeskManager*
HPSLATE	*FCOPY/V*	*MM/3000*
TDP/3000	*SORT-MERGE/V*	*PM/3000*
HPSpell	*NLS*	*HPFA*
HPDraw	*COBOL II/V*	
HPEasyChart	*Pascal/V*	
HPMAP	*RPG/V*	
IDS/3000 & IFS/3000	*HP Pascal/V*	
VisiCalc/3000	*BASIC/V*	
IMAGE/V	*HP Business Basic/V*	
TurboIMAGE/V	*SPL/V*	
HPSQL/V	*Transact/V*	*NOT SUPPORTED*
DBChange/V	*FORTRAN 66/V*	
KSAM/V	*HP FORTRAN 77/V*	*PPC Products*
QUERY/V	*VPLUS/V*	*HPEasyTime*
Inform/V	*Toolset/V*	*BRW/V*
Report/V	*Dictionary/V*	
TurboIMAGEProfiler/V	*Network Software*	
SILHOUETTE/V	*APS/3000*	
COPYCAT/V	*OPT/3000*	

Questions and Answers

Answers to the tough questions

Q: What are HP's future plans for security certification?

A: HP is very interested in security certification. We are working with the Department of Defense to certify MPE V/E at the C2 level within the next 18 months. We also plan to certify MPE XL at the C2 level. While certification beyond the C2 level doesn't seem necessary for our target markets, we will add specific additional features to meet our customers' needs.

Q: Will HP Security Monitor/V be available on MPE XL?

A: HP plans to migrate all HP Security Monitor/V functionality to MPE XL. In addition, we intend to make all of the user interfaces for the security product on MPE XL identical to the user interfaces on HP Security Monitor/V.

Q: Why are we charging for system security?

A: HP is charging for HP Security Monitor because system security is functionality which is not appropriate for all system environments. Remember, not all HP applications will support a highly secure environment.

System security has value to a select group of customers that are willing to pay for it. As a result, most of our competitors and third parties charge substantially for similar products.

Q: Will the security features affect customer application software?

A: All of the security features are optionally enabled on HP Security Monitor. When they are off, there are no security implications to applications because there is no additional security. However, depending on the specific security features enabled, there are some situations where customers might want to modify their programs, jobstreams, and UDCs to take full advantage of HP Security Monitor.

For example, if the Password Minimum Length requirement is set to 8 characters, any software which creates new users and their corresponding passwords will need to meet this requirement. Any software which currently creates 5 character passwords should be modified accordingly.

Q: Is HP Security Monitor supported with all HP application software?

A: Most HP application software is supported with HP Security Monitor. However, there are a few applications which are not currently supported with all of HP Security Monitor's features (see Compatibility). We are investigating these issues with all of the affected HP application divisions to evolve a strategy for the long run.

HPDeskManager is not supported only when the Password Prompting feature is fully enabled to apply to remote interactive log-ons, not just to standard interactive log-ons. HP Security Monitor specifically warns the customer about the implications of fully enabling this feature. This means that most customers can use HPDeskManager in a highly secure environment.

MM/3000 and the other MPD products are not supported only when the File Open and MPE Command Logging features are enabled because they increase stack space usage. In certain rare cases, this can result in a stack overflow condition. Again, this means that most customers can use MPD applications in a highly secure environment.

The PPC products are not supported when Password Encryption, Password Prompting, Terminal Passwords, and Idle Session, Termination features are enabled because they interfere with the PPC ease of use features.