Using PitBull® Trusted Computing Platform to Solve Real-world Problems

GENERAL DYNAMICS
Mission Systems

Presentation Outline

1. Introduction to PitBull
2. PitBull Mechanisms
3. Multilevel desktops
4. PitBull Use cases
5. More about PitBull
6. Q&A

Introduction to PitBull

What is PitBull?

- PitBull is a General Dynamics Linux distribution based on RHEL 7
  - PitBull is NOT something installable on top of an running Linux system
- PitBull is used in server, workstation, and infrastructure configurations
- PitBull has nothing to do with virtual machines or containers
  - however VMs and containers can be run on PitBull
- PitBull has been in use for over 25 years
  - PitBull has been used by many commercial and defense customers

What can PitBull do?

- Provides extreme security
  - risk reduction, damage containment, attack vector blocking, user/admin controls
- Enables complex architectures
  - including polyinstantiated, cross domain (CDS), and multilevel security (MLS)
- Facilitates system evaluation and accreditation
  - designed for Protection Level 3 and Protection Level 4 (PL3 & PL4)
  - enforces security on all users and applications
  - included in multiple US accreditations with multiple accrediting agencies

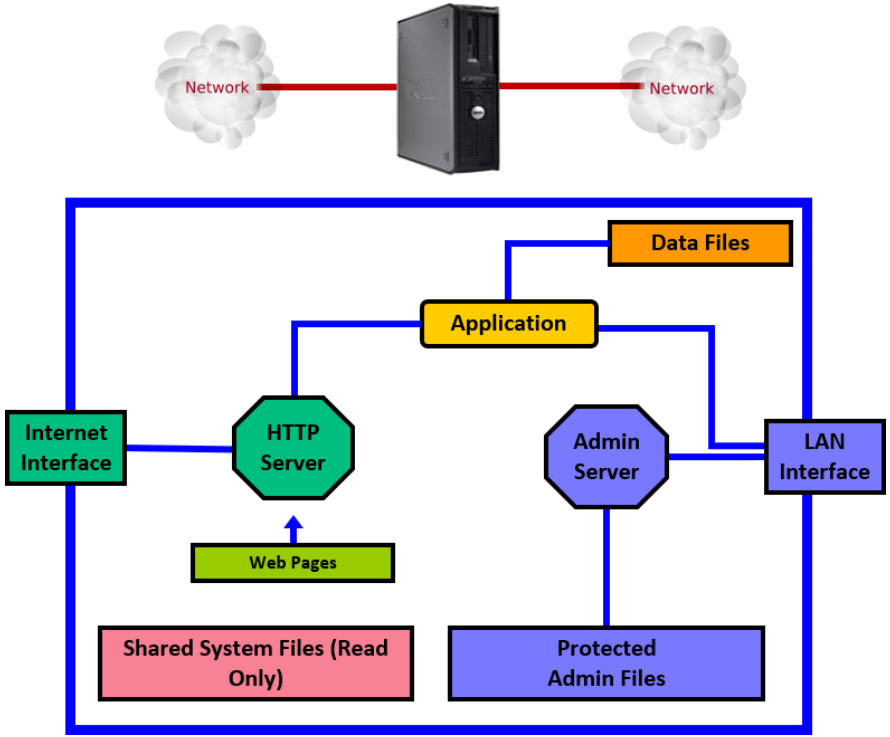
What PitBull isn’t

- PitBull isn't **encryption**
- PitBull isn't a **firewall**
  - but it does include advanced networking filtering
- PitBull isn't **intrusion detection**
  - but it does include tools to detect changes to files
- PitBull isn't **virus scanning**
- PitBull isn't **system hardening**
  - but it does significantly harden a system

How does PitBull do it?

- PitBull uses kernel enhancements to implement mechanisms
  - mechanisms cannot be bypassed or shut down
- PitBull does not use SELinux, VMs, or containers
- PitBull uses attribute-based controls
  - there are no rule databases to analyze or maintain

Compartmented Protection



PITBULL

What Security PitBull Provides

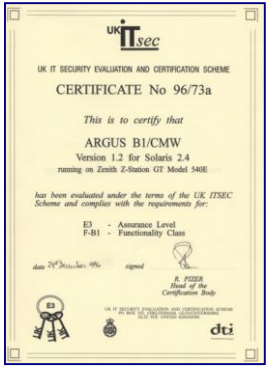
- Prevents any bug in any program from damaging the underlying system
- Controls what network resources can be used by each program
- Limits all user and administrator accounts
- Enforces a security policy on a system of malicious software

PitBull History

- Technology development
  - Original technologies developed in 1990 (DIA/CMW)
  - Ported to 30+ operating systems from 1992 to 2012
  - On Solaris 2.4 (1994) through Solaris 10
  - First commercial installation: Credit Suisse (1997)
  - Over 50 commercial installations by 2005 in Europe, North America, Asia
  - AIX PitBull technology sold to IBM in 2005
- Ported to Red Hat Enterprise Linux (RHEL) in 2012

Evaluations and Accreditations

- Evaluated under ITSEC to F-B1/E3
  - 1996 and 1999; two certificates each
  - included networking and MLS GUI
  - evaluated on Solaris
- Evaluated under Common Criteria
  - 2006 and 2007 LSPP/EAL4+
  - evaluated on AIX
- Included in accreditations to PL4
  - Base for NSA/DIA TNE accreditation
  - Four configurations of MLS desktop



UK ITSEC

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFICATE No 96/73a

This is to certify that

ARGUS B1/CMW
Version 1.2 for Solaris 2.4
running on Zenith Z-Station GT Model 540E

has been evaluated under the terms of the UK ITSEC Scheme and complies with the requirements for:

E3 - Assurance Level
F-B1 - Functionality Class

date 24th December 1996 signed

R. PIZER
Head of the Certification Body

dti

Deutsches IT-Sicherheitszertifikat

BSI

BSI-DSZ-CC-0396-2007

IBM AIX 6L for POWER V5.3
Technology level 5300-05-02
with Argus Systems Group PitBull
Foundation Suite 5.0 and optional IBM
Virtual IO Server (VIOS) Version 1.3

from

IBM Corporation and
Innovative Security Systems, Inc.

sponsored by

IBM Corporation

Evaluation Results:

PP Conformance: Labeled Security Protection Profile (LSPP), Issue 1.b, 8 October 1999

Functionality: PP conformant (plus product specific extensions)
Common Criteria Part 2 extended

Assurance Package: Common Criteria Part 3 extended
EAL4 augmented by ALC_FLR.1 - Basic flaw remediation

Bonn, 10 January 2007

The President of the Federal Office
for Information Security

Security Certified

Protection Levels: What They Really Mean

Here is a description of what each PL means in practical terms and what kind of operating systems are needed for each level.

Protection Level	Clearance/Approval Status	Operating System	
1	Everyone on the system is cleared and approved to see everything on the system	No operating system requirements for security enforcement except for login	any OS
2	Everyone on the system is cleared and approved to see everything on the system, but we want to limit access to some things by some users	Standard commercial operating systems with the ability to have users control access to their own files	any well-configured OS
3	Everyone on the system is cleared to see everything on the system, but not everyone is approved to see everything, so we must enforce a formal need-to-know policy	Standard commercial operating systems with strong configuration and extra tools to limit access to files based on a need-to-know policy	
4	Not everyone is cleared to see everything on the system, but the range of clearances is typically SEC with releasabilities or TS with compartments, but sometimes UNC-SEC or SEC-TS can be approved	Operating systems that have a “mandatory access control” (MAC) capability built into them to restrict access by users to files, networks, and other objects based on the users’ clearances	
5	Not everyone is cleared to see everything on the system and the system can support essentially any collection of user clearances on the system simultaneously	Operating systems that have MAC built into them plus are designed with high assurance separation and hardening	

Environments Ideal for PitBull Security

- Electronic Commerce
- Internet Banking
- Financial Services
- Multinational Commands
- ASP/CSP/ISP Servers
- Transaction Database Servers
- Medical/Health Services
- Secure Web Servers
- PKI / Certificate Authorities
- Trusted Firewalls

PitBull Mechanisms

PitBull's Six Key Architecture Mechanisms

1) Compartmentalization (isolation)
2) Polyinstantiation (file system objects and network objects)
3) Unidirectional low-to-high data flow
4) Unidirectional high-to-low data flow
5) Immutable data storage
6) Roles and role-based access to executables
7) Highly restricted privilege model (no superuser/root)

Note: these are all independent, orthogonal mechanisms that can be used together or separately

Compartmentalization (isolation)

1) Collections of programs can be isolated in compartments
   - no interaction by networking, file systems, or IPC
   - doesn't involve VMs, compartments, or chroot
2) Compartments can contain compartments
   - PitBull supports 4096 simple compartments
   - PitBull supports over 8 million duplex compartments
3) All processes and files can by managed using standard tools
   - system management can be relatively simple

Polyinstantiation

- Networking
  - multiple programs can simultaneously listen on the same port
  - network traffic is automatically routed to the appropriate process
- File system
  - there can be multiple files with the same name in the same directory

…a single installed program can be run multiple times simultaneously without having to reconfigure its networking and file system parameters

Unidirectional low-to-high data flow

1) PitBull supports US DoD classifications, compartments, and releasabilities
2) Full multilevel security (MLS) using the Bell-LaPadula model
   - complete support for DoD PL4
3) Adding, deleting, and managing labeling components is simple
   - there are no rules or relationship databases
4) Enforced for *all* system components
   - file system, printers, GUI, networking, devices, etc.

Unidirectional high-to-low data flow

1) Supports the Biba models for integrity controls
2) Protects high-integrity files and process from being corrupted by low-integrity users and processes
3) Can be used in conjunction with the low-to-high controls to create highly specified security policies and data flow controls

Immutable data storage

1) PitBull adds the concept of operational vs configuration mode
2) File system objects can be marked to be immutable while the system is in operational mode
   - cannot be modified, moved, renamed, or deleted
   - there is no user, administrator, or role that can override this restriction
   - no process, no matter how privileged, can bypass this control
3) Referred to “trusted computing base” (TCB) on PitBull

Roles and role-based access to executables

1) Any executable can be restricted to be run by only certain roles
2) Users can have zero or more roles
   - a user's role can affect how an application or utility will run
   - privilege level can be determined by the role of the user
   - internal functionality can be different based on the role of the user
   - provides for multiple admin types and division of responsibility
3) PitBull has a "four-eyes" mechanism to enforce 2-person admin
   - at login, a user may have to wait for 2-person authorization

Highly restricted privilege model

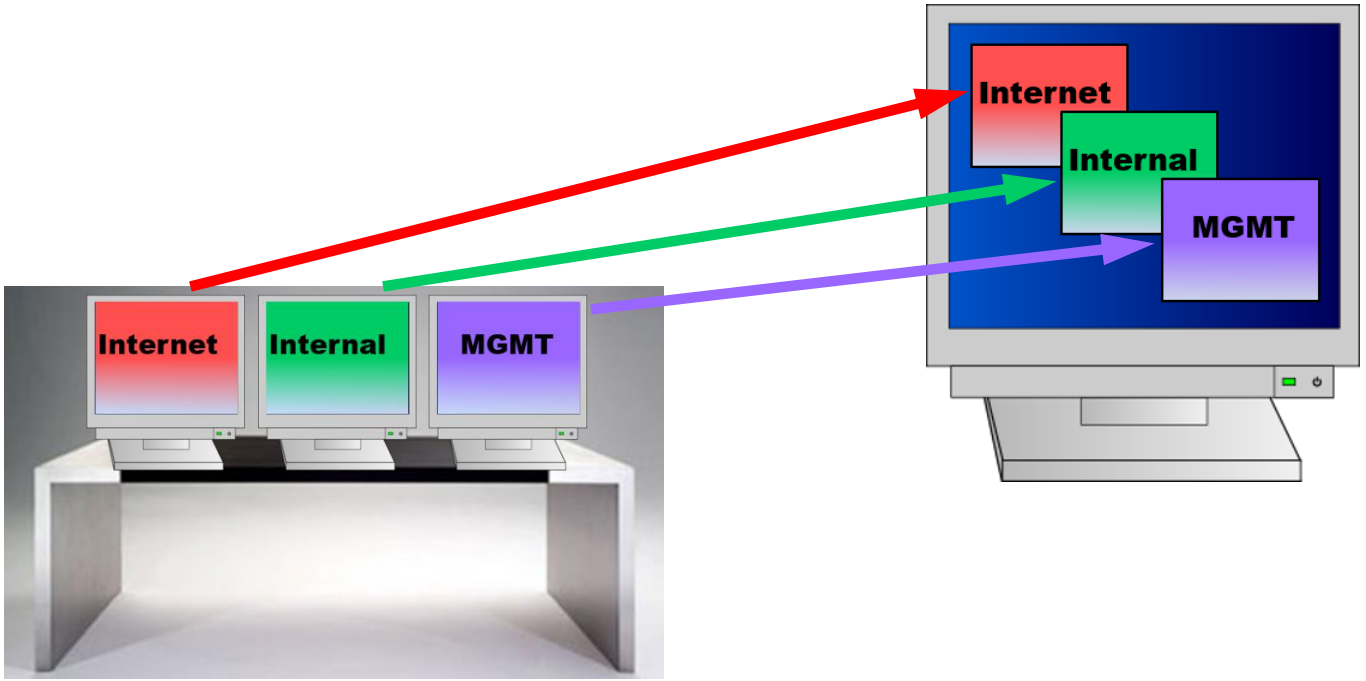
1) Superuser/root has been eliminated from the kernel
2) Fine-grained privileges can be assigned to programs and processes
3) PitBull has strong protections against privilege escalation
   - admin controls can override programmer controls
   - permanent, non-overridable limits to privilege escalation
   - comprehensive and meticulous algorithms for privileges on exec()

Multilevel Desktops

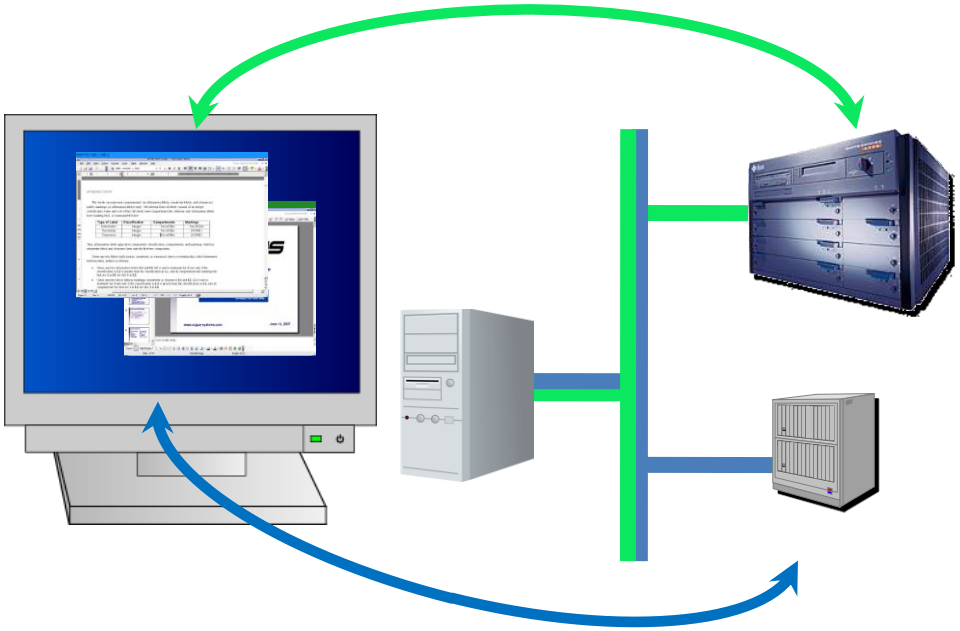
Multilevel Desktops

- PitBull solves the multiple box problem
- PitBull networking, OS, and X Window security create an integrated MLS desktop environment
- Cut-and-paste between windows is fully supported
  - Can be limited based on roles of users

Consolidating user hardware



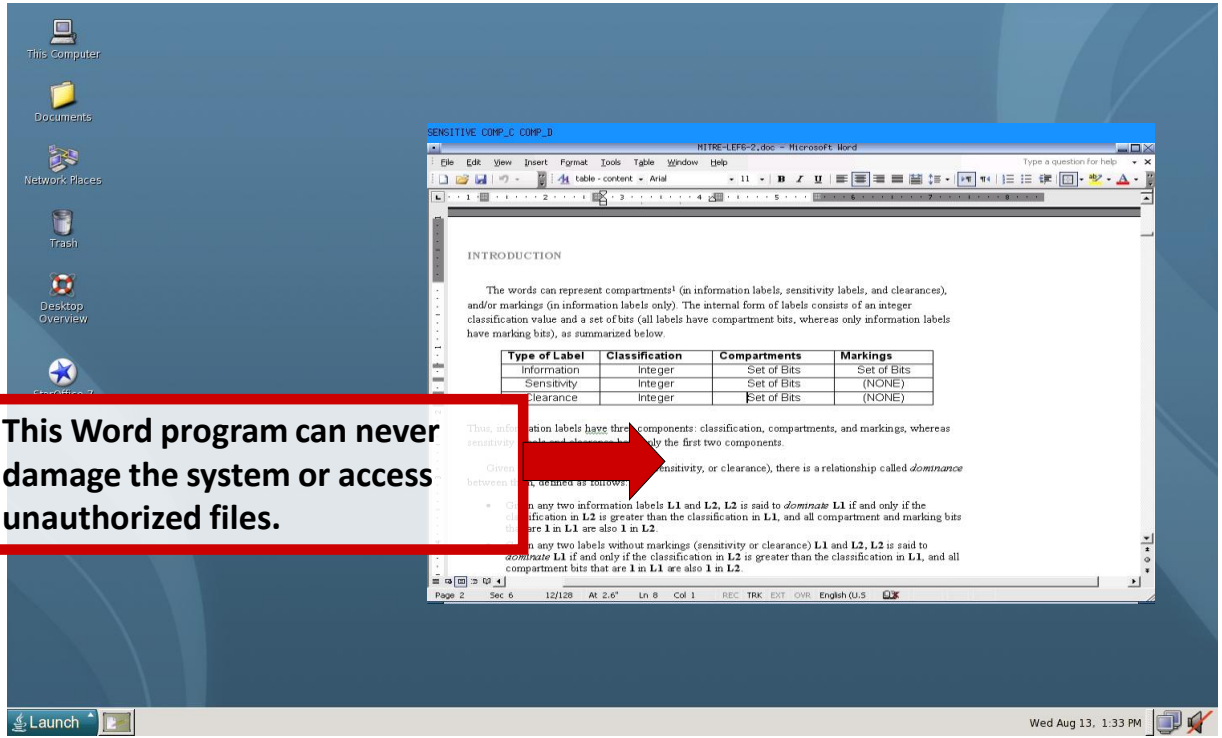
MLS From Desktop to OS to Network



Example uses of a secure desktop

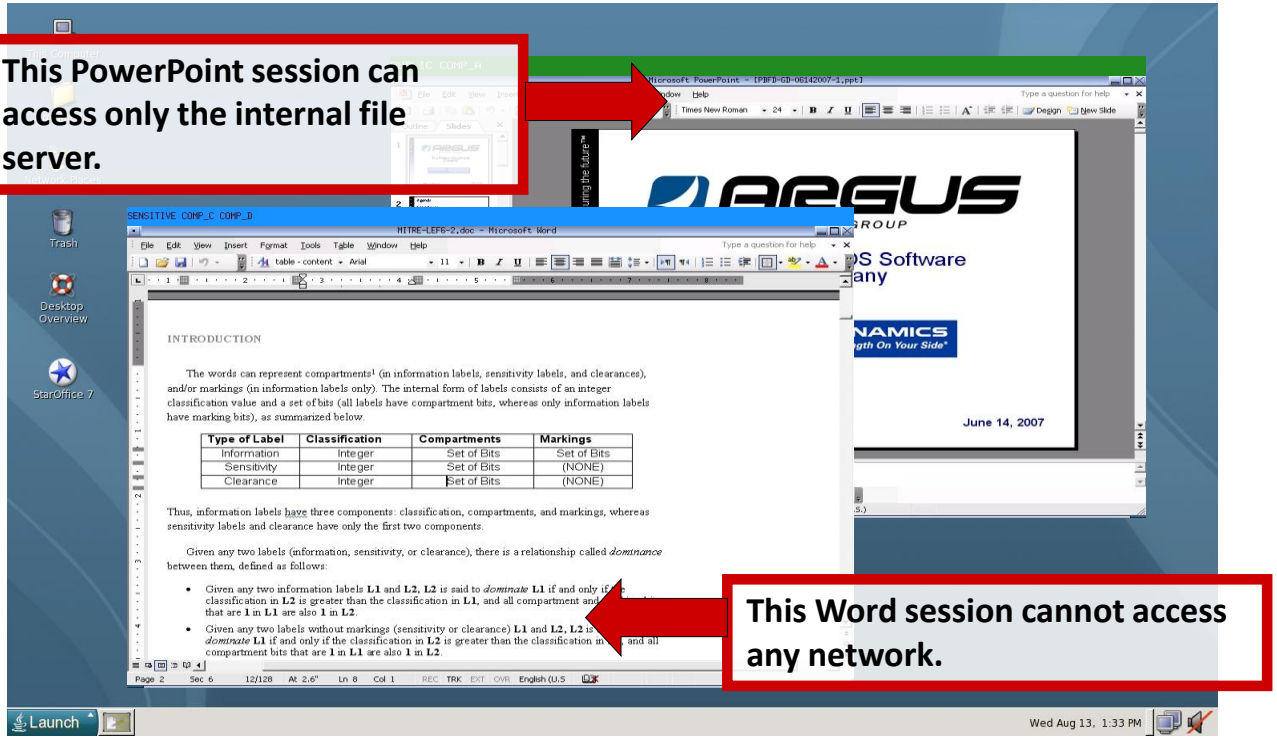
- Simultaneous browser sessions securely open to internal and external web servers
- External servers accessible for copying information into sensitive documents with no danger of system attack or data leakage to outside networks
- Documents of different security levels simultaneously viewed and edited without danger of accidentally releasing restricted data
- Using the system as a personal desktop while the system is supporting administrative and infrastructure services

Example #1: Operating system protection



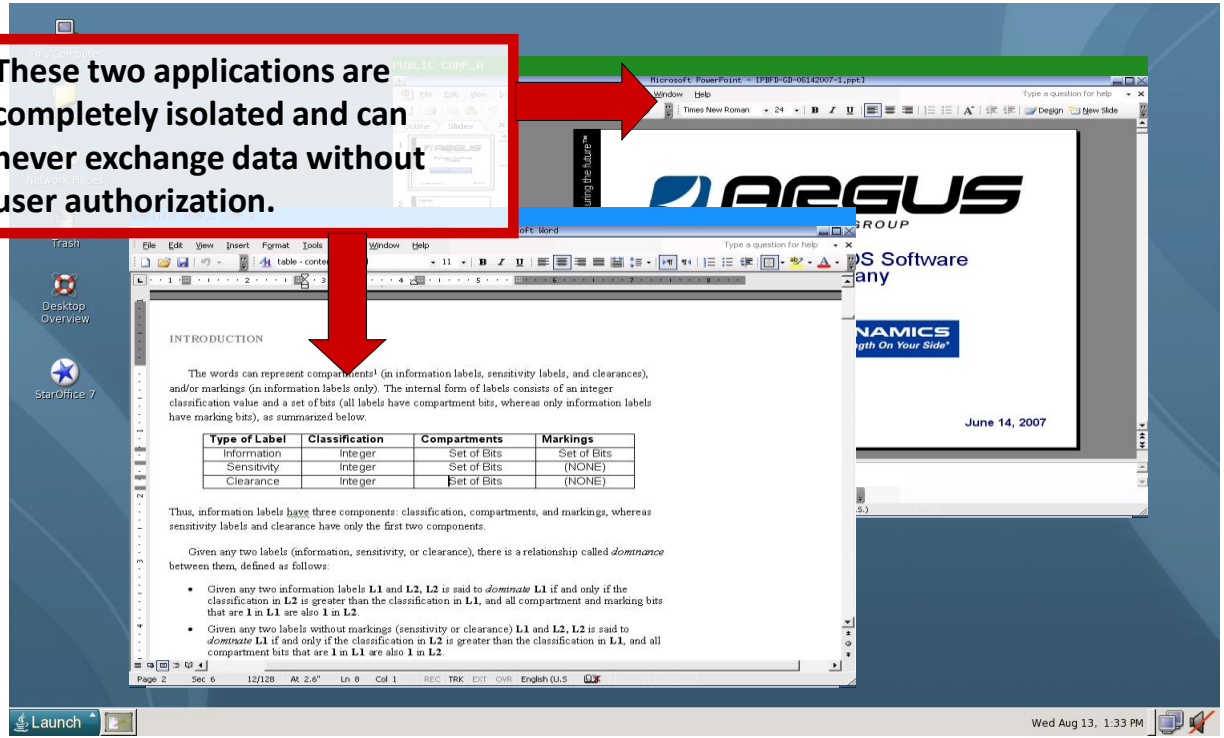
Markings are for demonstration purposes only

Example #2: Network protection



Markings are for demonstration purposes only

Example #3: Application isolation

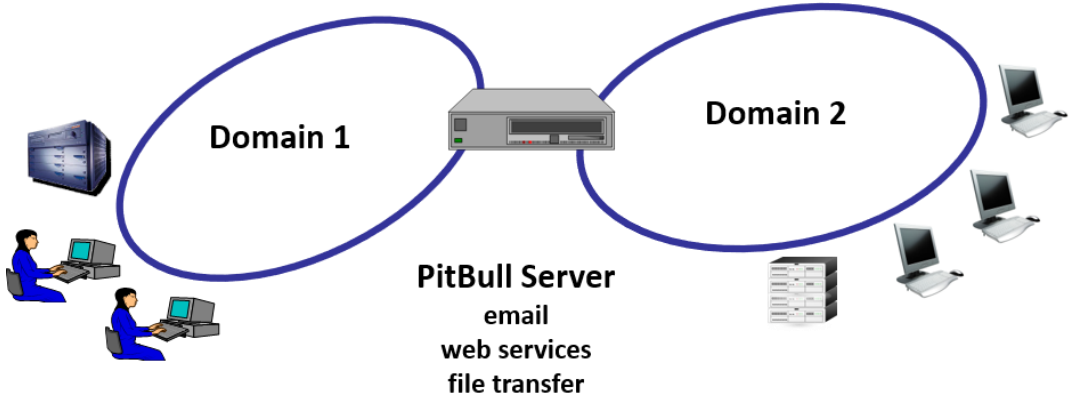


Markings are for demonstration purposes only

PitBull Use Cases

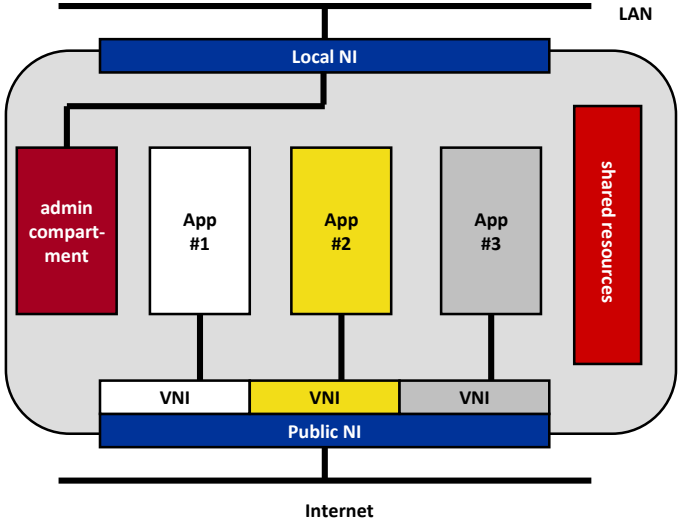
Use Case #1: Multidomain Servers

- Multiple networks can connect to a single server
- Domains can be isolated or hierarchical
- No "leakage" between domains
- Same file names / URLs resolve to different files



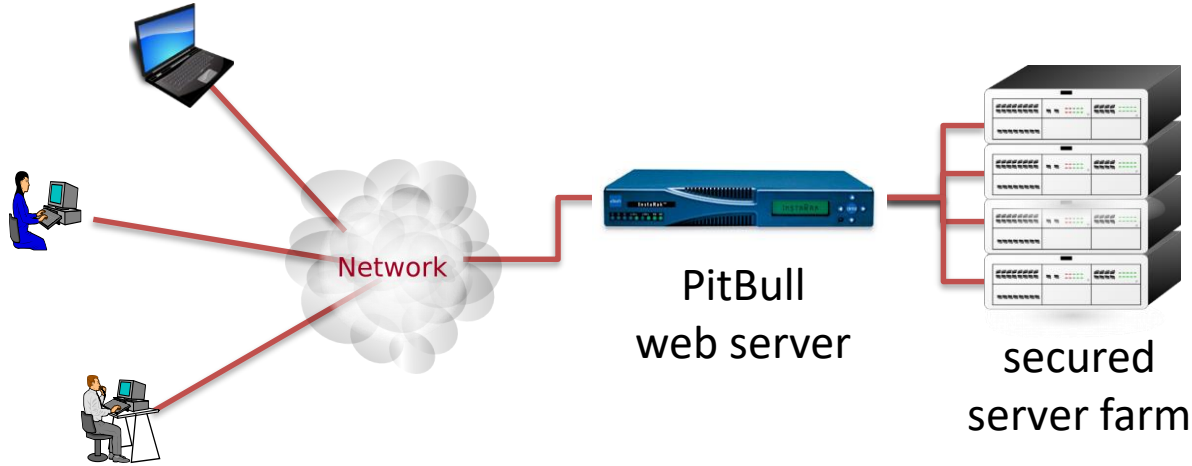
Use Case #2: Polyinstantiated App Servers

- Multiple instantiations of a single installed app
- App files are part of one administrative file system
- No danger of cross attack or data compromise



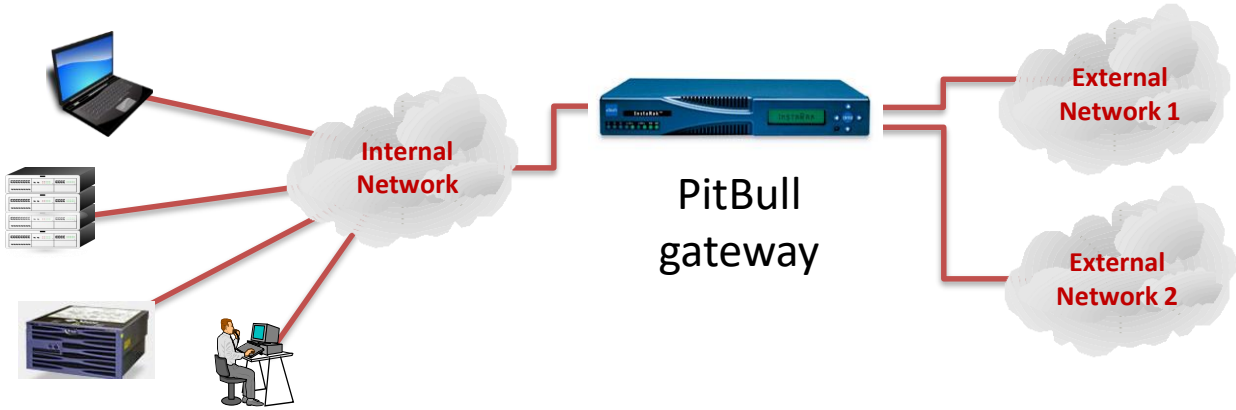
Use Case #3: High Security Web Servers

- Web apps on server are isolated from each other
- Front end / back end are strongly separated
- Strong protection against sophisticated attacks



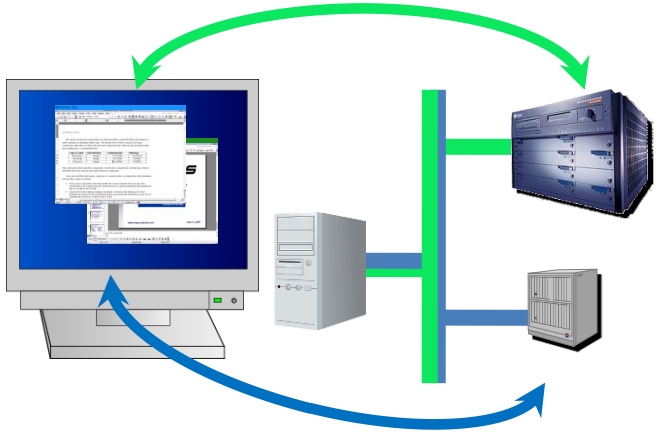
Use Case #4: Targeted Partner Gateways

- Highly secured external-internal connectivity
- Fine-grained remote access down to file level
- File/URL names resolve based on external network
- Hierarchy possible on remote hosts / networks



Use Case #5: Multihomed Desktops

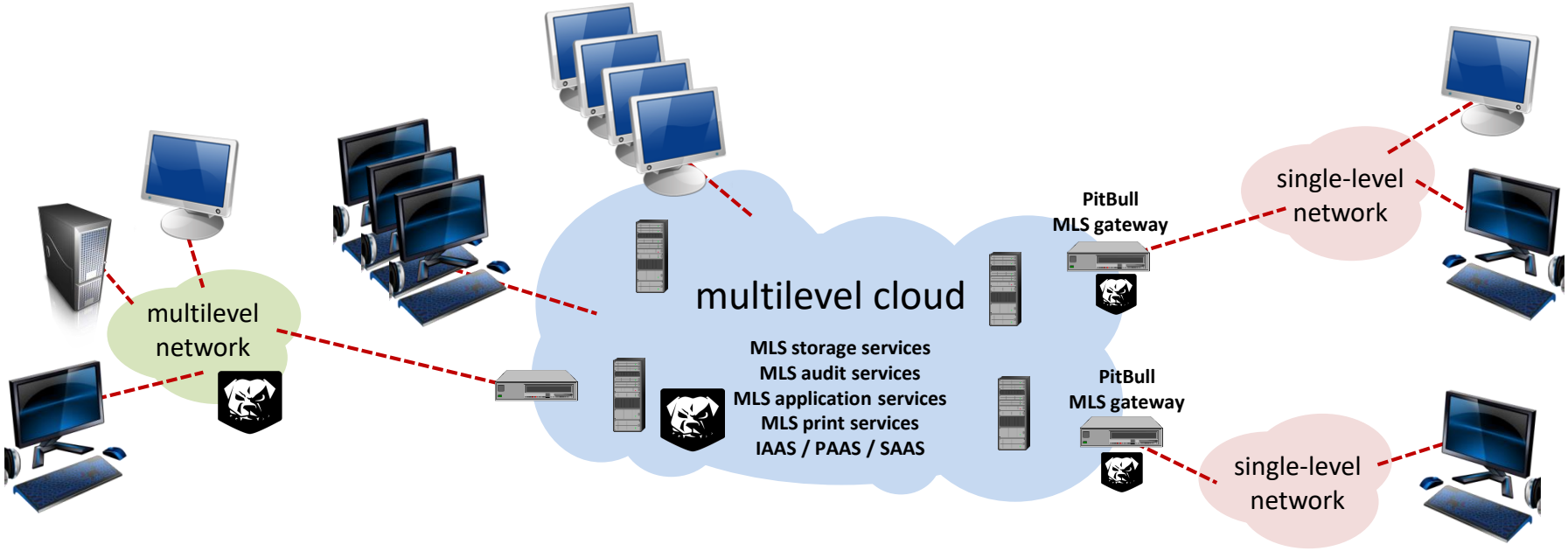
- A desktop system can connect to multiple networks
- Apps run associated with one network
- No chance of internal or network-level data leakage



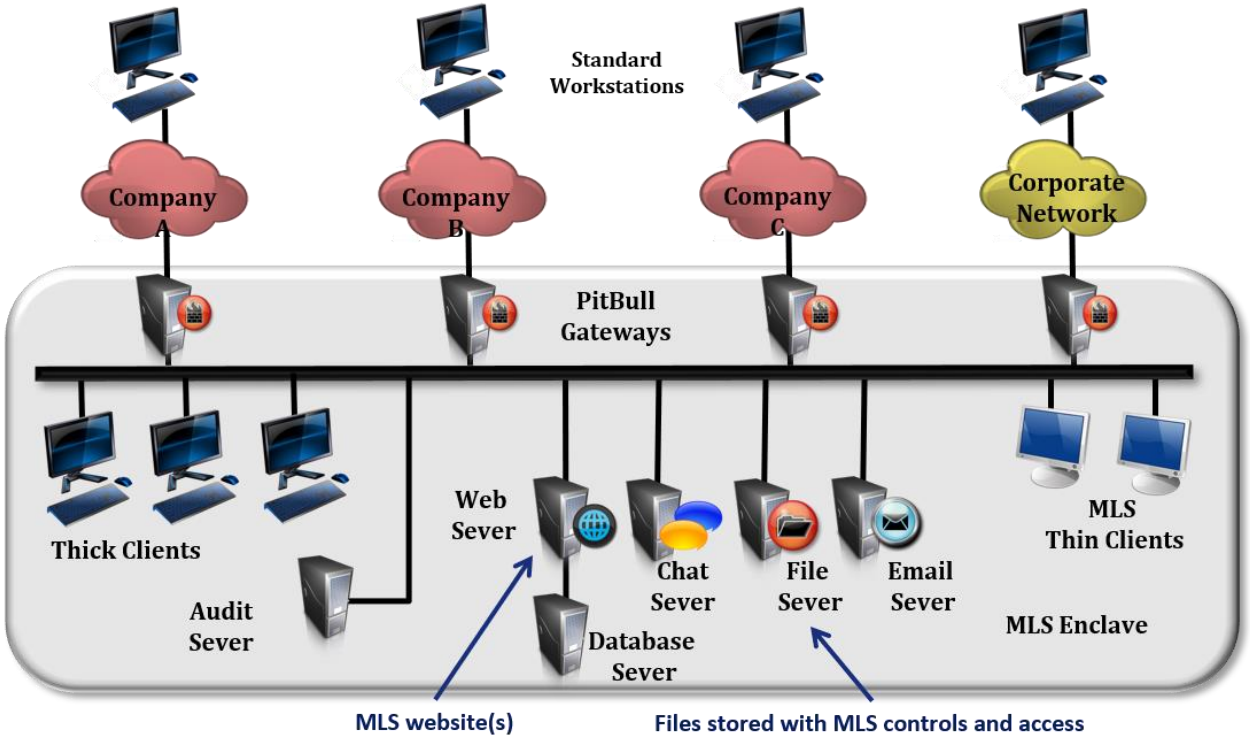
Use Case #6: Multilevel (MLS) Cloud

- PitBull can be the basis for an MLS cloud
  - complete support for MLS storage and services
- Legacy single-level (PL2/3) networks can be connected
  - a PitBull MLS gateway will enforce label controls
  - all systems on the SL network will be marked with the correct labeling
- Other MLS networks can integrate seamlessly with the MLS cloud
- Web-based or MLS workstation access to cloud services

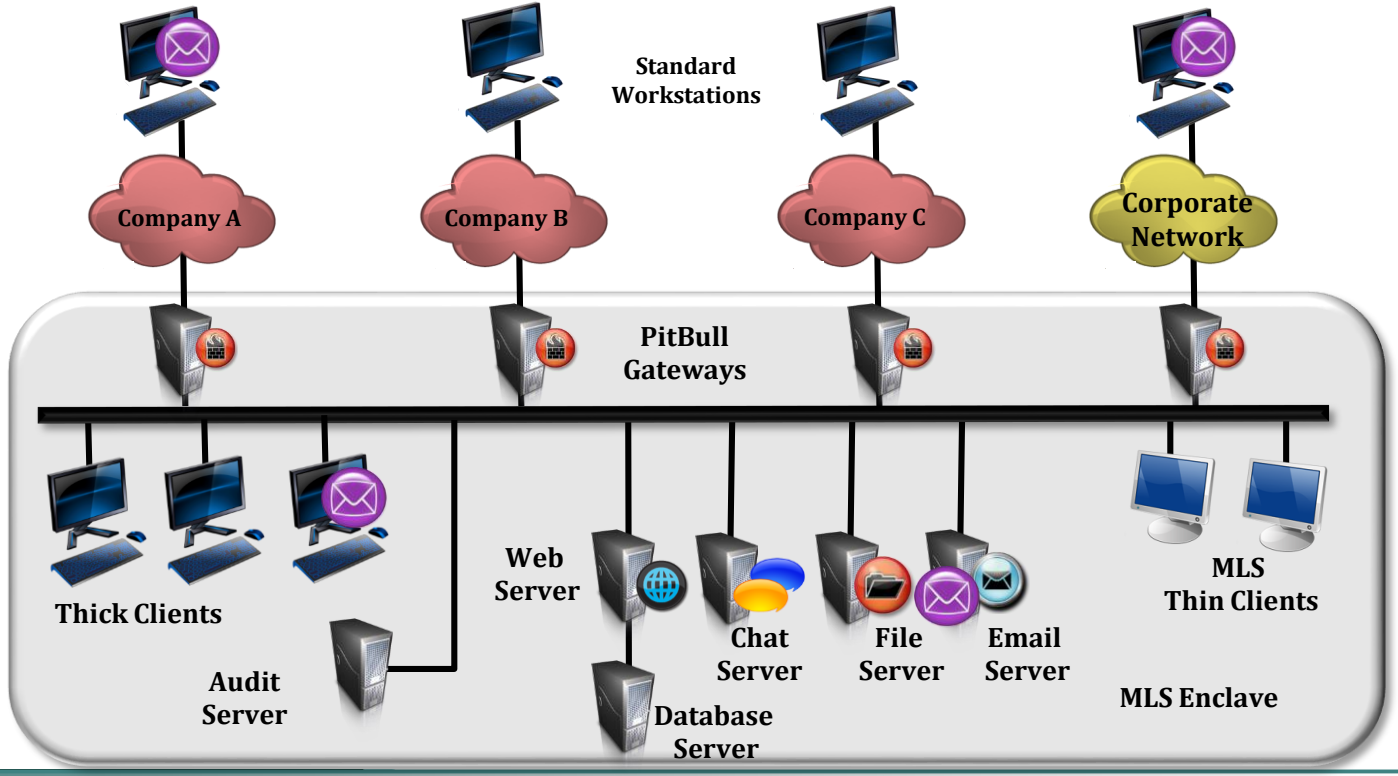
Use Case #6: MLS Cloud (cont'd)



MLS Enterprise Architecture



MLS Email Between Compartments



More about PitBull

Compatibility Issues – Program Integration

- PitBull is binary and source compatible with RHEL
  - enhanced API and ABI
- Any program without a kernel module can be made to work on PitBull
  - all can be made more secure
  - some can be made very secure
- Most programs with a kernel component can be made to work
- PitBull software can be compiled on non-PB systems
  - requires only header files and libraries

Compatibility Issues – Non-PitBull Systems

- PitBull systems integrate seamlessly into networks
- A PitBull system can impose security on non-PB systems
  - you specify the security of network interfaces and hosts
- A PitBull system can connect a remote port, host, subnet, or network interface with its file system security policy

Compatibility Issues – User Apps

- User/desktop apps for Linux will work on PitBull
  - StarOffice, etc.
- A VM running Windows can be run on PitBull
  - VM networking will be controlled by PitBull
- WINE-based products support Microsoft® apps
  - Crossover from CodeWeavers supports MS Office ®

Software Development Issues

- PitBull extends the RHEL API
  - new system calls and libraries
  - extended functionality in existing system calls
- Software for PitBull can be compiled on non-PitBull systems
- Main topics programmers need to know:
  - programming issues related to privilege
  - secure programming practices
- An advanced training course is available for software developers writing programs to be run on PitBull

PitBull Training Courses

- Bull Introductory Training
- PitBull Advanced Training *
- PitBull Software Developer Training
- PitBull Webapp Software Developer Training

* ***under development***

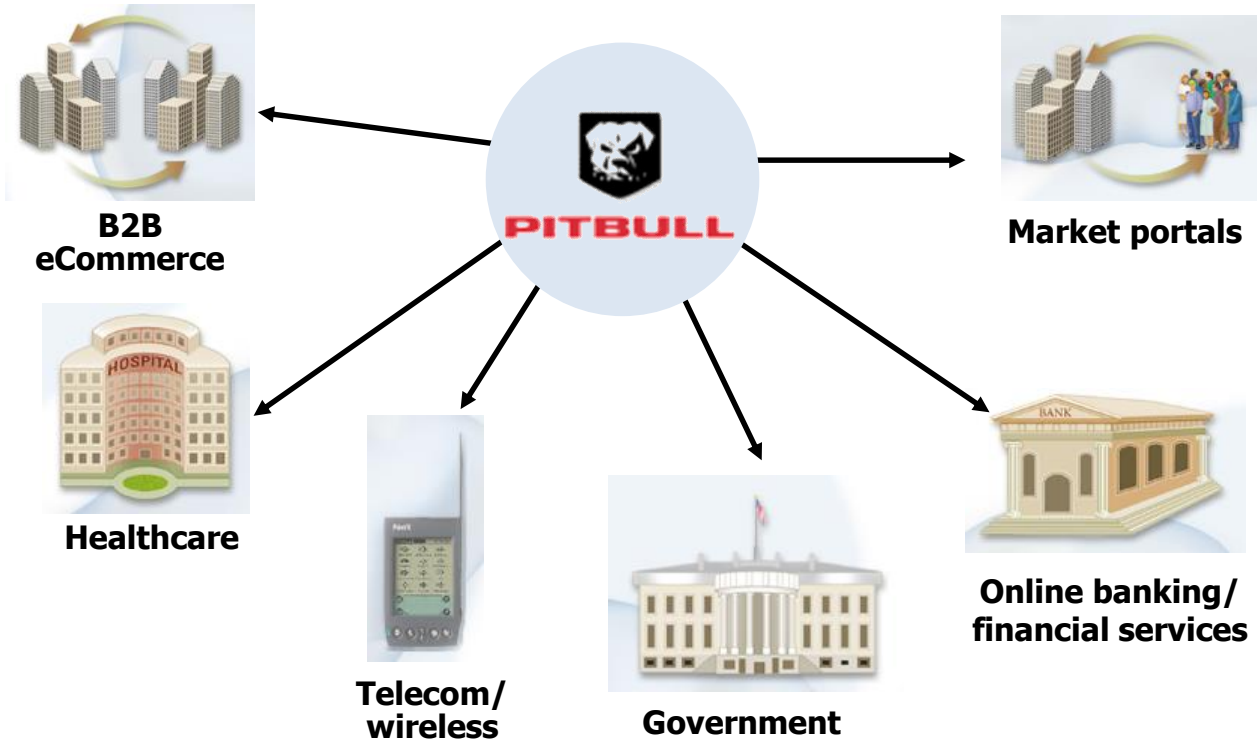
Key "Only" Points about PitBull

- Security only
  - no new functionality is added
- Software only
  - no hardware components
- Linux only
  - but interoperable with other systems
- Operating system only
  - no encryption, firewall, access control

Why PitBull?

- It’s REAL
  - It has been deployed in operational environments for over 25 years.
- It’s FUNCTIONAL
  - The underlying technology has been evaluated at EAL4 under LSPP. Networking is fully integrated. Unmatched features.
- It’s EASY
  - Installation is trivial. Lock down tools are included. Training is available.
- It’s COMPATIBLE
  - All applications work without the need for source code modification.

Where is PitBull needed?



Questions and Answers