

# Novell<sup>®</sup>

# Privileged User Manager

**Ziemowit Buczyński**

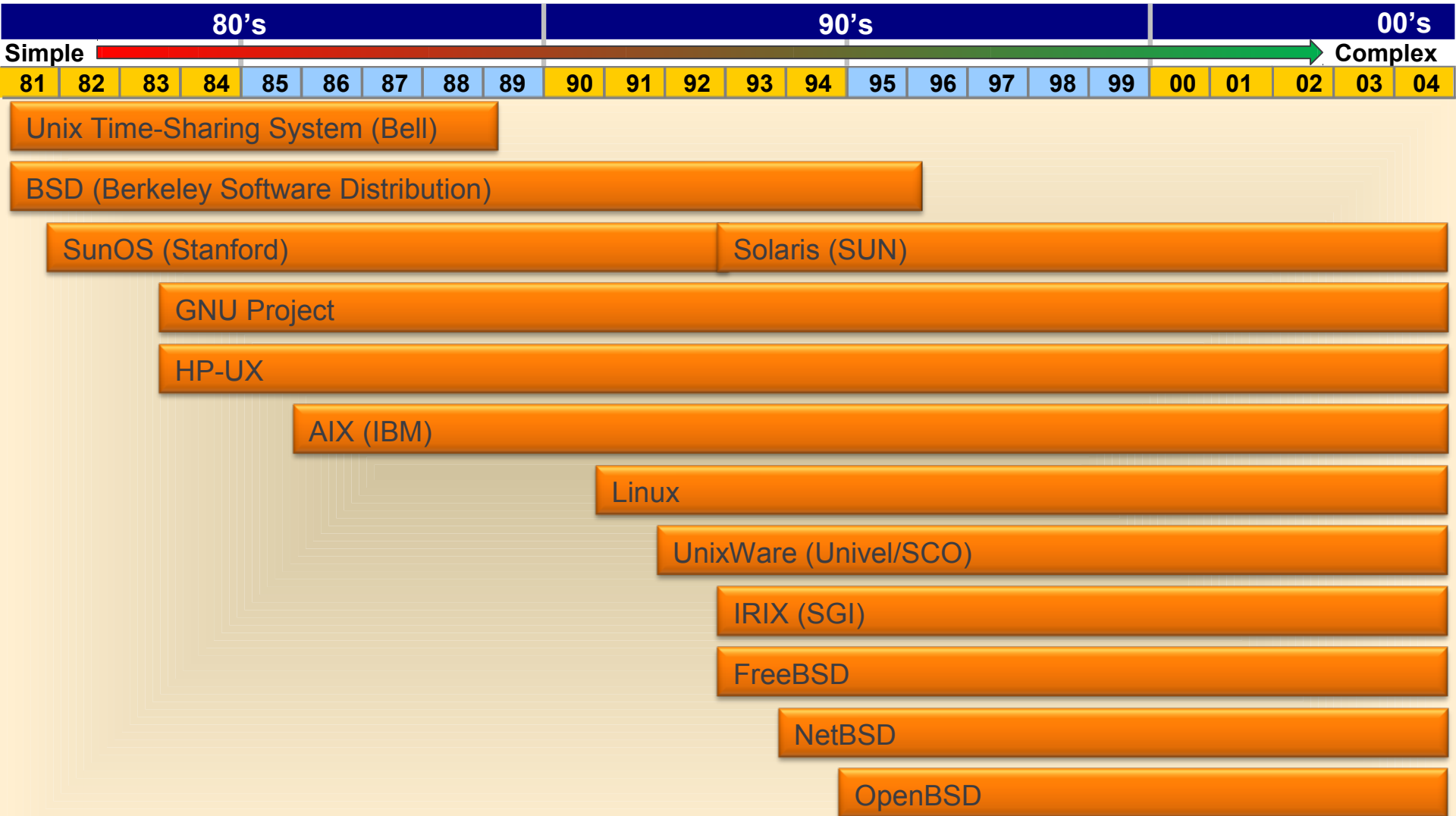
Solution Architect

[zbuczynski@novell.pl](mailto:zbuczynski@novell.pl)

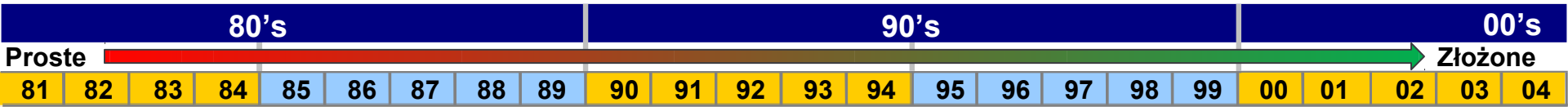
**Novell<sup>®</sup>**

Krótkie spojrzenie na łoś

# Wzrost liczby systemów UNIX/Linux



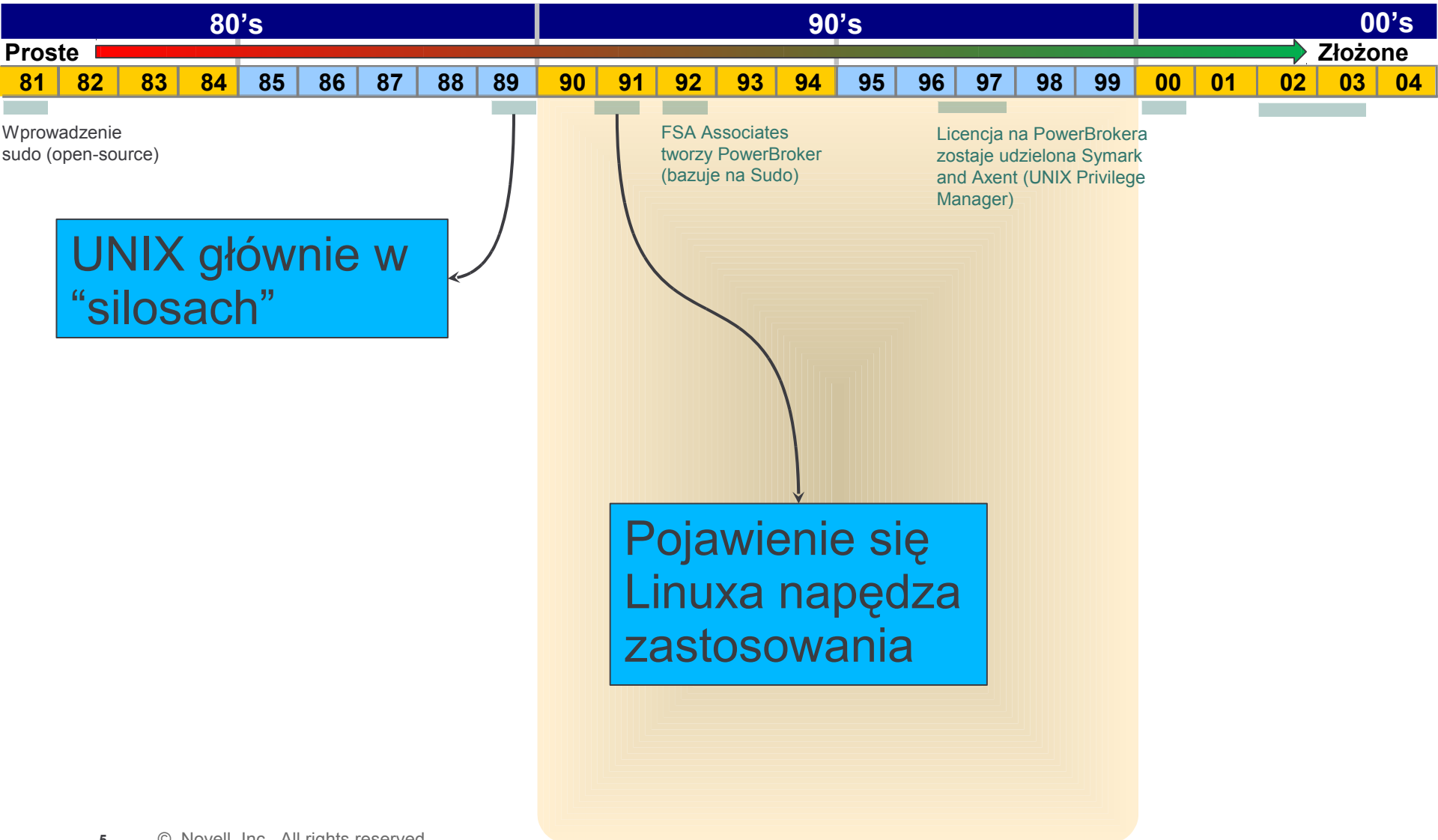
# Bezpieczeństwo w latach 80-tych



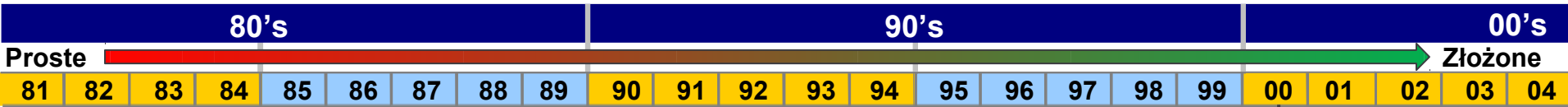
Wprowadzenie  
sudo (open-source)

Zaczął narastać  
problem

# Wzrost ilości systemów Linux



# Potrzeba zgodności z regulacjami



Wprowadzenie  
sudo (open-source)

FSA Associates  
tworzy PowerBroker  
(bazuje na Sudo)

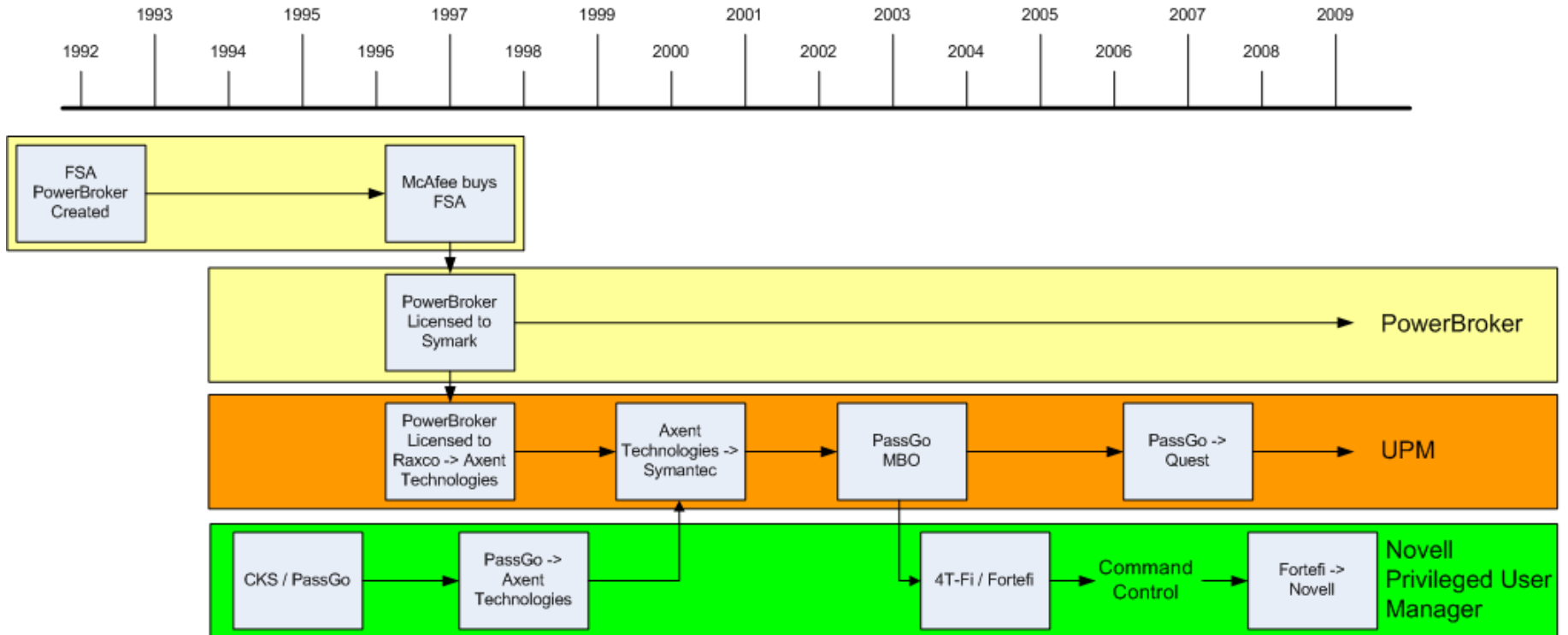
Licencja na PowerBrokera  
zostaje udzielona Symark  
and Axent (UNIX Privilege  
Manager)

Przejęcia powodują pojawianie się olbrzymiej liczby różnych systemów w firmach

9/11, Enron – wymagane podniesienie poziomu bezpieczeństwa. Regulacje: SOX, Gramm-Leach-Bliley...

\*\*Firmy chcąc szybko poprawić sytuację wybierają to co jest dostępne\*\*

# Skąd się wzięliśmy w tej grze?



Więc dziś jest już lepiej, tak?

# Rosnąca ilość naruszeń bezpieczeństwa

“Urząd Skarbowy Wielkiej Brytani potwierdził, że zapłacił 'informatorowi' za dane o kontaktach swoich obywateli w Liechtensteinie.”

- Rząd Niemiec zapłacił za podobne dane ponad 6 mln dolarów.

- *InfoWorld, 21-07-2008*

## **Naruszenia bezpieczeństwa**

- \* 80% - przypadek
- \* 20% - złośliwość

Kiedy przychodzi do rozwiązania problemu to i tak nie ma znaczenia – trzeba naprawić i upewnić się, że już się nie powtórzy

“...Terry Childs, administrator sieci WAN zatrudniony przez City of San Francisco, został aresztowany i skazany za czterokrotne manipulowanie danymi.”

- *The Examiner, 9-12-2010*

## **Średni koszt**

\$50k – external breach  
\$2.7m – internal breach

**70% naruszeń bezpieczeństwa  
pochodzi z wewnątrz!**

**Dlaczego ludzie powinni się obawiać?**

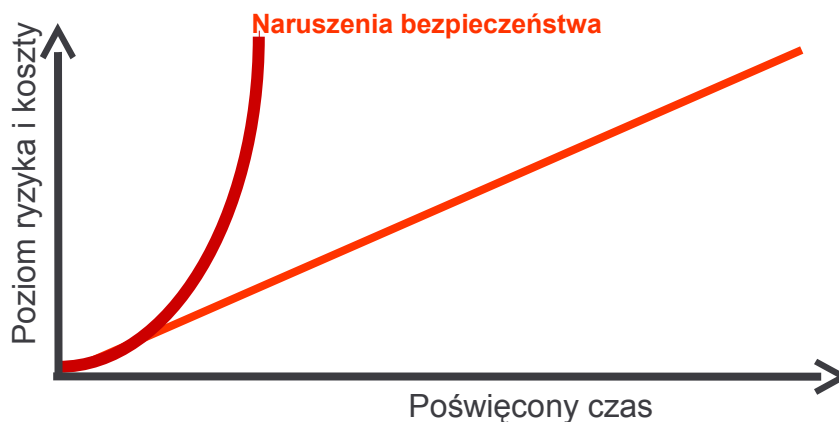


**Bezpieczeństwo reaktywne**

**A gdzie jest proaktywne?**

# Bezpieczeństwo – *potrzeba dowodów*

- Wyzwanie
  - Zbyt wiele zebranych danych może być trudne w zarządzaniu (przykład: TJX)
  - Zbyt mało zebranych danych może zostawić luki dowodowe
- Skracanie analizy dowodowej staje się krytyczne
  - Czas poświęcony na analizy = \$millions



# Bezpieczeństwo – *potrzeba należytej staranności*



- Co to jest?
  - Proaktywne sprawdzanie działalności użytkowników
- Kto to robi?
  - Przełożeni i wewnętrzni audytorzy
- Co oni robią?
  - Podpisują się pod działaniami swoich podwładnych
- Jak to pomaga?
  - Zgodność z regulacjami może być dowiedziona przed audytorami zewnętrznymi
  - Zmniejszanie ryzyka i zapobieganie naruszeniom
  - Spokój ducha...

# Trzy kroki do podniesienia bezpieczeństwa systemów UNIX/Linux

## Krok 1

- 100% zapisywanych akcji
  - Automatyczne porządkowanie ryzyk
- 

## Krok 2

- Zarządzanie uprawnieniami “superuserów”
  - Kontrola i alarmy w czasie rzeczywistym
- 

## Krok 3

- Proaktywne zarządzanie zgodnością
- Audytowanie audytora



# Kontrola zgodności z regulacjami

**Symark PowerBroker Auditing**

**Novell Auditing**

**Wbudowany mechanizm analizy ryzyka** – każde zdarzenie jest oznakowane kolorem na podstawie polecenia uznanego jako najbardziej ryzykowne od **zielonego** (niskie ryzyko) to **czerwonego** (wysokie ryzyko)..

# A ty jak byś wolał **administrować**?

```

1  #! /bin/ksh
2  PATH=/usr/bin:/usr/local/bin:.
3  export PATH
4  if (( $# < 2 )); then
5      print -u2 "Usage: $0 client command";
6      exit 1
7  else
8      typeset MYACCOUNT=$1;
9      typeset -x LOGNAME=$1;
10     typeset ARGV=$2;
11  fi
12
13  if [ "X$MYACCOUNT" = "Xcidgen" ]; then
14     typeset HOME_DIR="/filedir/re
15  else
16     typeset -l -R2 CLNT=$MYACCOUNT
17     typeset HOME_DIR="/filedir/re
18  fi
19
20  if [ ! -d $HOME_DIR ]; then
21     print -u2 "Error: cannot acc
22     exit 1;
23  elif [ ! -f "$HOME_DIR/.profile" ]; then
24     print -u2 "Error: cannot acc
25     exit 2;
26  fi
27
28  HOME=$HOME_DIR
29  export HOME
30  cd $HOME
31  . ./profile;
32  jj=$(date "+%C%y%m%d.%H%M%S")
33  jt=$EBSLOGS/sj.$ARGV.$jj
34  ksh -vx ujes $ARGV >> $jt 2>&1
35

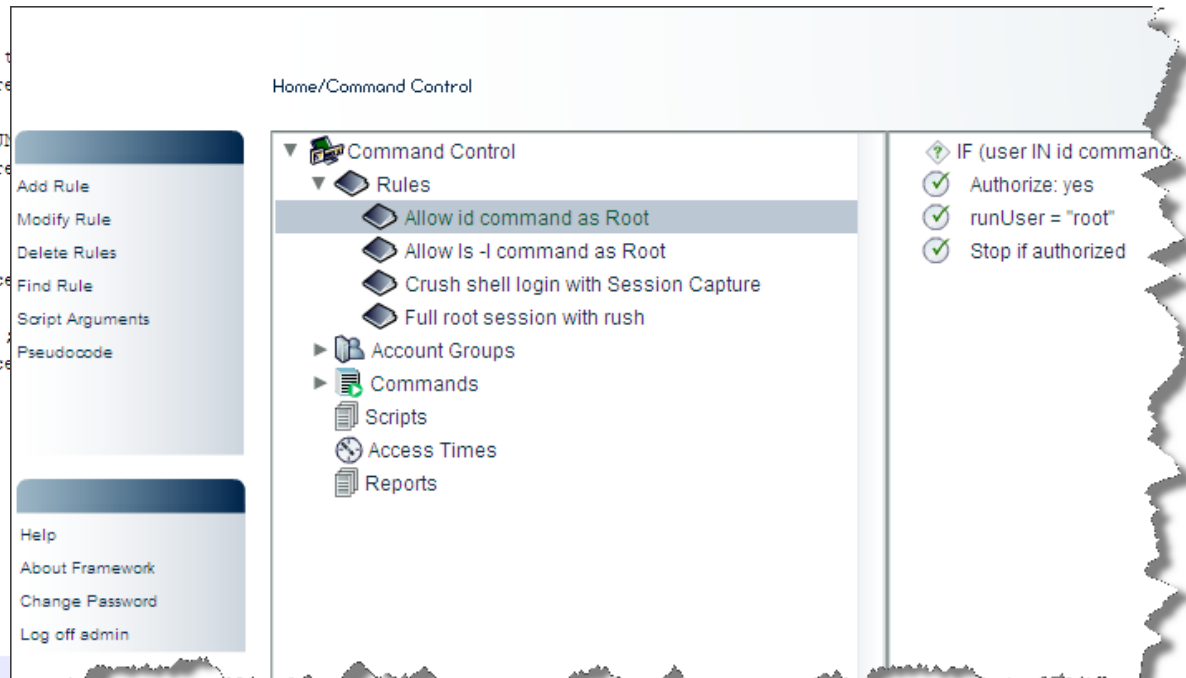
```



Symark PowerBroker / Quest UPM / Sudo

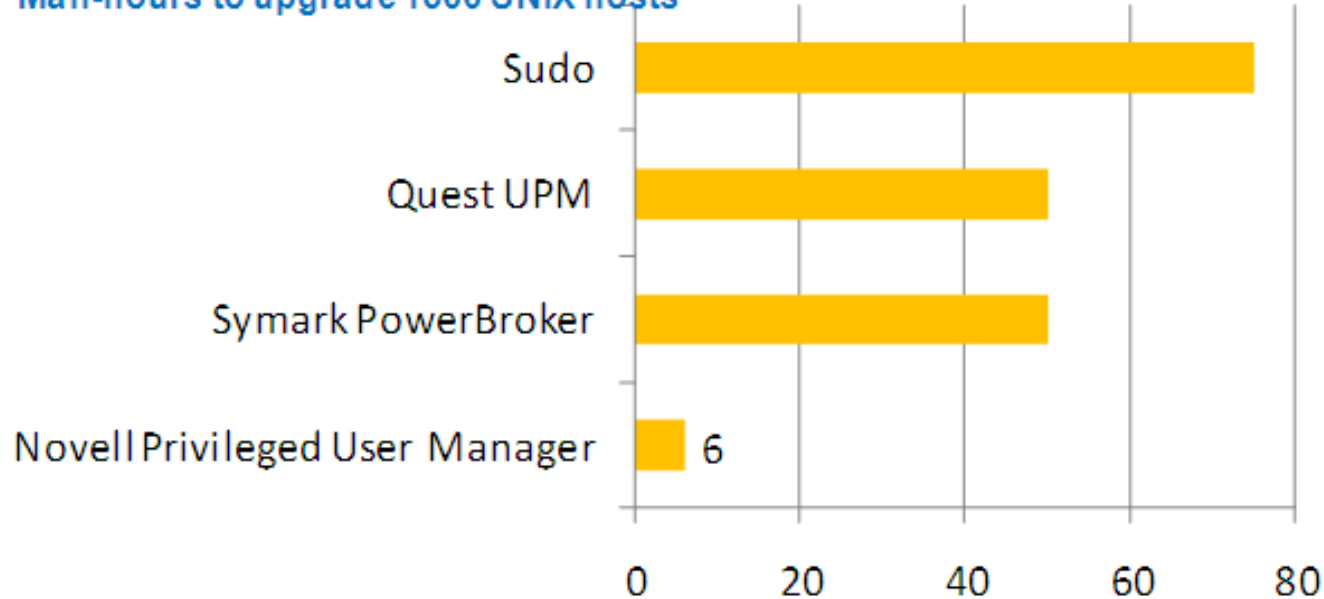


Novell® Privileged User Manager



# Dlaczego łatwość zarządzania jest czynnikiem krytycznym?

Man-hours to upgrade 1500 UNIX hosts



**Łatwość zarządzania** jest czynnikiem krytycznym np. w momencie planowania uaktualnień lub zmian organizacyjnych.

Novell® Privileged User Manager pozwala firmom **szybciej reagować** na wciąż zmieniające się: wymagania regulatorów i zasady bezpieczeństwa firmy.

# Dlaczego Privileged User Management jest taki ważny?

## Bezpieczeństwo

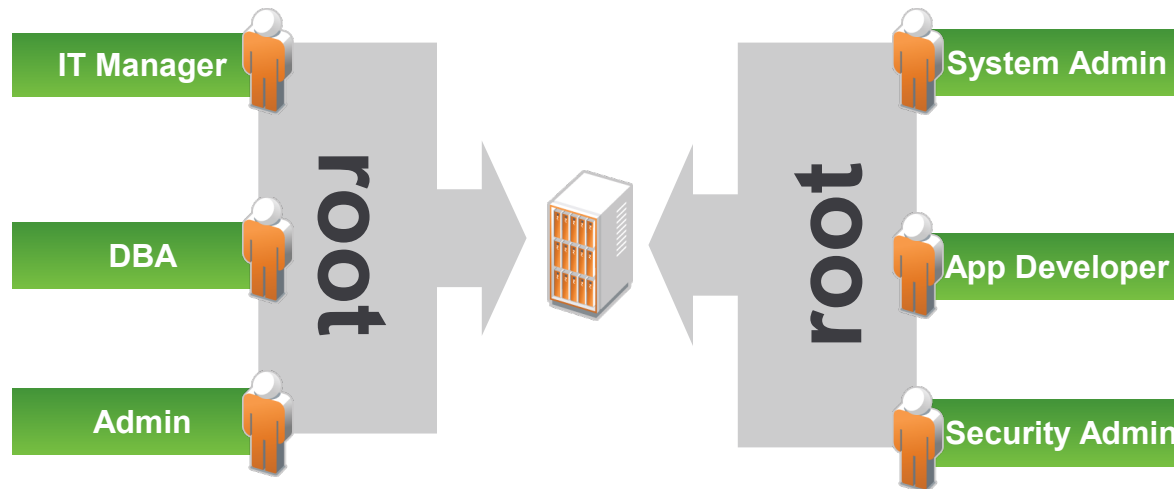
- Systemy UNIX i Linux pracują jako szkielet wielu krytycznych usług
- Wielu użytkowników (IT admins, application developers, DBAs) może mieć *pełne* przywileje “superusera”
- Większość użytkowników potrzebuje tylko ograniczonego dostępu
- Organizacje nie mają odpowiedniej kontroli nad dostępem do kont root, co prowadzi do zwiększenia ryzyka, nadużyć i upomnień ze strony audytorów/regulatorów.

## Koszty

- Kary i straty związane z naruszeniami bezpieczeństwa
- Uszczerbek w reputacji firmy
- Erozja zaufania klientów

# Delegowanie uprawnień Superusera

- Administratorzy systemów Linux/UNIX potrzebują wyższych uprawnień aby wykonywać swoją pracę



**Novell® Privileged User Manager**  
może ich dostarczyć

# Novell Privileged User Manager



- Kontroluje dostęp do kont uprzywilejowanych
- Audyt wszystkich działań użytkowników ze 100% logowaniem naciskanych klawiszy
- Analiza potencjalnych zagrożeń na podstawie polityk opisujących poziomy ryzyka
- Upraszcza raportowanie audytowe przy pomocy odpowiednich, kontekstowych informacji
- Wspiera zgodność z politykami wewnętrznymi i zewnętrznymi regulacjami

Klienci

# Klienci używający Novell® Privileged User Manager to m.in.:



# Przykłady wdrożeń

- Barclays

- Olbrzymie środowisko, >4500 serwerów UNIX na świecie
  - Migracja z PassGo/Quest UPM
  - Okna serwisowe zostały zredukowane do 12% początkowych
- 

- ING

- Migracja z Symark PowerBroker
- Uznany za wystarczająco ważny, aby być jedynym zakupem w 2008
- Spełnia wszystkie nowe wymagania audytowe
- Czas audytu pojedynczej sesji zredukowany z 45 minut do mniej niż 5 min

# Obserwacje Klientów

- Spełnia wszystkie wymagania SOX
- Zamiast przeprowadzać walidację co sześć sekund robi ją **sześć razy na sekundę**
- Można migrować do Novell® Privileged User Manager stopniowo (może współistnieć z innymi rozwiązaniami)
- Bardzo małe obciążenie serwerów
- Znakomite szyfrowanie

# Co czyni Novell® Privileged User Managera tak odmiennym?

- Skalowalność (obsługuje tysiące hostów per framework)
- Uprzedzające działania w celu utrzymania zgodności (zachowanie należytej staranności)
  - Analiza ryzyka znakowana kolorami wskazuje zagrożenia
- Szybka analiza dowodowa (wyszukiwanie działań użytkownika, zarządzanie logami)
- Graficzna administracja
  - mniej administracji + szybszy audyt = ROI
- Łatwe wdrożenie (szybkie, zarządzane centralnie, nieinwazyjne)
- Technologia (napisane od podstaw z myślą o szybkości i bezpieczeństwie)
- Ciągłość pracy (auto failover nawet w czasie uaktualniania produktu)

# PUM 2.3 w Twojej organizacji

## Ceny, licencjonowanie

- Zadzwoń na infolinię **800 22 66 85**
  - *od poniedziałku do piątku w godz. 8:00-16:00*
- Skorzystaj z formularza
  - [www.novell.pl/formularz.html](http://www.novell.pl/formularz.html)
- Strona produktu, demo, kalkulator ROI
  - [www.novell.com/products/privilegedusermanager](http://www.novell.com/products/privilegedusermanager)
- Nośniki: testuj bezpłatnie przez 90 dni
  - Novell-PUM-2.3.0.iso 527.5 MB
  - [http://download.novell.com/Download?buildid=kzJo-ud\\_jAI](http://download.novell.com/Download?buildid=kzJo-ud_jAI)

Pokaz

Pytania?

**Novell®**

## **Unpublished Work of Novell, Inc. All Rights Reserved.**

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

## **General Disclaimer**

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

