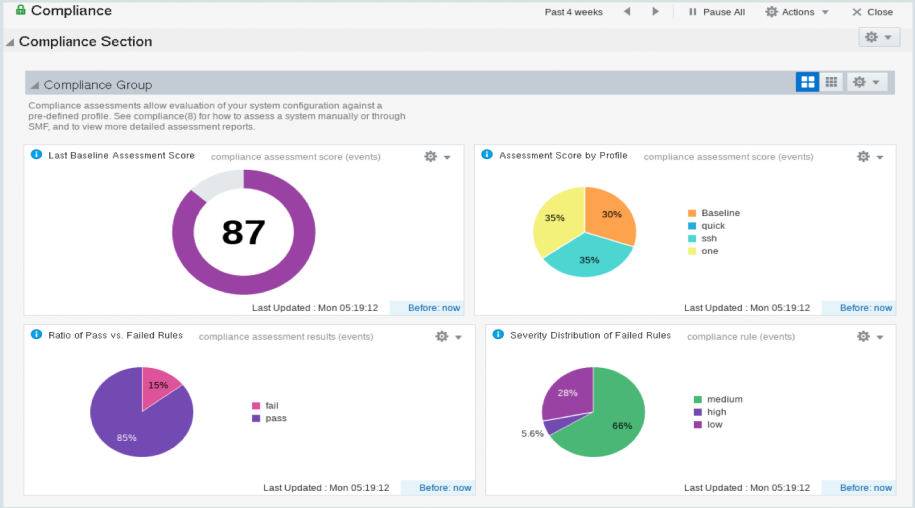

ORACLE®



Oracle Solaris Security Advantages: from Hardware to Compliance

Keeping Solaris workloads secure & compliance from inception to retirement

Darren J Moffat
Senior Software Architect
Oracle Solaris Engineering

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Continuous Security
3 Axis of Risk needs 3 Axis of Control

People

RADIUS Authentication, OpenSSH, Kerberos PKINIT (X.509). Kerberos data in LDAP. Root login disabled by default. Role auth via user password, Authentication caching. Auditing on by default, audit policy in SMF, Secure remote audit trail. Sudo with auditing. Fine-grained user/group/command/RBAC management, LDAP support. /etc/pam.d Linux Compat & Minimisation, Per User PAM stack, Kerberos client multi master, Last failed login time Audit Remote Server Extended Policy – privileges on objects, pfedit, auths admin command, RAD usermgr **Time Based and Access control Qualified User Attributes**

Platform

Immutable Zones, Sandboxing: new basic privileges, further executable address space reduction. Network data-link & IP anti-spoofing for Zones. Transparent Hardware Encryption for Solaris, Java. OpenSSL 4x faster. file integrity scanner Signed binaries & packages, Boot Key Management, appliance integration, FMA & Security Extensions Framework, rsyslog (GSSAPI & TLS), OpenSCAP Compliance tool, TPM key migration, SHA512/t, Large DSA keys, Intel RDRAND, AES XTS, Perf improvements SPARC & Intel, PCI Compliance Reporting, Verified Boot Immutable Zones for Global and Kernel Zones, Kerberos Credentials for Delayed Execution, Kerberos integration with Auto Install

Data

Per File Audit, ZFS filesystem, swap, dump and zvol encryption, NFSv4/NT style ACLs, Multilevel security with file labeling, IPsec/IKE policy per zone. Per Zone NFS server and Kerberos Realm. Per file security labels, multiple zones per security label, 1024 groups for AUTH_SYS/NFS

Authentication/Account Management

Core PAM modules

- UNIX pam_unix_{auth,cred,account}
  - Traditional Username/Password but using strong hashes
  - All the password complexity and aging rules you **shouldn't** use but we provide
  - Time/Day based Access
- LDAP (OUD, OpenLDAP or Active Directory with RFC2307 schema)
- Kerberos (MIT or Active Directory KDC)
- Smartcard
  - pam_pkcs11 + PC/SC + USB CCID (New in Solaris 11.3 SRU)

Authentication / Access Control

- One Time Password HOTP/TOTP (New in 11.3 SRU)
  - pam_otp_auth: Works with iOS/Android Apps and YubiKey hardware tokens
- RADIUS authentication via pam_radius_auth (11.4 Beta)
  - Configuration set in svc:/network/radius/client
  - Traditional RADIUS and RADIUS over TLS
  - Often this is OTP but from a centralized service
- pam_fm_notify Alert on FMA issues at administrator login (11.4 Beta)
- pam_list enhancements
  - Wildcard, UNIX Group and file comments (11.3 SRU)

Authentication

- Authentication policy set per system:
  - /etc/security/policy.conf:PAM_POLICY=ldap
- Per User authentication policy overrides
  - Policy stored with RBAC data

```
# usermod –S ldap –K pam_policy=ldap+radius darrenm
# usermod –S ldap –q @prod_db_hosts –K pam_policy=otp darrenm
# usermod –S ldap –q @dev_web_hosts –K pam_policy=unix darrenm
```

Authentication Policy at Install Time

- Legacy of multiple configuration files from SVR4 + Solaris
  - /etc/default/login
  - /etc/default/passwd
  - /etc/default/su
  - /etc/security/policy.conf
- New SMF service svc:/system/account-policy:default
  - Multiple property groups and more modern sensible property names
  - Opt in and uses SMF stencils, svcio(8), to write out the legacy files
  - Allows use of customization via SMF layers
  - Better integration with SMF aware Configuration Management system

Control Where & When

Scoping RBAC Profiles

- Qualification of profile assignments to: user/host/netgroup
  - LDAP lookup order:
    - Host specific
    - Netgroup specific
    - Unqualified
- Allows granting a user rights on a subset of hosts
- Use in conjunction with Time Based control & Multi-factor
- For Example:
  - Network Management only granted Mon-Fri 9-5 on development hosts
  - Require use of Password + OTP

Granting administrator rights

Directly assigned to users, alternative to using shared account roles

```
# usermod –S ldap –q @dev –K profiles+=”Network Management” darrenm
$ pfexec ipadm create-addr …

# usermod –K auth_profiles+=”Network Management” darrenm
$ ipadm create-addr …
Re-authentication by darrenm is required to use profile:
      Network Management
(Use ^C to cancel)
Password: ************
OTP Code: ******
```

Auditing administrative change

Who, What, When, Where

- First introduced with SunOS 3.5 as unbundled extra
- On by default in Solaris 11.0 for login/logout only
  - Significantly more audit records generated by default in 11.4
  - Audit records visible via Stat Store and WebUI
- Events generated by privileged programs, syscalls, kernel subsystems
- Events grouped into Classes
- Upload events to Oracle Audit Vault, or send binary trail over secure transport or use syslog
- Session Annotation (at login and privilege elevation) (11.4 Beta)

But Why ? Why,did you do that ?

Session Annotation

- One line description of why you are here making change
  - Expected to be a ticket number or similar from your change control process
- Set at login and privilege elevation
- Policy set via user_attr entries annotation=[yes|no|optional]
- Stored in the process cred and recorded in every audit record

```
$ ssh sc-db-ldm-kz-146.example.com
Password:
Session Annotation: SR-3-4526292 patch update
Last login: Thu Mar  1 17:16:26 2018 from 10.163.198.80
NOTE: system has 4 active alerts; run 'fmadm list' for details.
Oracle Corporation      SunOS 5.11      11.4.Beta   December 2017
sc-db-ldm-kz-146$ pfexec admhist
```

Administrative History

admhist(8)

- Shell History like view on the audit trail with easy date ranges
- Subset of auditrail for interesting administrative change events
- Mostly commands that used some privilege

```
$ ssh sc-db-ldm-kz-146.example.com
Password:
Session Annotation: SR-3-4526292 patch update
Last login: Thu Mar  1 17:16:26 2018 from 10.163.198.80
NOTE: system has 4 active alerts; run 'fmadm list' for details.
Oracle Corporation      SunOS 5.11      11.4.Beta   December 2017
sc-db-ldm-kz-146$ pfexec admhist
2018-02-27 23:30:02.201+00:00 /usr/sbin/zfs destroy builds/ssh-upgrade
2018-03-01 17:22:42.550+00:00 /usr/bin/vim vi /etc/security/policy.conf
2018-03-01 17:26:36.857+00:00 /usr/bin/vim vi /etc/user_attr
```

Per File Audit

Finally able to see the wood from the trees (11.4 Beta)

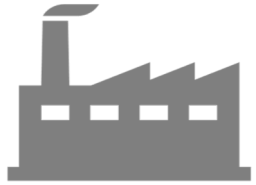
- Until now file change auditing in kernel was only via syscalls
  - Generates far to many records that are next to impossible to read
  - All or nothing, and filtering could only be done by auditreduce in postprocessing
  - Performance impact to some applications
  - Didn't work for NFS or SMB remote access
- Now set policy via ACL – using chmod(1) or even from Windows SMB tool
  - Supported over NFS and SMB
  - No impact on syscall performance
  - Meaningful audit records

Per File Audit

Finally able to see the wood from the trees (11.4 Beta)

```
# chmod A+everyone@:write_data:successful_access:audit /data


header,159,2,open(2) - write,creat,trunc,ace,laptop-vm,2018-03-06
09:24:41.349+00:00

subject,darrenm,oracle,staff,oracle,staff,12402,4040703500,171 2 laptop-vm

path,/data/ora.ini

attribute,100644,oracle,staff,65538,278044,18446744073709551615

return,success,4
```

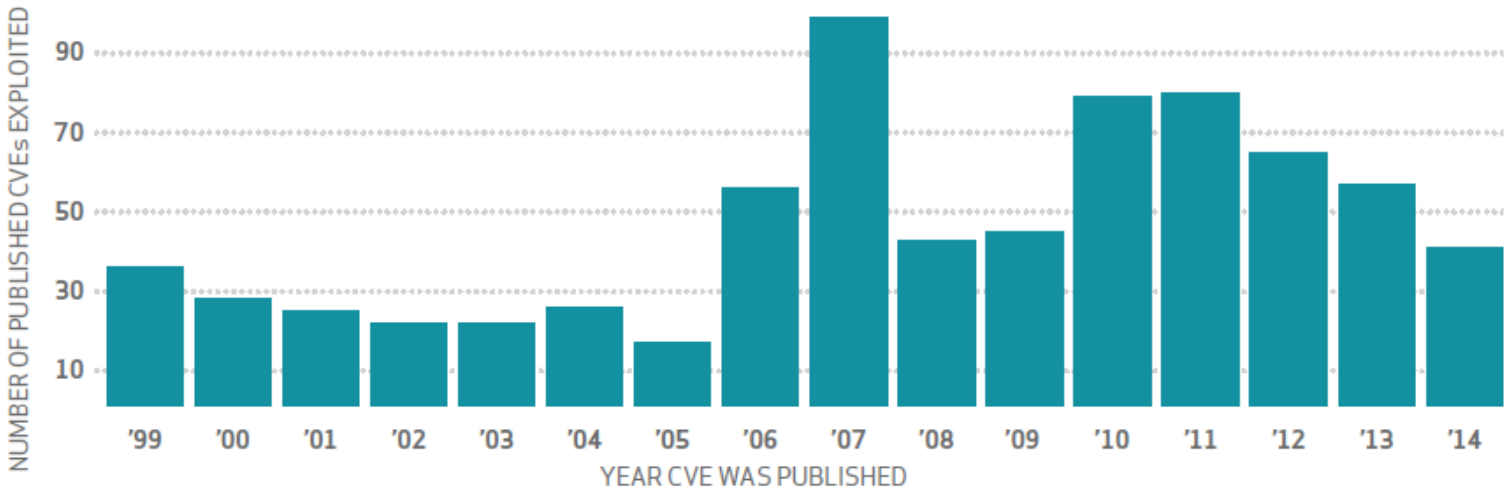
Install Compliant Minimized Oracle Solaris

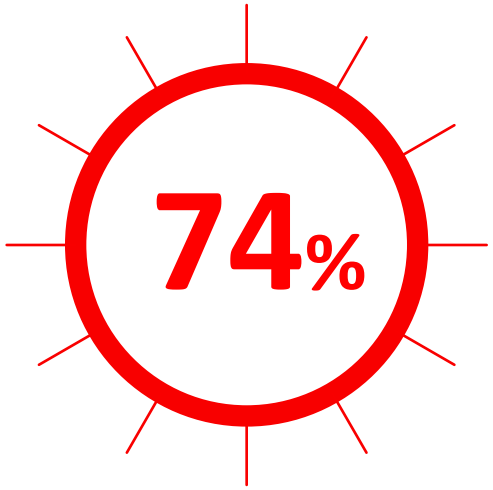


- If it isn't installed
  - You don't need to patch the security vulnerabilities
  - Your auditor won't get false positives on versions
  - It can't be configured in a non-compliant way
- Group packages as starting points
  - Add only what you need
  - Packages removed from a group stay removed unless required in future for a dependency.
  - Better to start small & add than start big & remove
- Signed packages using secure transport from boot loader onwards

- **pkg:/group/system/solaris-minimal-server**
  - Minimal supported installation
- **pkg:/group/system/solaris-small-server**
  - Adds major features such as Oracle Solaris Zones
- **pkg:/group/system/solaris-large-server**
  - Adds most features including automated installer, many more services
- **pkg:/group/prerequisite/oracle/oracle-rdbms-server-12-1-preinstall**
  - Oracle Database dependencies
- **pkg:/group/prerequisite/oracle/oracle-ebs-server-R12-preinstall**
  - Oracle E-Buisiness Server R12 dependencies

Exploited Vulnerabilities Compromised





OF ORGANIZATIONS
TAKE 3 MONTHS+
TO PATCH

Source: Verizon Data Breach Investigations Report, 2015; IIOUG Data Security Survey, 2014

One Step Security Patching

```
# pkg update solaris-11-cpu@latest
```

The solaris-11-cpu IPS package contains the CVE number to package version mapping.

Integrated with Compliance Reporting

Considering a Security Fix only support train for future releases

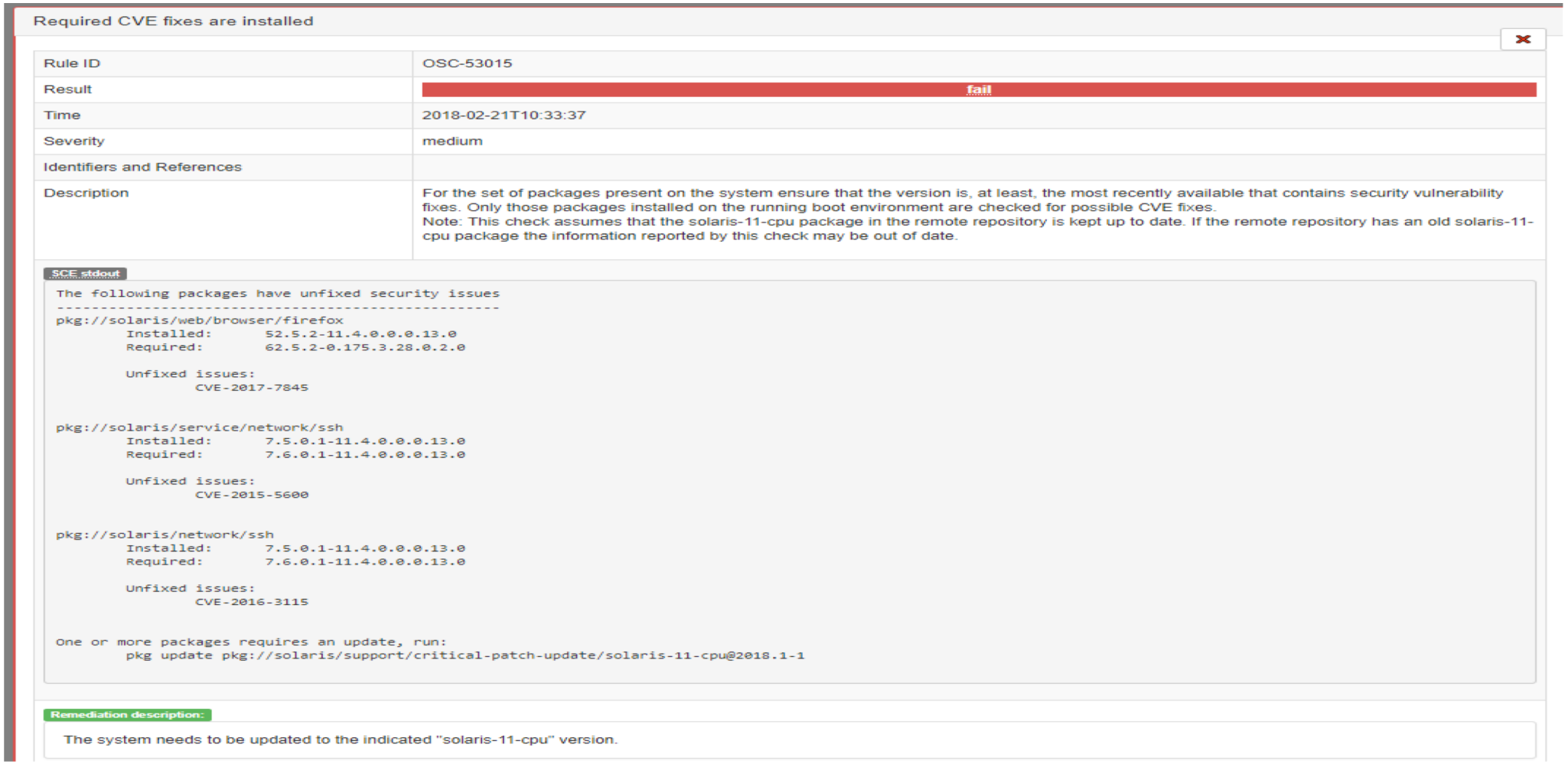
ORACLE

Compliance Reporting

Why Solaris Compliance reporting?

- Auditors want comprehensive reports
  - Don’t always have deep knowledge of OS, Application, Deployment Context
  - Auditors often use tools which use wrong interfaces for OS release
- Configuration reporting is a low value activity for expensive staff
- Provide **correct** compliance check interfaces for OS release
- Provide vendor interpretation of security controls (> 235 checks)
  - *New checks for Solaris Cluster and LDOMs planned for 11.4*
- Don’t *force* customers to use 3rd party products –
  - Integrate with them using standard data formats SCAP/OVAL/XCCDF
- Integrates with Oracle Enterprise Manager Compliance Pack

Detailed CVE Reporting for Compliance



Required CVE fixes are installed

Rule ID	OSC-53015
Result	fail
Time	2018-02-21T10:33:37
Severity	medium
Identifiers and References	
Description	For the set of packages present on the system ensure that the version is, at least, the most recently available that contains security vulnerability fixes. Only those packages installed on the running boot environment are checked for possible CVE fixes. Note: This check assumes that the solaris-11-cpu package in the remote repository is kept up to date. If the remote repository has an old solaris-11-cpu package the information reported by this check may be out of date.

SCE stdout

```
The following packages have unfixed security issues
---------------------------------------------------
pkg://solaris/web/browser/firefox
        Installed:      52.5.2-11.4.0.0.0.13.0
        Required:       62.5.2-0.175.3.28.0.2.0

        Unfixed issues:
                CVE-2017-7845


pkg://solaris/service/network/ssh
        Installed:      7.5.0.1-11.4.0.0.0.13.0
        Required:       7.6.0.1-11.4.0.0.0.13.0

        Unfixed issues:
                CVE-2015-5600


pkg://solaris/network/ssh
        Installed:      7.5.0.1-11.4.0.0.0.13.0
        Required:       7.6.0.1-11.4.0.0.0.13.0

        Unfixed issues:
                CVE-2016-3115


One or more packages requires an update, run:
        pkg update pkg://solaris/support/critical-patch-update/solaris-11-cpu@2018.1-1
```

Remediation description:

The system needs to be updated to the indicated "solaris-11-cpu" version.

Multi-Node Periodic Compliance Reporting

Because nobody has just one Oracle Solaris system

- Muti-Node compliance reporting
  - Push or Pull results
- SMF compliance service
  - Declares system benchmark/profile/tailoring
  - Set assessment schedule using SMF periodic
    - Default is once a day for Solaris Baseline
- Assessments now stored by UUID
  - Find and produce summary report based on matching parameters
- Dashboard & Trending via Stat Store & WebUI

Compliance

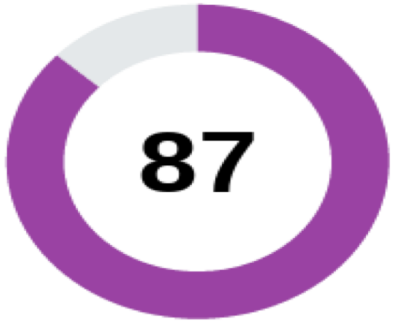
Past 4 weeks | Pause All | Actions | Close

Compliance Section

Compliance Group

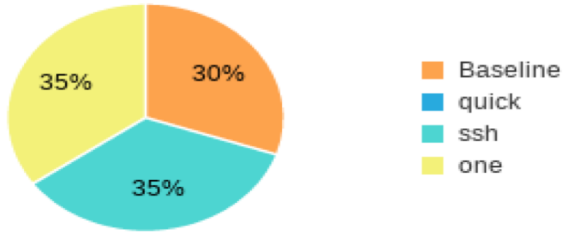
Compliance assessments allow evaluation of your system configuration against a pre-defined profile. See compliance(8) for how to assess a system manually or through SMF, and to view more detailed assessment reports.

Last Baseline Assessment Score — compliance assessment score (events)



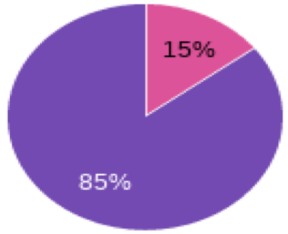
Last Updated : Mon 05:19:12 | Before: now

Assessment Score by Profile — compliance assessment score (events)



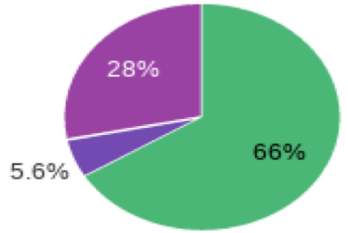
Last Updated : Mon 05:19:12 | Before: now

Ratio of Pass vs. Failed Rules — compliance assessment results (events)



Last Updated : Mon 05:19:12 | Before: now

Severity Distribution of Failed Rules — compliance rule (events)

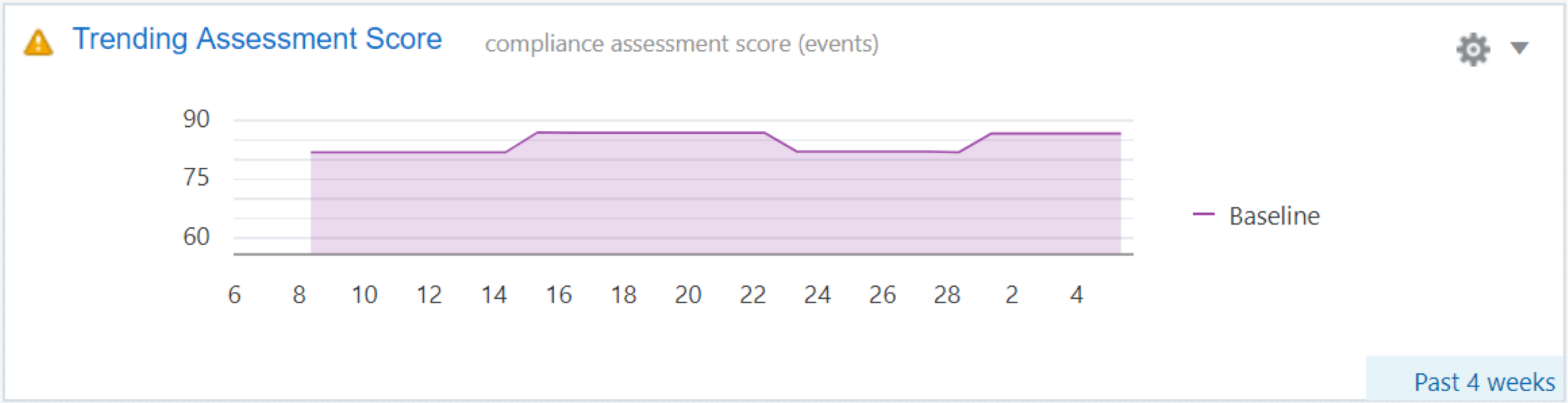


Last Updated : Mon 05:19:12 | Before: now

Compliance assessment is point in time

Trend should be more important

Compliance assessments allow evaluation of your system configuration against a pre-defined profile. See compliance(8) for how to assess a system manually or through SMF, and to view more detailed assessment reports.



System Identity X.509 Certificate

svc:/system/identity:cert

- RAD/REST and Web Dashboard need a well formed certificate for TLS
  - Generating one that browsers accept isn't easy with openssl or even pktool
- Deliver system key/certificate at install time via SMF profile
  - svc:/system/identity:cert
- Or auto-generated
- *Warning* of expiry via svc:/system/identity:cert-expiry
- Integrated with svc:/system/ca-certificates
  - Default Trusted Certificate Authorities for RAD & other TLS clients

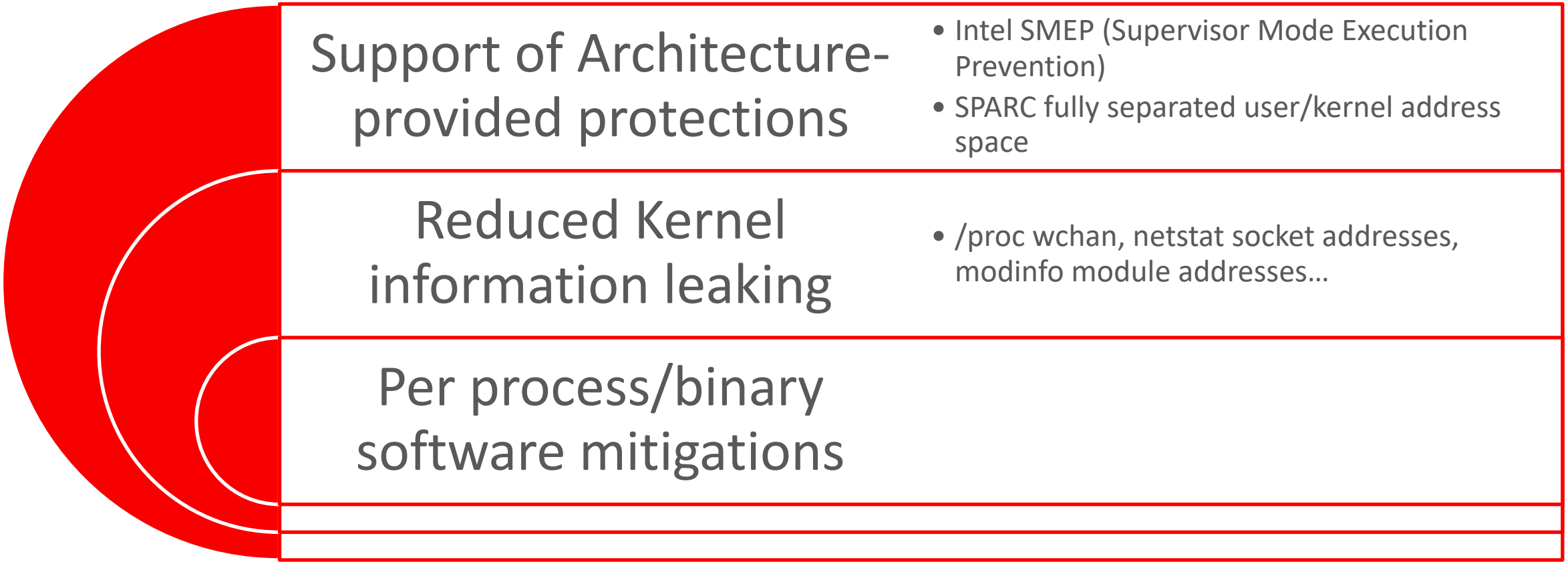
Exploit Mitigation

Introduction

- Prevent or reduce the ability of an attacker to take advantage of a bug
- Study attackers techniques, deploy counter measures
- Tradeoff between performance, usability and security
- Not all scenarios/mitigations are the same
  - Some require hardware support
  - Others require compiler support
  - The best are runtime defences the OS gives you without performance impact
  - **NONE** are full proof

Exploit Mitigation

Architectural features



Exploit mitigation features: sxadm(8)

NXSTACK Non Executable Stack	Been around since Solaris 2.6 but now controlled via sxadm(8) Now **on** by default Tag at build time with: -z nxstack=enable|disable
NXHEAP Non Executable Heap	New in 11.3, not enabled system wide by default since there are a small number of legitimate uses for an executable HEAP. Tag binaries at build time with: -z nxheap=enable|disable
ASLR Address Space Layout Randomisation	Added 11.1 Not enabled system wide by default
sxadm delcust	Go back to vendor delivered defaults
Install Time Policy	svccfg extract security-extensions

Oracle SPARC Exploit Mitigation with SSM for 11.4

ADISTACK Non Executable Stack	Automatic detection of buffer overflows that overwrite the register save area of a stack frame when the save area contains valid contents.
ADIHEAP Non Executable Heap	Heap allocators (such as malloc() in libc) may use this feature to reliably detect adjacent buffer overflows and statistically defend against stray pointers and use-after-free.
Kernel ADI	Kernel Heap Memory and buffer tag protection.

Continuous Security Protection

Tamper Resistant Immutable Systems

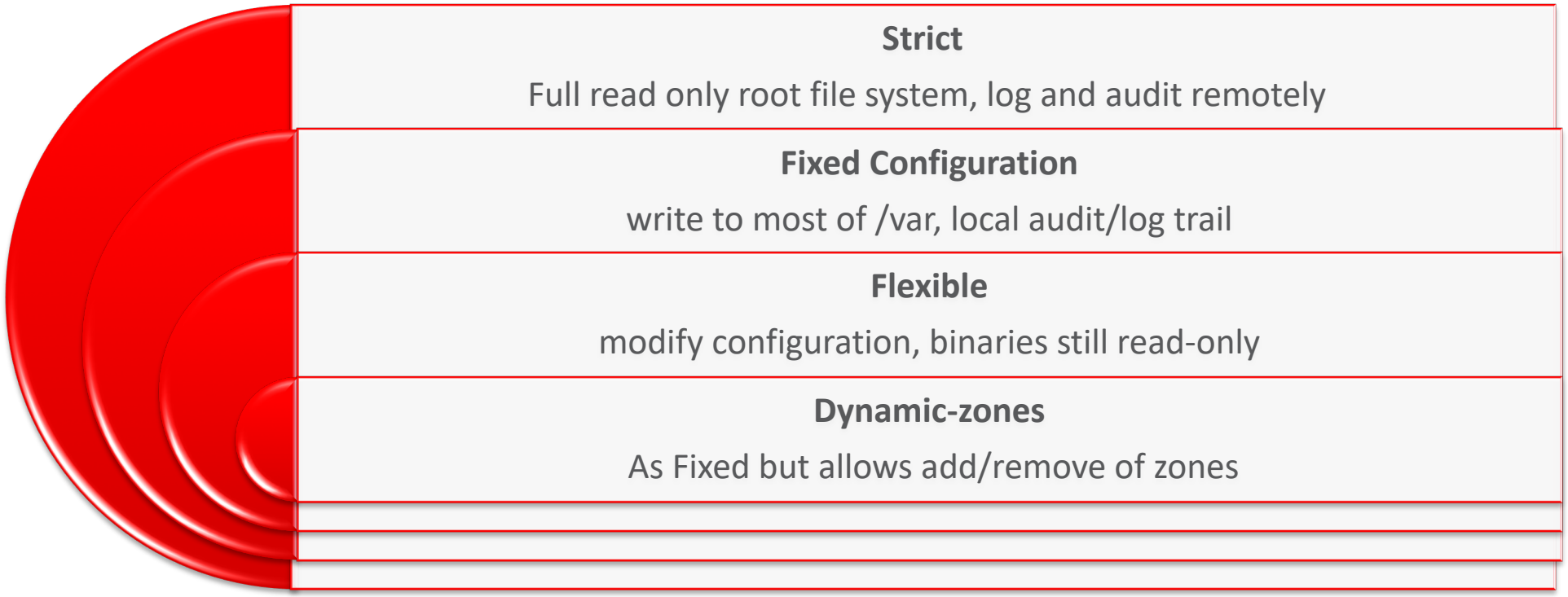
- Reduce risk of establishing a foothold
- Prevent administrator mistakes
- Update even though it's un-writable by admin users and applications

Tamper Evident Software

- Firmware to Applications
- Install only known, trusted software
- Verified Boot

Immutable System

- Lock down a system with preconfigured security profiles
- Trusted Services via SMF (11.4 Beta)



Lifecycle: Immutable Zones at Scale with Puppet

```
# zonecfg -z myzone 'set file-mac-profile=fixed-configuration'
# zoneadm -z myzone boot

# zlogin myzone
[Connected to zone 'myzone' pts/3]
myzone# rm /etc/passwd
rm: /etc/passwd: override protection 644 (yes/no)? y
rm: /etc/passwd not removed: Read-only file system

$ svcprop –p method_context/trusted_path puppet:agent
trusted_path = true

We had to have set puppet up to run on the trusted path previously.
Best practice would be via an SMF profile at initial install
```

Sandboxing Applications

Control Privileged and Non Privileged Applications

- File read & write privileges take pathnames
  - {file_write}:/var/log/my-app-errors.log
- net_privaddr: Port number ranges and protocol
  - {net_privaddr}:443/tcp
- proc_setid: username or uid range
- proc_exec: pathname
- File and proc_exec can use wildcards in last path component eg:
  - {proc_exec}:/usr/bin/*

My auditor says delete all the setuid root programs!

Automatic Sandboxing for setuid root programs

- The setuid bit for a root owned file is now just a marker
- Kernel upcalls to pfexecd asking for privilege specification
- Examples:
  - Forced Privilege:solaris:cmd:RO::/usr/lib/utmp_update:\
  - privs={zone}\:/system/volatile/utmp*
  - Forced Privilege:solaris:cmd:RO::/usr/sbin/ping:\
  - privs=net_icmpaccess,sys_ip_config
  - Forced Privilege:solaris:cmd:RO::/usr/sbin/traceroute:\
  - privs=net_icmpaccess,net_rawaccess
  - Forced Privilege:solaris:cmd:RO::/usr/sbin/whodo:privs=proc_owner

Sandboxing Applications

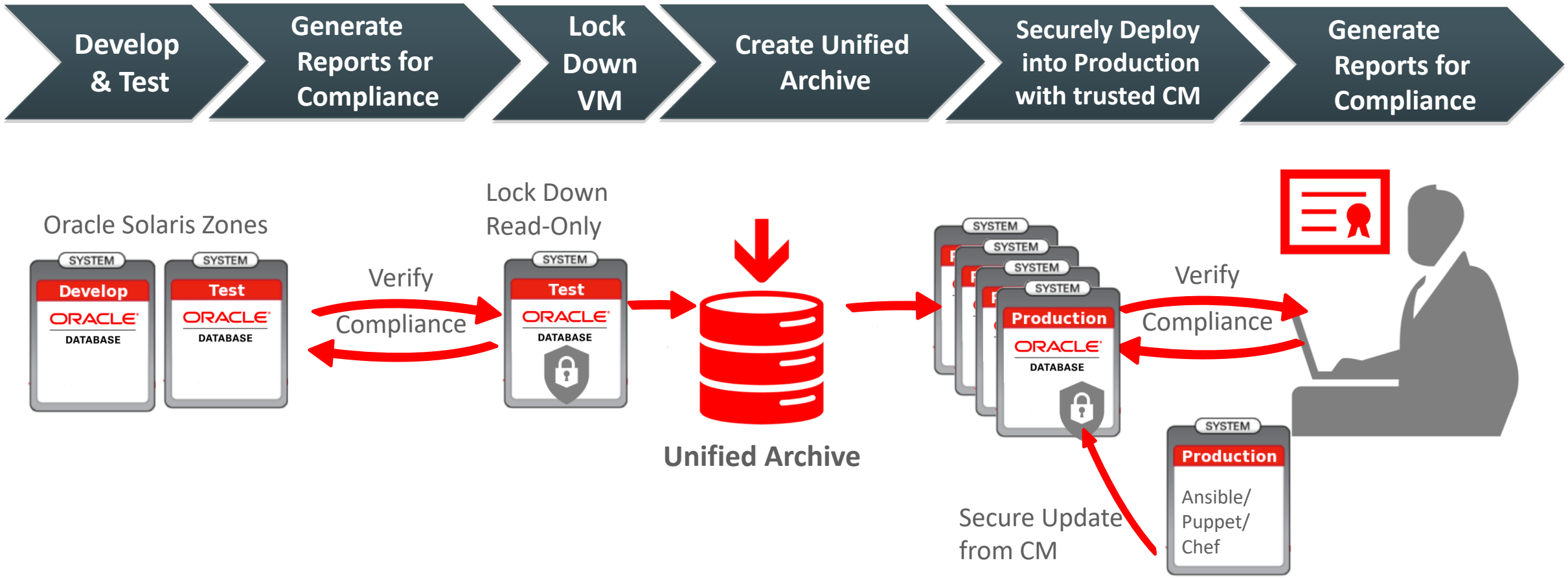
Can’t you make that easier for me ?

- Yes! in Oracle Solaris 11.4 application sandboxing is much easier.
- Sandbox is combination of:
  - privilege
  - process labeling (from Trusted Solaris)
  - Projects
- Ad-hoc and persistent sandboxes

```
# pkg install security/sandboxing
adhoc$ sandbox myapp
```

Install and Maintain Security & Compliance

Traditional or DevOps Deployment



ORACLE
Solaris

Leading Crypto Performance. Easiest to use, integrated Security, and data protection.

Combined with best of breed open source security tools.

Compliance Auditor Friendly

ORACLE


ORACLE®