

SNAP: Secure Network Access Partnering

(and Partnering for Secure Network Access)



Dynamic
Coalition Formation
at its best (sigmund@best)

- . Inherent Security
- . HA
- . High-Performance

- . Server/Storage Virtualization
- . Scalability
- . UNIX/Linux, Windows & Mac OS X Interoperability

Business Challenges for the Defense, Government, Intelligence, Public Safety Communities and High-Sensitive Industrial Areas

- Access to multiple overlapping Security Domains
- Secure data transfer between Domains
- Ability to meet the highest Common Criteria Evaluation Access Level (EAL)
- Scalability and HA
- Maximize operation efficiency
- MINIMIZE COST



Solutions of Access to Multiple Security Domains

Stove-piped ("Air Gap") Solution

- + physically isolated clients (networks)
- often resulting in up to 10 different PCs in a single office



Overlapping Domains Solution

- + allows collaboration on defined data by role-based individuals using defined processes on overlapping domains
- requires the highest Common Criteria Eval. Acc. Level (EAL) certification of the OS in order to become 'Air-Gap'-Secure





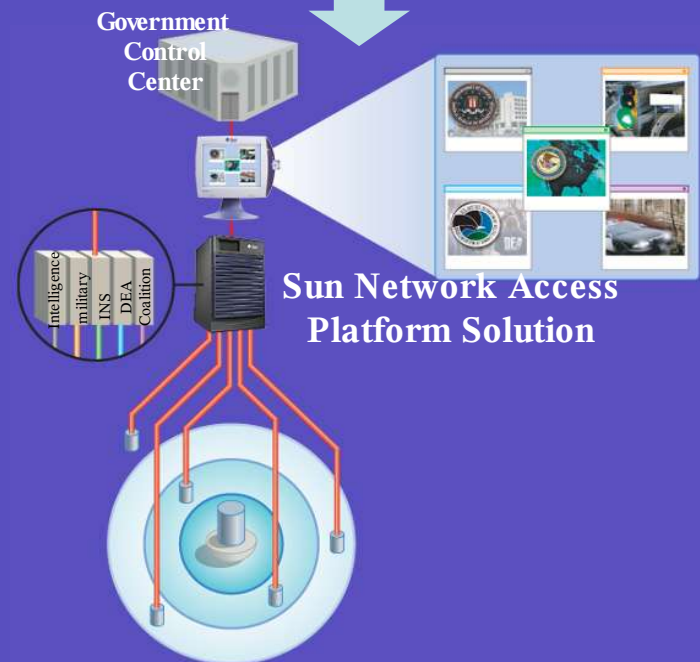
Overlapping Security Domains Solutions Proven in Real- World Applications

Joint Intelligence Center Pacific (JICPAC)

- Intelligence Center for the Pacific Command
- Collaboration between multiple disparate intelligence and military agencies requires simultaneous access to applications residing in multiple secure domains
- 24/7h operation of 1000 seats
- Maximize operation efficiency
- Projected 90% cost reduction over 5 years
- Meets highest levels of DOD Trusted Computing Deployment Criteria

Space and Naval Warfare Systems Command (SPAWAR)

- Secure collaboration among up to 60 countries involved in the coalition effort in Persian Gulf
- Multiple levels of security and access spec's



Ready for Collaboration-Deployment by Industry/Commerce, EDU&Research, Regional&Local Public Authorities?



Enterprise
Headquarters,
Central EDU
& Research
Institution

Regional Indus-
try or Commerce
Subsidiary, EDU
& Research Site,
Public Authority

Branch Office,
Local EDU&
Research Site,
Local Public
Authority

Home Office,
Collaborating Partner,
Outsourced Capacity,
Mobile Use,
Public Access Kiosk

OS Security Functions

	IBM	Sun	Sun	HP	Microsoft	Red Hat
Function	AIX 5L v5.3	Solaris 10	Trusted Solaris 10	HP-UX 11i	Windows Server 2003	Advanced Server 4.0 (SE Linux)
Independent Certification - Common Criteria						
EAL 4, CAPP, RBACPP, LSPP (B1)			√			
Provides the highest level of assurance of any OS						
EAL 4, CAPP (C2)	√	√	√	√	W2k oly	
Provides the second highest level of assurance of OS						
More Granular User Control						
Role-Based Access Control (RBAC) (Admins. enforced)						
Ability to allocate access rights based on role. <u>BENEFIT</u> : Increases the accountability and granularity of user control over other standard OS levels.	Partial (No Admins.)	√	√	Partial (No Admins.)	Partial (No Admins.)	Partial
User Rights Management						
Centralized database which specifies what users rights are granted to users. <u>BENEFIT</u> : Limits user's access to applications and functions within applications.		√	√		√	
Process Rights Management						
Fine-grained privileges are used instead of a single superuser. <u>BENEFIT</u> : Limits the power of applications so that they are not subject to abuse.		√	√			
Prevent "Eavesdropping" in Windows Environment						
Trusted X11 Windows Environment						
Enforces mandatory and discretionary access control within the window system. <u>BENEFIT</u> : All windows are labeled according to their sensitivity.			√		N.A.	

OS Security Functions (Cont'd.)

	IBM	Sun	Sun	HP	Microsoft	Red Hat
Function	AIX 5L v5.3	Solaris 10	Trusted Solaris 10	HP-UX 11i	Windows Server 2003	Advanced Server 4.0 (SE Linux)
Trusted Path						
Allows for uninterrupted communication between the Trusted X11 windows server and the window manager. BENEFIT: Helps assure that users are not tricked by hostile programs into supplying information that might be used to penetrate the system.			√			
Selection Confirmation						
Forces users to confirm the transfer of information (text, graphics, etc.) between windows. BENEFIT: Prevents information flow between windows system objects.			√			
Increased Privacy						
Mandatory Access Control (MAC)						
A system-enforced policy in which all data objects are labeled according to their sensitivity and users may be cleared for one or more labels. BENEFIT: Prevents information flow between users and processes unless they have compatible labels.			√			Partial
Labeled Printing						
Associates sensitivity label ranges with individual printers. Records label of data on each page and on banner and trailer pages. BENEFIT: Restricts the security levels of information sent to individual printers. Guarantees that output is properly labeled.			√			

OS Security Functions (Cont'd.)

	IBM	Sun	Sun	HP	Microsoft	Red Hat
Function	AIX 5L v5.3	Solaris 10	Trusted Solaris 10	HP-UX 11i	Windows Server 2003	Advanced Server 4.0 (SE Linux)
Trusted Networking						
All information flows on a system are labeled and access control is enforced. <u>BENEFIT</u> : Prevents information flow between clients and servers unless they have the same label.			√			
Multi-level File System						
All files and directories are protected according to their label <u>BENEFIT</u> : Prevents information from being downgraded via the file system.			√			
Reduced Risk of Security Violations						
Security Labels						
Allows information to be classified at appropriate security sensitivity levels. <u>BENEFIT</u> : Only owners with the corresponding security clearance can access the information residing on the device.			√			
Clearances						
The degree of security with which a user is entrusted. <u>BENEFIT</u> : Restricts access based on need to know.			√			
Audit all or Selected User Actions						
Records all security-relevant events in a tamper-proof audit trail. <u>BENEFIT</u> : Allows securing of data deemed highly secure.	√	√	√	√	√	Partial

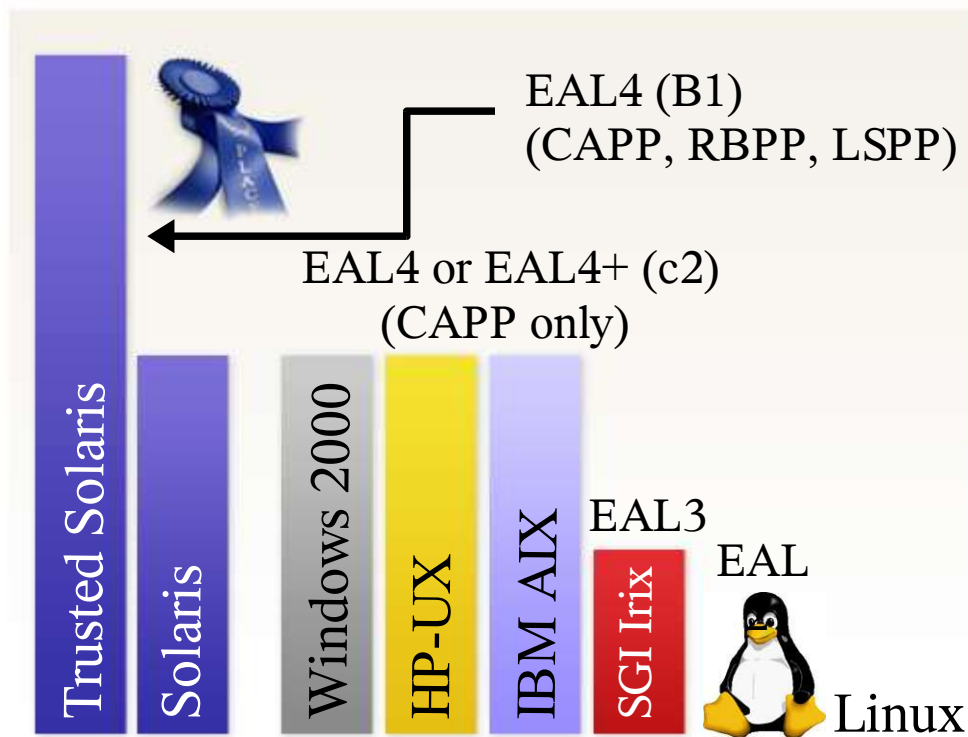
OS Security Functions (Cont'd.)

	IBM	Sun	Sun	HP	Microsoft	Red Hat
Function	AIX 5L v5.3	Solaris 10	Trusted Solaris 10	HP-UX 11i	Windows Server 2003	Advanced Server 4.0 (SE Linux)
Prevent Spoofing Programs						
Trusted Path Attribute						
A process attribute which indicates the ancestry of trusted programs. BENEFIT: Process with questionable ancestry can't acquire privilege via RBAC.			√			
Limit Privileges						
Defines an upper bound for a zone, or for an account. BENEFIT: Applications can't become more powerful than they already are.			√			
Protect Local Devices from Unauthorized Users						
Device Allocation based on Label						
Assigns a device or group of devices to a particular user or group of users based on security labels and MAC privileges. BENEFIT: Prevents unauthorized removal of data from the system.			√			
Pluggable Authentication Module						
An extensible authentication framework with standard APIs. BENEFIT: Provides failed-login account locking, trusted path checking, and machine generated passwords, without the need to change code.	√	√	√	√	No - proprietary	√
Name Service Support						
All systems share a common repository of security attributes and policies. BENEFIT: Provides a single system image with consistent identity and policy.	√	√	√	√	√	√

OS Security Functions (Cont'd.)

	IBM	Sun	Sun	HP	Microsoft	Red Hat
Function	AIX 5L v5.3	Solaris 10	Trusted Solaris 10	HP-UX 11i	Windows Server 2003	Advanced Server 4.0 (SE Linux)
Trusted Mail						
E-mail can be received by an account only if the message is within the account's clearance. BENEFIT: Prevents information flow between users unless they have the same label.			√			
Investment Protection						
Runs most Off-the-Shelf Solaris Apps.						
BENEFIT: Protects customer's existing application development.	N.A.	√	√	N.A.	N.A.	N.A.
Runs Alongside Standard Solaris						
BENEFIT: Allows customers to add Trusted Solaris security to systems as needed while continuing to use their existing systems.	N.A.	N.A.	√	N.A.	N.A.	N.A.

Summary: The Most Secure Certified Operating Environment in the Industry Is By Far the Trusted Solaris



Only OS Certified with EAL4 and 3 Protection Profiles in EAL4:

CAPP: Controlled Access Protection Profile (Ensures proper login)

RBPP: Role-based Protection Profile (Role-based access control allows the system administrator to define roles based on job functions within an organization. The administrator assigns privileges to those roles)

LSPP: Labeled Security Protection Profile (All data and application components are formally labeled addressed, and tracked through role based access control.

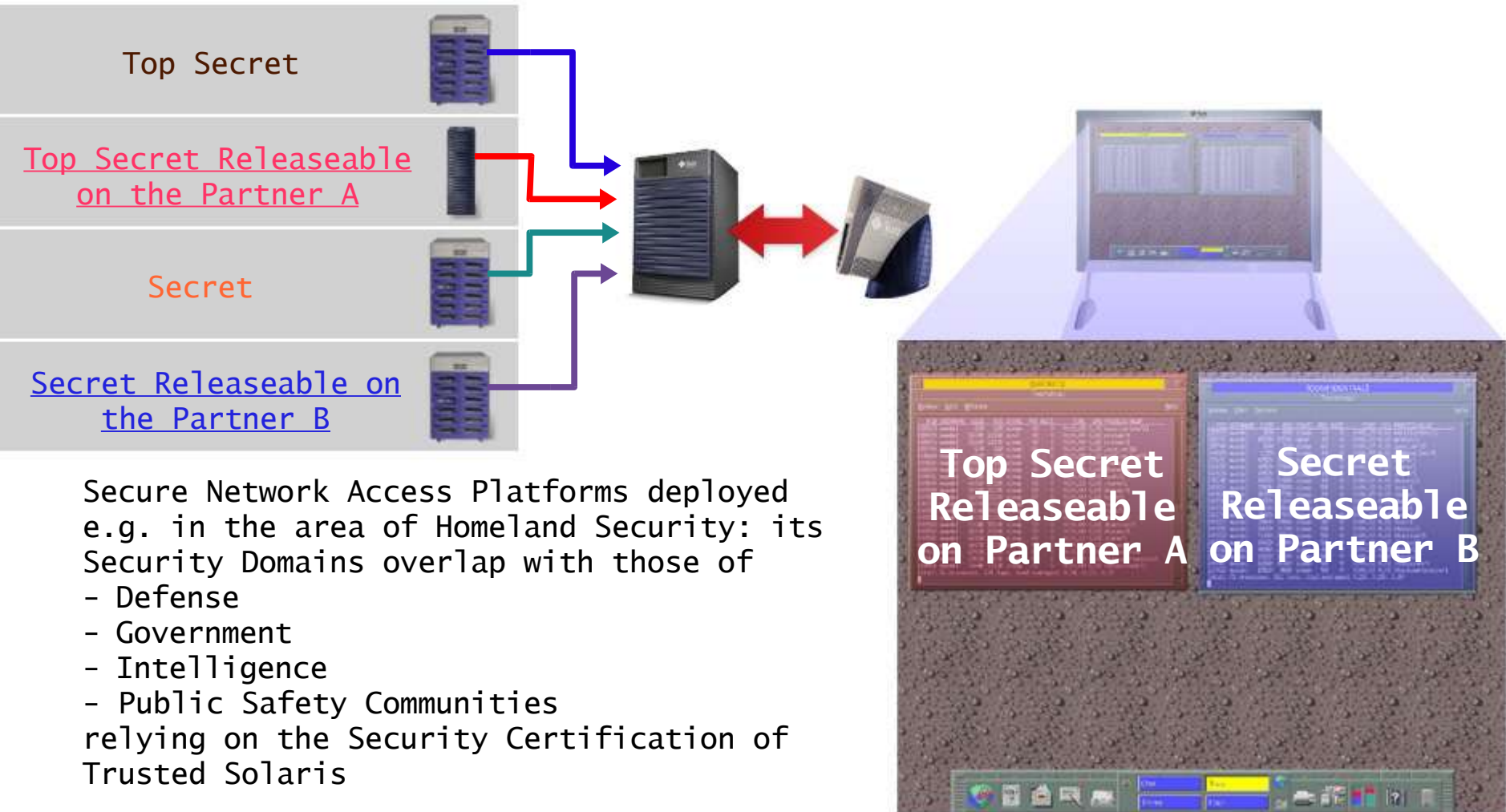
Based on data from

<http://www.commoncriteria.org/ccc/epl/productType/eplinfo.jsp?id=4>

Sun Microsystems Inc., All rights reserved

Implications:

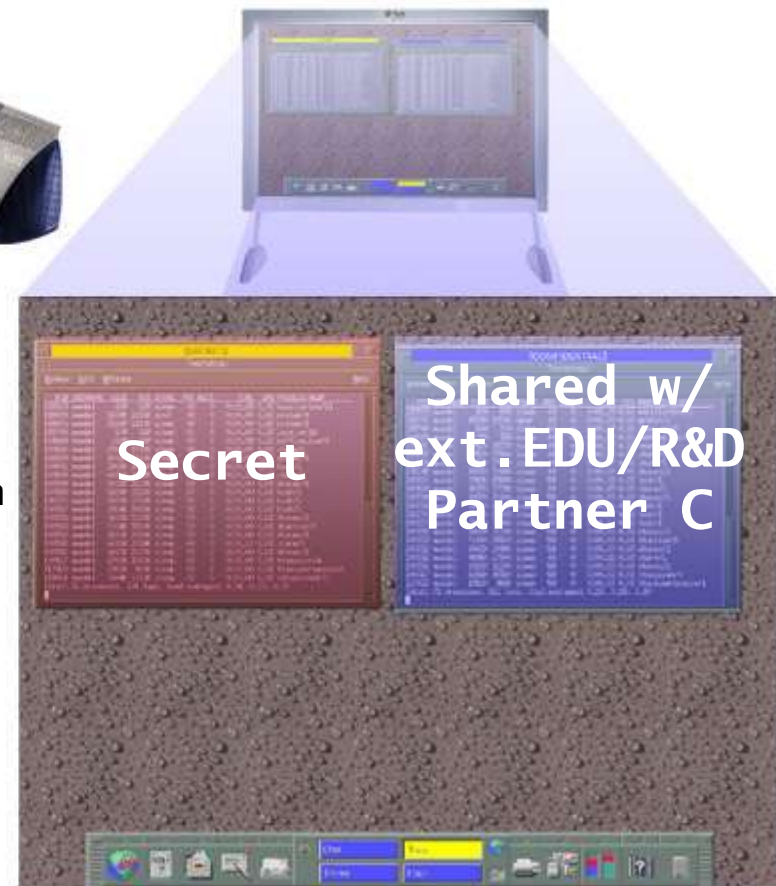
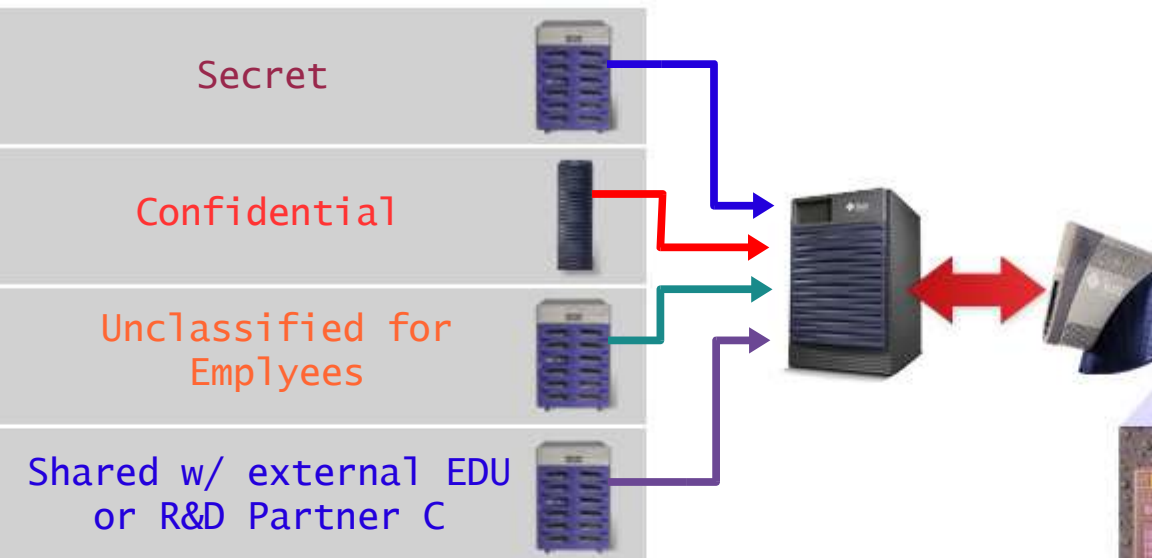
Widespread deployment of the Sun Secure Network Access Platform (SNAP) for collaboration in high-security areas with overlapping Security Domains



Ready for Industry/Commerce/Local Public Communities?

Don't reinvent the wheel: you can start to evaluate&implement Secure Network for Collaboration today - if you involve a local EDU and/or Public R&D partner

(Call sigmund@best - 089/9506080)

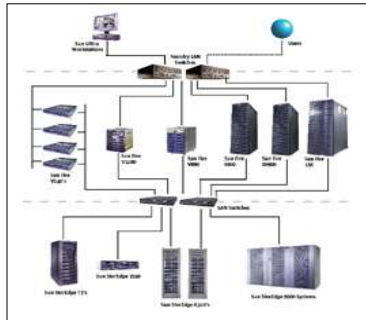


Secure Network Access Platforms for collaboration with your local EDU and/or Public R&D partners - they get Trusted Solaris for free if deployed in Research&Development Projects in conjunction with

- Industry
- Commerce
- Local, Regional or Government Public Authorities
- other EDU & Research Institutions

Don't Reinvent the Wheel

Use the proven Reference Architectures while collaborating w/
a local EDU or R&D institution of your choice



- Real-world proven Reference Architectures
- collaborative design within 2 hours on your site - flexible to meet your needs
- Customer-Ready-Solution coming pre-integrated&tested with detailed Techn.Guides
- best Systeme GmbH is a
 - . Sun Data Center System Provider
 - . Sun Service Manager
 - . Sun Accredited Installation Provider (AIP)
 - . Sun Cluster Specialty Partner
 - . Sun Campus Reseller for EDU & Research
 - . Preferred Oracle Real Application Cluster (RAC) Partner of Oracle Corp.
 - . Preferred Partner of Veritas, Legato, StorageTek, IBM, HDS, ADIC, Cisco

Anlässlich der Fachtagung **best Open Systems Spring'05** laden wir Sie zu unsem **Frühjahrs-Sonderprogramm** in Zusammenarbeit mit der bayerischen **Lehre & Forschung** ein, um die Praxisanbindung von F&L an die Industrie/Kommerz/Behörden in Bayern zu fördern *):

SNAP - Secure Network Access Partnering Action -
Pre-integrated&tested Secure Network Access Plattformen **)

SNAP-5 5 Arbeitsplätze

€ 8.500,00 (+MwSt.)

heterogene Secure Network Konfiguration

- 1 64-Bit AMD Opteron150 Workstation 2.4GHz/1GB/Grafik
- 1 64-Bit Unix RISC Workstation 1.5GHz/3GB/Grafik
- 2 SunRay Secure Clients
 - 1 SunRay Remote Secure Client (wie Notebook, inkl. TFT-LCD)
 - incl. aller SW-Liz. (m. Ausnahme der MS Win. Liz. f. d. Teilpos.1, Opter.WS) f. d. Dauer einer bis zu 2-Jahres-Aufbauphase von SNAP bei Ihnen
 - ext. Monitore nicht beinhaltet (beliebige PC-Monitore verwendbar)

SNAP-8 8 Arbeitsplätze

€ 11.500,00 (+MwSt.)

wie oben, jedoch

- 3 SunRay Secure Clients
- 3 SunRay Remote Secure Clients (inkl. TFT)

*) Zeitlich begrenzte Sonderaktion bis zum 13.5.2005
Irrtum und Änderungen der Hersteller vorbehalten

**) Call 089/9506080 oder sigmund@best.de

