



Privileged Management

Eliminate the “keys to the kingdom” problem, and get ahead of your security incidents.

Ronny Stavem | Enterprise Security Specialist

 #DellST14



The connected world
creates massive
opportunity.
And IT needs to
be the enabler.

Enter new markets

Drive efficiency

Create new products

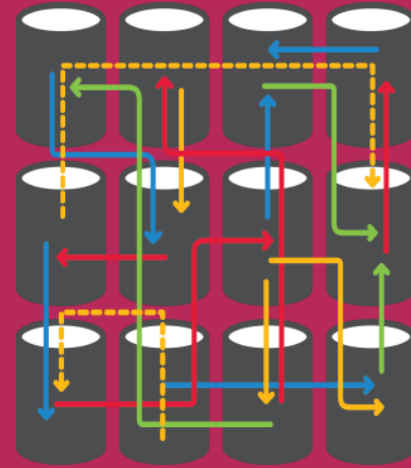
Use new technologies



But current approaches to security are siloed, creating risk and impeding innovation.

Fragmented

Reactive



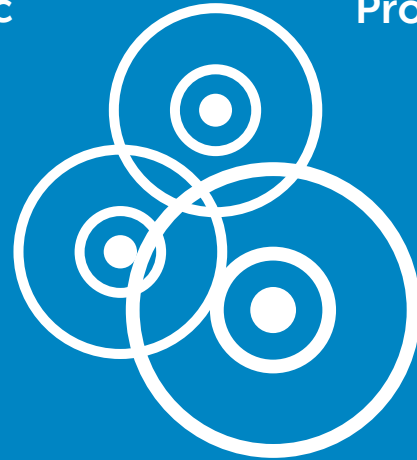
Intrusive



Dell delivers
a better way,
with security
that works together
across your whole
business.

Holistic

Proactive



Transparent



The Dell Security difference

**Connected
end-to-end**

**Closes gaps,
reduces
complexity and
mitigates risk**

Secure your business
from device to
datacenter to cloud

**Shared, context-
aware intelligence**

**Enables proactive
protection
everywhere**

Share real-time
threat information
system-wide

Built for humans

**Makes it easy for
people to do the
right thing**

Stands in the way of
threats, not people and
productivity



The result: better security, better business



Protect

the whole enterprise –
outside in and inside out –
efficiently and proactively



Comply

with regulations and
achieve consistent,
reliable governance



Enable

the enterprise to embrace
new technologies faster
than the competition



Delivering best-in-class security solutions



Network
Next Gen Firewall
Secure Mobile Access
Email Security

Data/Endpoint
Encryption
Protected Workspace
Configuration &
Patch Management
Secure Cloud Client

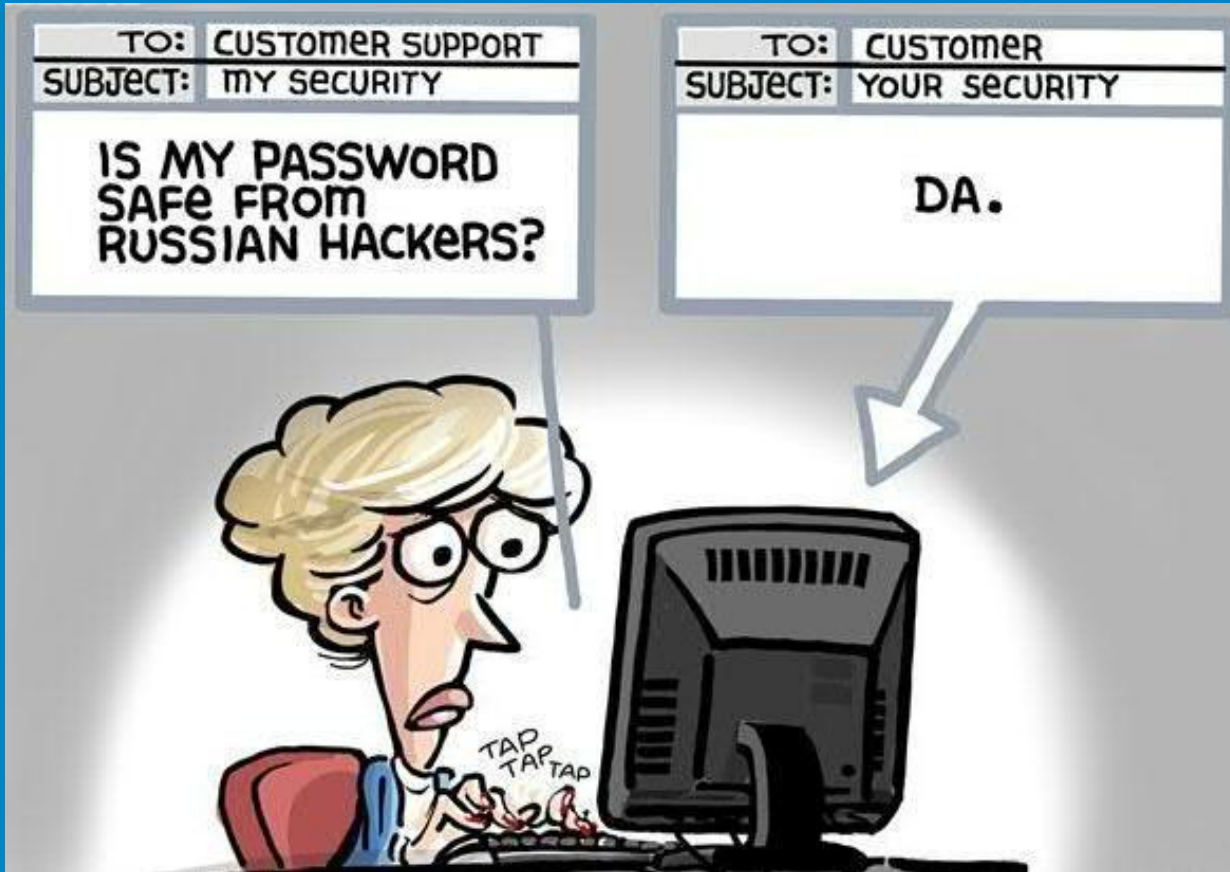


Identity & Access Mgmt
Identity Governance
Privileged Mgmt
Access Mgmt
Compliance & IT Gov

Security Services
Incident Response
Managed Security Svcs
Security & Risk Consult
Threat Intelligence



Who do you trust?



Who in your organisation has access to the Keys to your IT Kingdom?

Administrators

Contractors

Vendors

Service providers

DBAs

Terminated employees

Applications

Developers



Security and risk mitigation



57% of companies have made policy adjustments to mitigate mobile computing risks.

—Ernst & Young



1/2 of sensitive information is actually protected.

—IDC

79% of surveyed companies experienced security incidents within the past year with a financial and/or reputational impact

— McAfee

How do breaches occur?

—Verizon

- 52%** used some form of hacking (-)
- 76%** of network intrusions exploited weak or stolen credentials (-)
- 40%** incorporated malware (-)
- 35%** involved physical attacks (+)
- 29%** leveraged social tactics (+)
- 13%** resulted from privilege misuse and abuse (+)

Cyber incidents **increased by 782%** between 2006 and 2012.

-- US Government Accountability Office

A plus (+) sign indicates either a 10% or greater increase from the previous year's report

A minus(-) sign indicates a 10% or greater decrease from the previous year's report



Risk of unsecured Privileged Identities

- **You do not know** of all logins that exist in your network
- **You have no record** of which credentials are known to who
- **You have no proof** of who has logins to gain access, when and why
- **There is no way to verify** that each password is strong enough, sufficiently unique, and are changed often enough
- **You have no reliable list** of logins stored within your applications, and no way to know which in-house and vendor personell can use these credentials to access sensitive information





Ever wondered what it would be like to have a



The iPhone 6 WILL launch two weeks



Husbands who tell their wives they're



Boris Johnson applies to become

Personal data belonging to 4.5MILLION American hospital patients stolen in cyber attack by Chinese

TOP STORES IN BUSINESS

1 of 12



Buffett Enters Tax Fray With Burger Kin...



How Steve Ballmer Became a Basketball M...

2 of 12

U.S. Judge Overturns GMO Crop Curbs in ...

Target Now Says 70 Million People Hit in Data Breach

Neiman Marcus Also Says Its Cu...

Email Print 72 Comments

NOK6 A WEEK FOR

By PAUL ZIOBRO And DANNY YADRON

Updated Jan 10, 2014 8:36 p.m. ET

ComputerSweden



Åsa Schwarz: "Datalagring - inte dum"

KATEGORIER ▾ PODCAST TV EVENT BLOGGAR NYHETSREBREV CS JOBB IT24 SÄKERHET

Så kan hackare skapa trafik kaos

Publicerad 2014-09-08 09:39



Av Martin Wallström

Dragonfly: Western Energy Companies Under Sabotage Threat

Created: 30 Jun 2014 12:58:04 GMT • Updated: 30 Jun 2014 19:04:46 GMT • Translations available: Français, Deutsch, Italiano, 日本語, 韓

TRENDING: Emerging Tech • Android • What matters in the fall smartphone lineup • Reviews • Resources/White Papers

COMPUTERWORLD

Popular Now: ▾

Twitter LinkedIn Facebook Google+ RSS

Home > Security > Cybercrime & Hacking

NEWS

Target breach happened because of a basic network segmentation

Hackers gained access to credentials belonging to

26-åring stjal lønningene til 55 sykehus-topper



By Jaikumar Vijayar Computerworld | Feb

En IT-konsulent (26) er tiltalt for å ha overført lønningene til 55 ledere i Helse Sør-Øst til kontoer han selv disponerte.

The resu

seg/DELE FACEBOOK TWITTER LINKEDIN MAIL

E24 07:33 - 22.04.2014

Lørdag 30. august

ca. 32 mill.

Blir det 1 vinner?

LOTTO

50 bedrifter i oljebransjen er bekreftet angrepet i tidenes hackerangrep mot Norge

- Evnen til angrep er økende.



Why does it happen?

Today's management practice with Privileged users is a high risk activity.

"We have an IAM system but privileged management is the forgotten arm."

- Shared account and passwords usage
- Excessive privilege/No granularity
- Hidden/Sleeping accounts
- No revocation of access
- Unenforced access controls
- No monitoring and auditing
- Infrequent replacement of credentials

Know your Jedi's

**Control and
monitor their
forces!**





The power to do more

Privileged Management

The Privileged Appliance and Modules **TPAM**

- **Privileged Password Manager (PPM)**

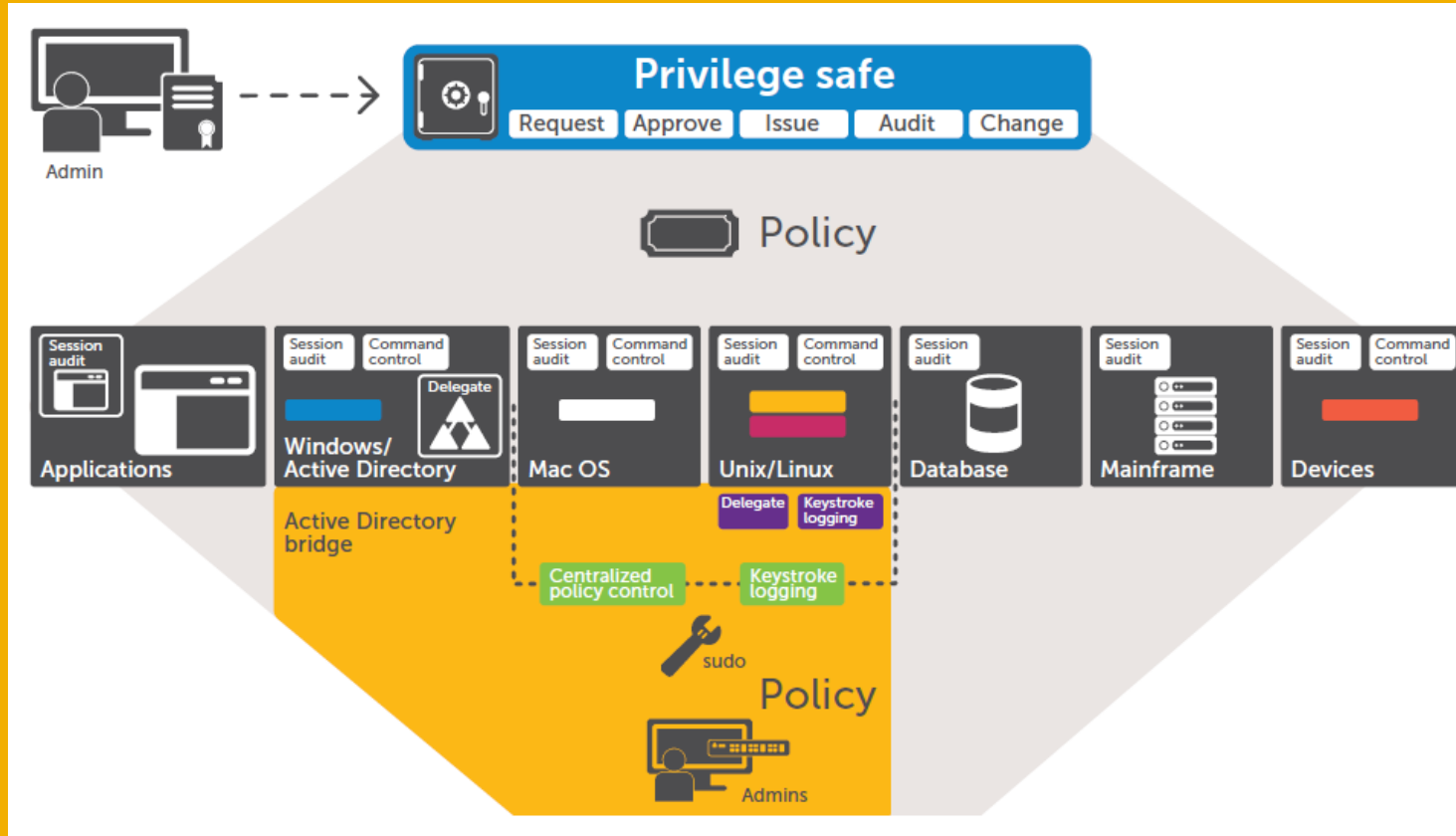
Enables secure storage, release control and change control of privileged passwords across a heterogeneous deployment of systems and applications, including passwords that are hardcoded in scripts, procedures and programs.

- **Privileged Session Manager (PSM)**

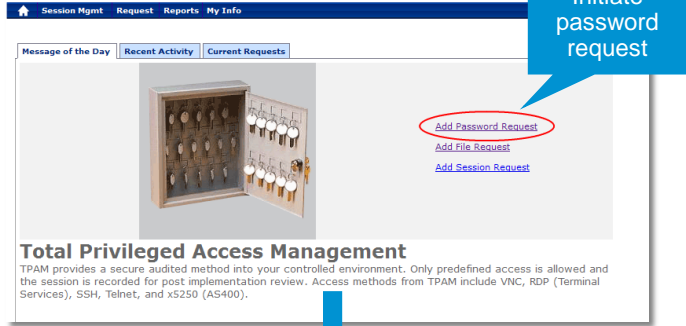
Enables you to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users, with full recording and replay for auditing and compliance.



Dell Privileged management - The solution



Workflow – password request



Initiate password request

[Add Password Request](#)

[Add File Request](#)

[Add Session Request](#)

Total Privileged Access Management

TPAM provides a secure audited method into your controlled environment. Only predefined access is allowed and the session is recorded for post implementation review. Access methods from TPAM include VNC, RDP (Terminal Services), SSH, Telnet, and xS250 (AS400).

Password Request Management

Select accounts then click Details tab.

Filter & select account(s)

Selected	System Name	Account Name	Access Policy
<input type="checkbox"/>	Jupiter	Barney	Requestor
<input checked="" type="checkbox"/>	Jupiter	funcacct	Requestor
<input checked="" type="checkbox"/>	Jupiter	test123	Requestor

Enter date/time/duration/reason password is needed

Optional ticket field. Can be active (check ticket) or passive

Password Request Management
Specify details and save changes.

Request Immediate: Date/Time Required: (MM/DD/YYYY) 8 / 2 / 2011 09 : 00 AM

Requested Duration: 0 Days 2 Hours 0 Minutes

Reason Code: Test

Request Reason: Need to perform testing

Remaining: 977

Ticket System: MyCompanyTicketSystem Ticket Number: 2356892

Sel.	System Name Account Name	Status	Access Policy Max Duration	Locked? Last Released	Ticket System Ticket #
<input checked="" type="checkbox"/>	Jupiter funcacct	Approval Required	Requestor 7d:0h:0m	No n/a	MyCompanyTi 2356892

Retrieve password

Password Request Management
RequestID: 157 Account: test123 System: Jupiter

g3463drvsryhswy

Font Used for Password Display: COURIER
Zero = 0, One = 1, Uppercase i = I, Lowercase l = L, Uppercase o = O
This window will close in 19 seconds



Workflow – session request

Message of the Day | Recent Activity | Current Requests

[Add Password Request](#)
[Add File Request](#)
[Add Session Request](#)

Total Privileged Access Management

TPAM provides a secure audited method into your controlled environment. Only predefined access is allowed and the session is recorded for post implementation review. Access methods from TPAM include VNC, RDP (Terminal Services), SSH, Telnet, and x5250 (AS400).

Session Request Management

Specify details and save changes.

Request Immediate | Date/Time Required: (MM/DD/YYYY) 8 / 2 / 2011
Requested Duration: 0 Days 2 Hours 0 Minutes
Reason Code: Select a Reason Code
Request Reason: * Need access to check performance issues.
Remaining: 960

Ticket System: * MyCompanyTicketSystem | Ticket Number: * 88888888888

Select Accounts

Sel.	System Name Account Name	Status Max Duration	Access Policy Command	Locked? Last Released	Ticket System
<input checked="" type="checkbox"/>	Jupiter funcacct	Approval Required 7d:0h:0m	Requestor n/a	No 7/18/2011 7:03 PM	MyCompanyTicketSystem 88888888888

Session Request Management

Select accounts then click Details tab.

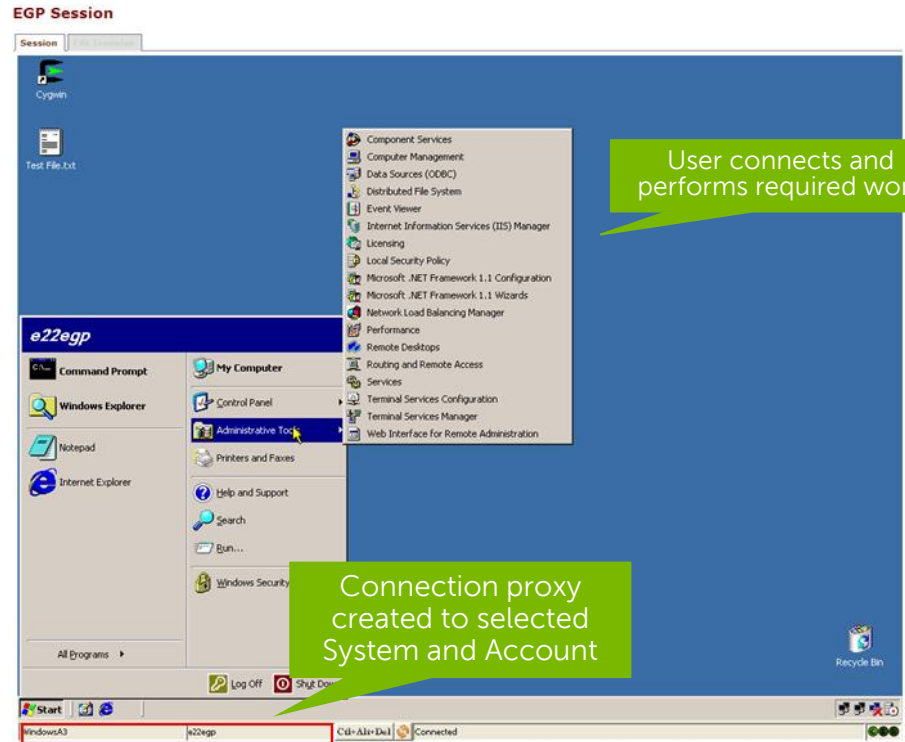
Selected	System Name	Account Name	Command Name	Access Policy	Min Ap
<input type="checkbox"/>	Jupiter	Barney		Requestor	0
<input checked="" type="checkbox"/>	Jupiter	funcacct		Requestor	1
<input checked="" type="checkbox"/>	Jupiter	test123		Requestor	0

Save Changes | New Request | Export to Excel | Export to CSV | New Accounts | **Connect** | 024x768

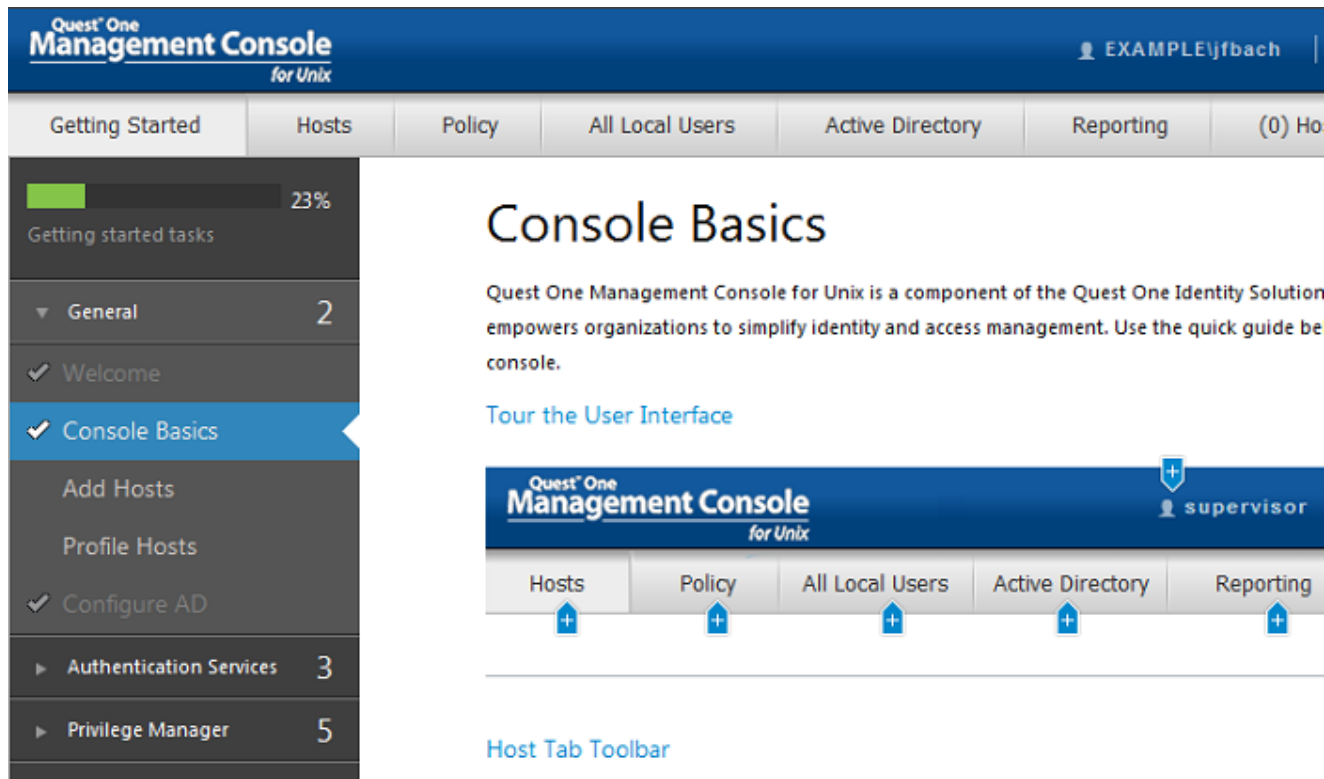


Workflow – session request

- A session can be configured for interactive or auto-login
- Every action on the target system will be recorded
- If a session extends beyond the requested time, configurable alert notifications of session overrun can be sent
- Active sessions can be manually terminated by authorized administrators



Intuitive administration



The image shows the Quest One Management Console for Unix interface. At the top, there is a dark blue header with the logo and the text "Quest One Management Console for Unix". On the right side of the header, there is a user profile icon and the name "EXAMPLE\jfbach". Below the header is a horizontal navigation bar with several tabs: "Getting Started", "Hosts", "Policy", "All Local Users", "Active Directory", "Reporting", and "(0) Ho".

On the left side, there is a sidebar menu. At the top of the sidebar, there is a progress bar labeled "Getting started tasks" with a value of "23%". Below this, there are several menu items with expandable arrows and counts:

- General 2
- Welcome
- Console Basics (highlighted)
- Add Hosts
- Profile Hosts
- Configure AD
- Authentication Services 3
- Privilege Manager 5

The main content area is titled "Console Basics" and contains the following text:

Quest One Management Console for Unix is a component of the Quest One Identity Solution empowers organizations to simplify identity and access management. Use the quick guide be console.

[Tour the User Interface](#)

Below the text, there is a smaller screenshot of the console interface. This screenshot shows the same navigation bar as the main image, but with a user profile icon and the name "supervisor" on the right. Below the navigation bar, there are five tabs: "Hosts", "Policy", "All Local Users", "Active Directory", and "Reporting". Each tab has a small blue plus sign icon below it.

[Host Tab Toolbar](#)



Key drivers for Privileged Account and Session Management

Insider threats

Risk and compliance

Moving to the cloud

Targeted Cyber attacks



Summary: What measures to take

Minimize the number of logins with privileged access. Reduces **RISKS**.

Monitor the privileged users and **Log all changes**.

Enforce use of complex passwords; that nobody knows.

Implement check in/check out routines for extracting passwords.

No sharing of privileged accounts. Assign individual **accountability**.

Monitor the activities of privileged users. Enforce **least privileges**.



The power to do more

