

Protecting your Linux environment through Identity Consolidation

Who Am I

Patrick van der Veen

- Director, Sales Engineering – Northern Europe
- 3,5 years @ Delinea (Thycotic / Centrify)
- Over 16 years in pre-sales
- Infrastructure, virtualization, disaster recovery, data security, vulnerability management, penetration testing, endpoint detection and response, Privileged Access Management (PAM).



Certified Information
Systems Security Professional



Certified Cloud
Security Professional



Agenda

PAM Maturity Model

Use Cases

Functionality

Windows

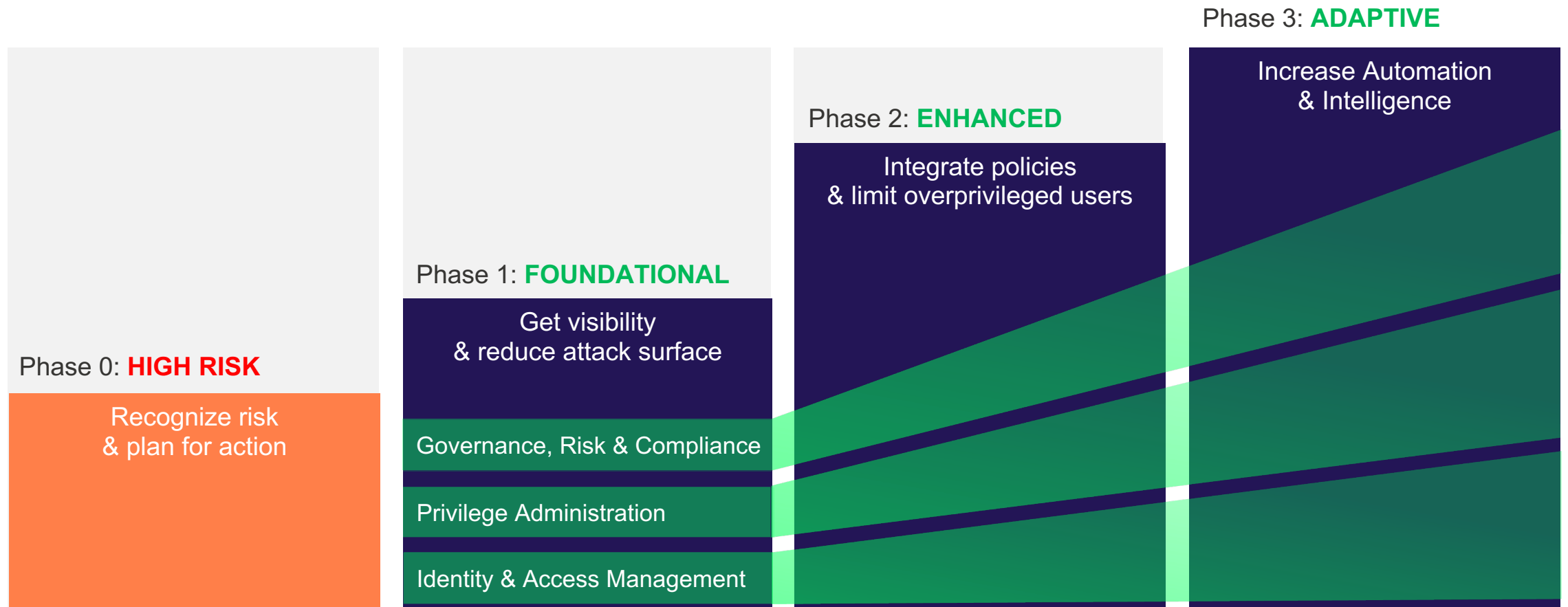
Linux

How it Works

Demo

The PAM Maturity Model

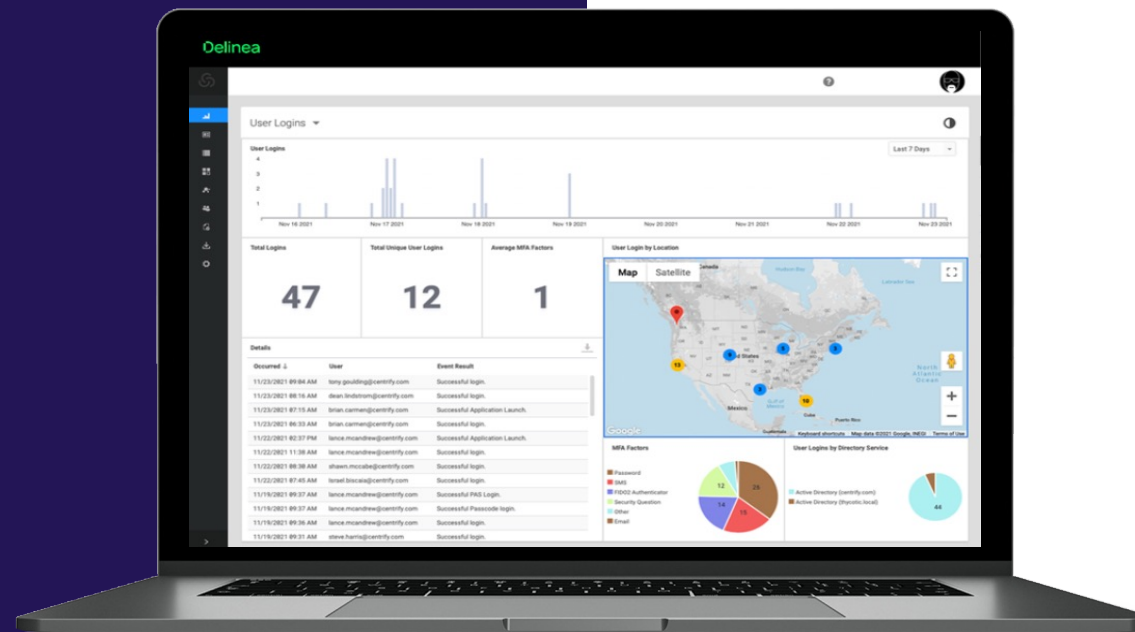
Where does Server Suite fit?





Server Suite

Privileged access
Management across
all Linux, Unix, and
Windows systems



 Consolidate identities

 Zero Trust best practices

 Implement least privilege

 Enforce MFA

 Improve compliance

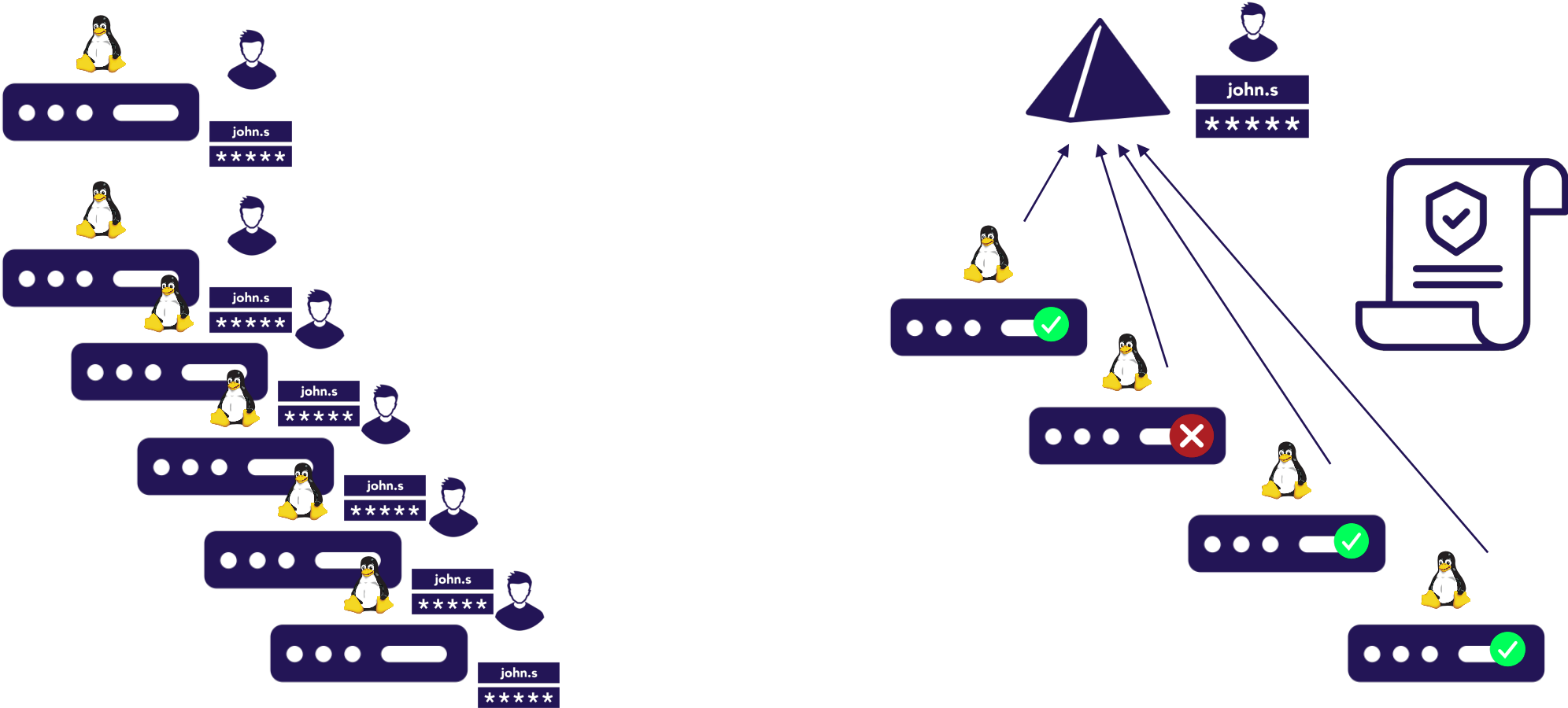
What are we trying to address – Use Cases

Active Directory focus

- Consolidate identities – Linux / Unix
- Centralized configuration management (GPO) - Linux / Unix
- Reduce attack surface by removing standing privileges – Linux / Unix - SUDO management
 - Just in Time
 - Just Enough
- Host level auditing – Linux / Unix

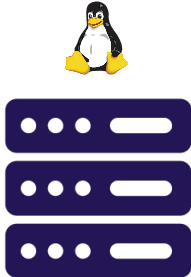
Identity Consolidation / Active Directory integration

Linux / Unix



Reducing attack surface

Remove standing privileges



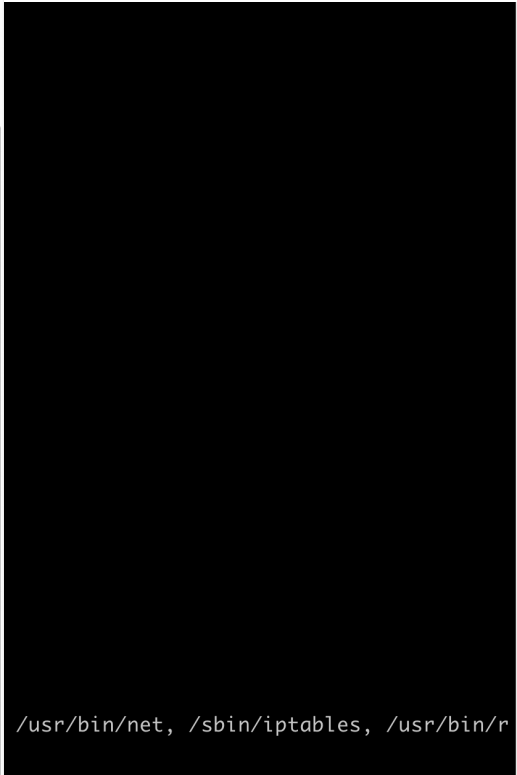
```
[adm-patrick@lab-centos01 ~]$ dzinfo

Always permit login:
false

PAM Application Avail Source Roles
-----
* Yes UNIX Login/Linux
Zone

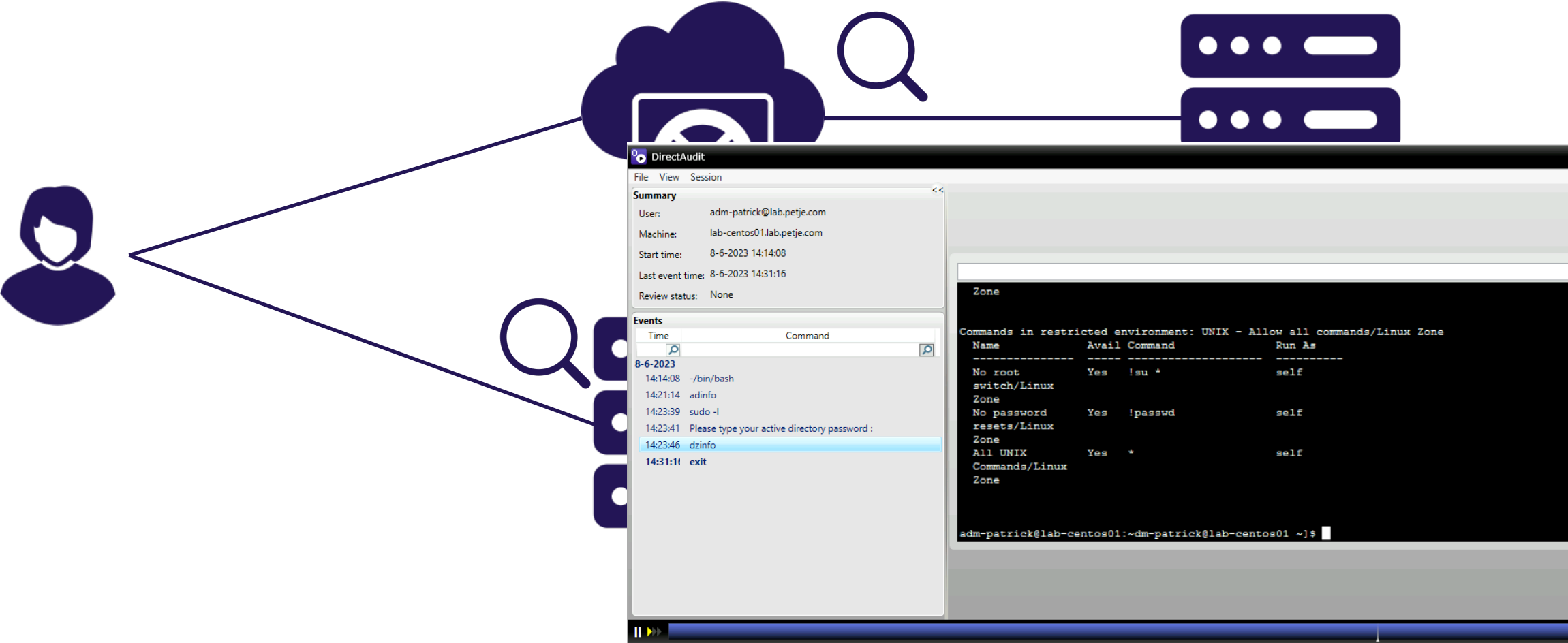
Privileged commands:
Name Avail Command Source Roles
-----
No root switch/Linux Zone Yes !su * UNIX - Allow all
commands/Linux Zone
No password resets/Linux Zone Yes !passwd UNIX - Allow all
commands/Linux Zone
All UNIX Commands/Linux Zone Yes * UNIX - Allow all
commands/Linux Zone

Commands in restricted environment: UNIX - Allow all commands/Linux Zone
Name Avail Command Run As
-----
No root switch/Linux Zone Yes !su * self
No password resets/Linux Zone Yes !passwd self
All UNIX Commands/Linux Zone Yes * self
```



Host level auditing

Record always

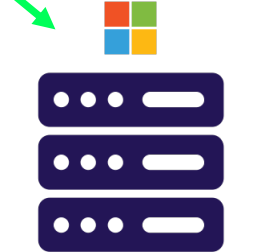
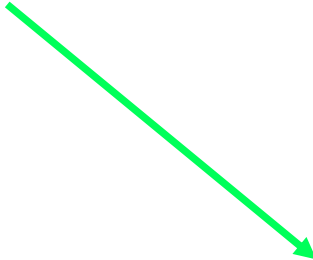
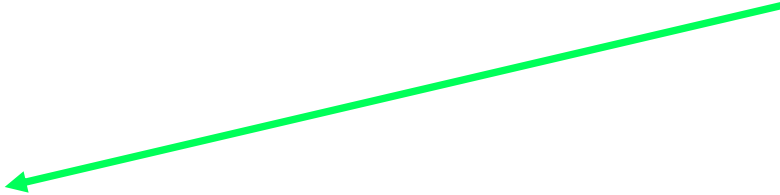
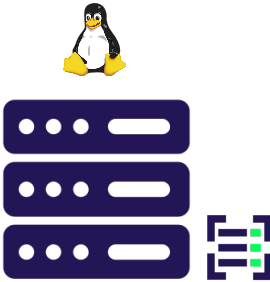




How does it work?

Components involved

Direct Audit



Audit Collector



Audit DB Store

Delinea Audit Manager - [Audit Manager\LabInstallation [lab-sql01.lab.petje.com - DefaultManagementDatabase] \Audited Systems (System-based)]

File Action View Window Help

Audited System	IP Address	Status	Uptime	Last Update Time
lab-ubuntu04.lab.petj...	192.168.50.106	Disconnected		31-3-2023 09:58:16
LAB-DE01.lab.petje.co...	192.168.50.101	Connected	24 days 18 hours 4...	24-4-2023 11:29:51
lab-sql01.lab.petje.com	192.168.50.110	Connected	26 days 13 hours 2...	24-4-2023 11:29:51
lab-ubuntu01.lab.petj...	172.16.0.4	Connected	40 days 23 hours 1...	24-4-2023 11:30:17
LAB-DC01.lab.petje.c...	192.168.50.50	Connected	19 days 23 hours 2...	24-4-2023 11:29:51

Components involved

Direct Audit



Delinea Audit Analyzer - [Audit Analyzer - LabInstallation[lab-sql01.lab.petje.com - DefaultManagementDatabase]\Audit Sessions\Unix DirectAudit Related Action]

File Action View Window Help



Audit Analyzer - LabInstallation[lab-sql01.lab.petje.com - DefaultManagementDatabase]

User	Display Name	Account	Machine	Auc
Enter text here	Enter text here	Enter text here	Enter text here	Enter text here

- ▼ Audit Sessions
 - > All, Grouped by User
 - > All, Grouped by Machine
 - > All, Grouped by Audit Store
 - > Today
 - > Yesterday
 - > This Week
 - > This Month
 - > Active Sessions
 - > Sessions to be Reviewed
 - > Sessions Pending for Action
 - > Unix Password Access
 - > Unix Software Installation
 - > Unix Privileged Commands
 - > Unix DirectAudit Related Actions
 - > Windows MMC Tools
 - > Windows UAC Prompt
 - > Windows Command Prompt
 - > Windows Registry Editor
 - > Windows DirectAudit Related Tools
 - > Linux Desktop Sessions
 - > Sessions to be Deleted
 - > Infrastructure Services - Privileged sessions
- > Audit Events
- > Reports

21 items

DirectAudit

File View Session

Summary

User: adm-patrick@lab.petje.com
Machine: lab-ubuntu01.lab.petje.com
Start time: 17-9-2021 09:41:56
Last event time: 17-9-2021 10:57:28
Review status: None

Events

Time	Command
17-9-2021	
09:41:56	-/bin/bash
09:41:58	dainfo
09:48:21	dcinfo
09:48:31	adinfo
09:50:28	sudo visudo
09:50:30	Please type your active directory password :
10:32:49	dainfo
10:56:13	id
10:56:22	sudo visudo
10:56:24	Please type your active directory password :
10:57:28	dzdo -l

```
-/bin/bash
adm-patrick@lab-ubuntu01:~$ dainfo
Pinging adclient: adclient is available
Daemon status: Online
Current installation: 'LabInstallation' (configured locally)
Current collector: LAB-CSS01.lab.petje.com:5063:HOST/LAB-CSS01.lab.petje.com
.PETJE.COM
Session offline store size: 484.00 Bytes
Dequeue rate: 0.00 Bytes/second
Audit trail offline store size: 0.00 Bytes
Getting offline database information:
  Size on disk: 7.50 KB
  Database filesystem use: 3.15 GB used, 28.90 GB total, 25.74 GB free
DirectAudit NSS module: Active
User (adm-patrick) audited status: Yes
DirectAudit is not configured for per command auditing.
adm-patrick@lab-ubuntu01:~$
```



DEMO

Conclusion / Summary

- Consolidate identities – Linux / Unix ✓
- Centralized configuration management (GPO) - Linux / Unix ✓
- Reduce attack surface by removing standing privileges – Linux / Unix - SUDO ✓
 - Just in Time
 - Just Enough
- Host level auditing – Linux / Unix ✓



Thank you

Delinea

Defining the boundaries of access