

ZENworks Endpoint Security Management 11

Jacek Nienaltowski

Konsultant

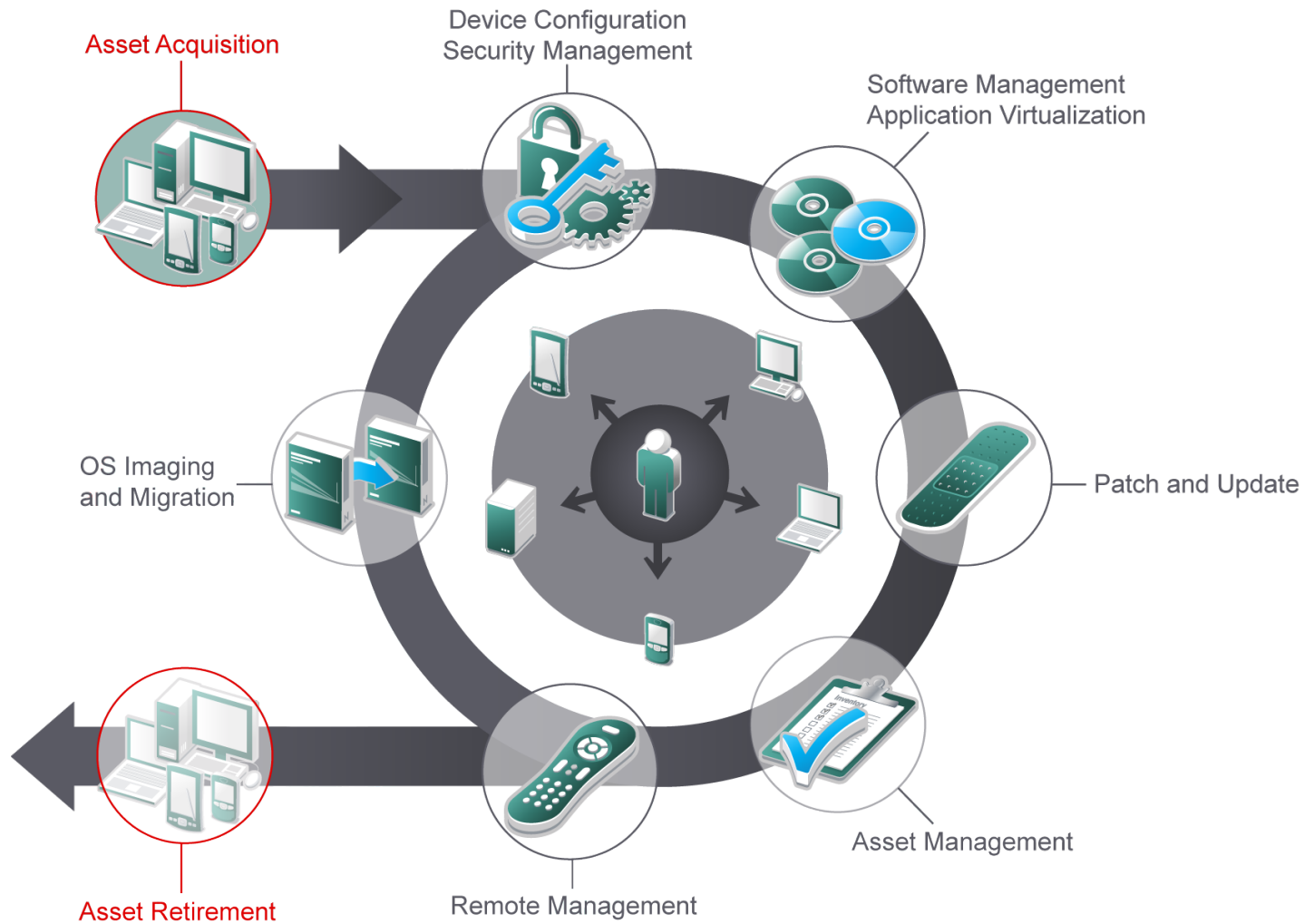
Novell Sp. z o.o.

jnienaltowski@novell.pl

Novell®

**Rodzina produktów firmy Novell
do zarządzania zasobami IT
(System & Resource Management)**

Cykl „życia” urządzenia w organizacji



Rodzina produktów System & Resource Management

- ZENworks Configuration Management 11
- **ZENworks Endpoint Security Management 11**
- ZENworks Asset Management 11
- ZENworks Patch Management 11
- ZENworks Application Virtualization 8
- Novell Service Desk 6.2

ZENworks 11
wspólna platforma



Pełna integracja produktów

- **Jedna konsola webowa** do zarządzania wszystkim produktami – ZENworks Control Center
- Tylko **jeden modularny agent** instalowany na zarządzanym urządzeniu, obsługujący wszystkie funkcjonalności
- **Wspólna modularna infrastruktura** serwerowa obsługujące wszystkie funkcjonalności
- **Integracja** z eDirectory/Active Directory

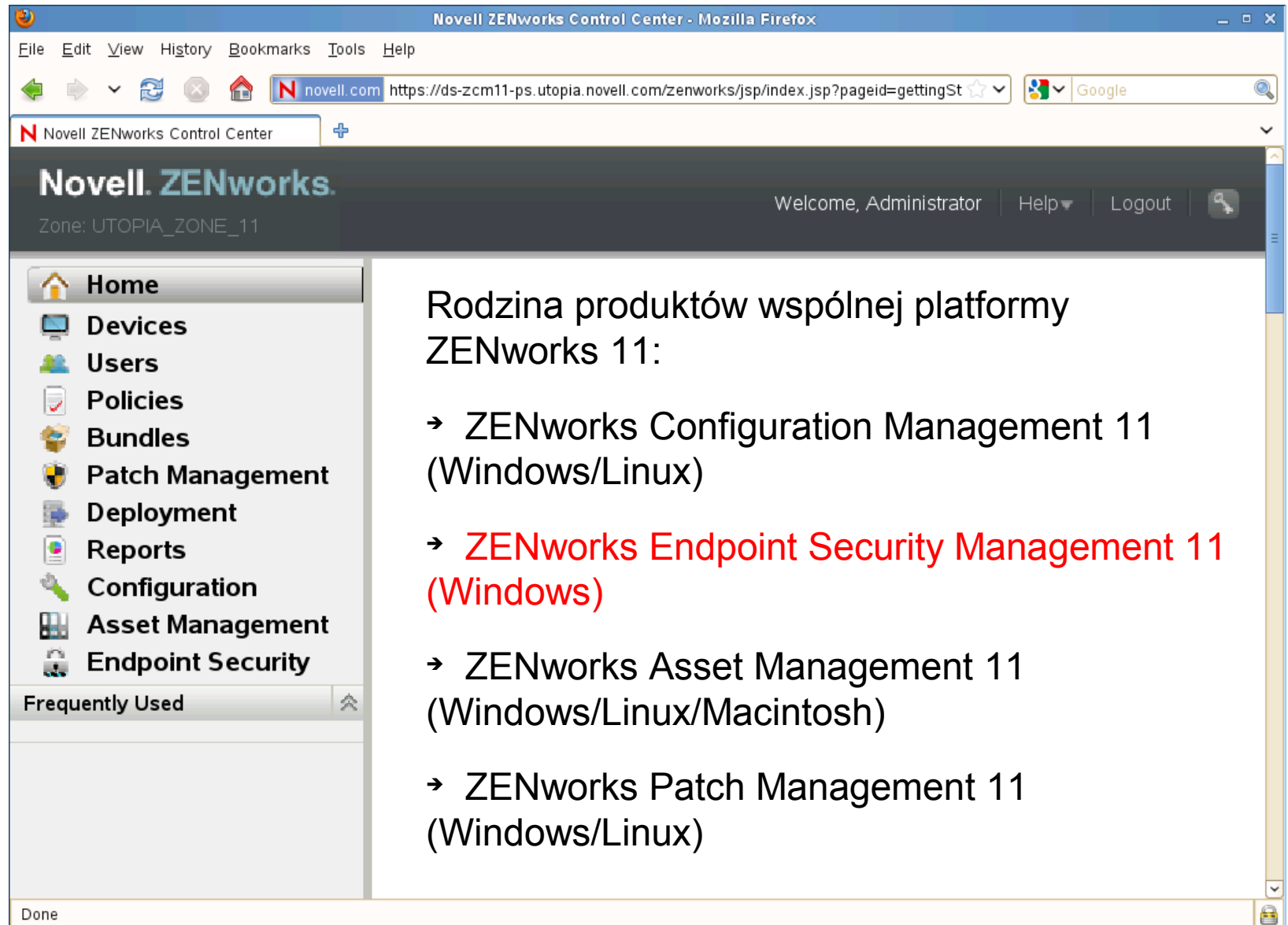


Pełna integracja produktów cd.

- **Wspólna baza danych** przechowująca konfigurację i dane pochodzące z oraz dotyczące wszystkich produktów
- Dwa **systemy raportowania** obsługujące wszystkie funkcjonalności – uproszczony w ZENworks Control Center oraz rozbudowany ZENworks Reporting Server
- **Łatwe wdrożenie** dodatkowej funkcjonalności poprzez jedynie aktywację kolejnego produktu!



Wspólna konsola – ZENworks Control Center



Novell ZENworks Control Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

novell.com https://ds-zcm11-ps.utopia.novell.com/zenworks/jsp/index.jsp?pageid=gettingSt

Novell ZENworks Control Center

Novell. ZENworks.

Zone: UTOPIA_ZONE_11

Welcome, Administrator Help Logout

- Home
- Devices
- Users
- Policies
- Bundles
- Patch Management
- Deployment
- Reports
- Configuration
- Asset Management
- Endpoint Security

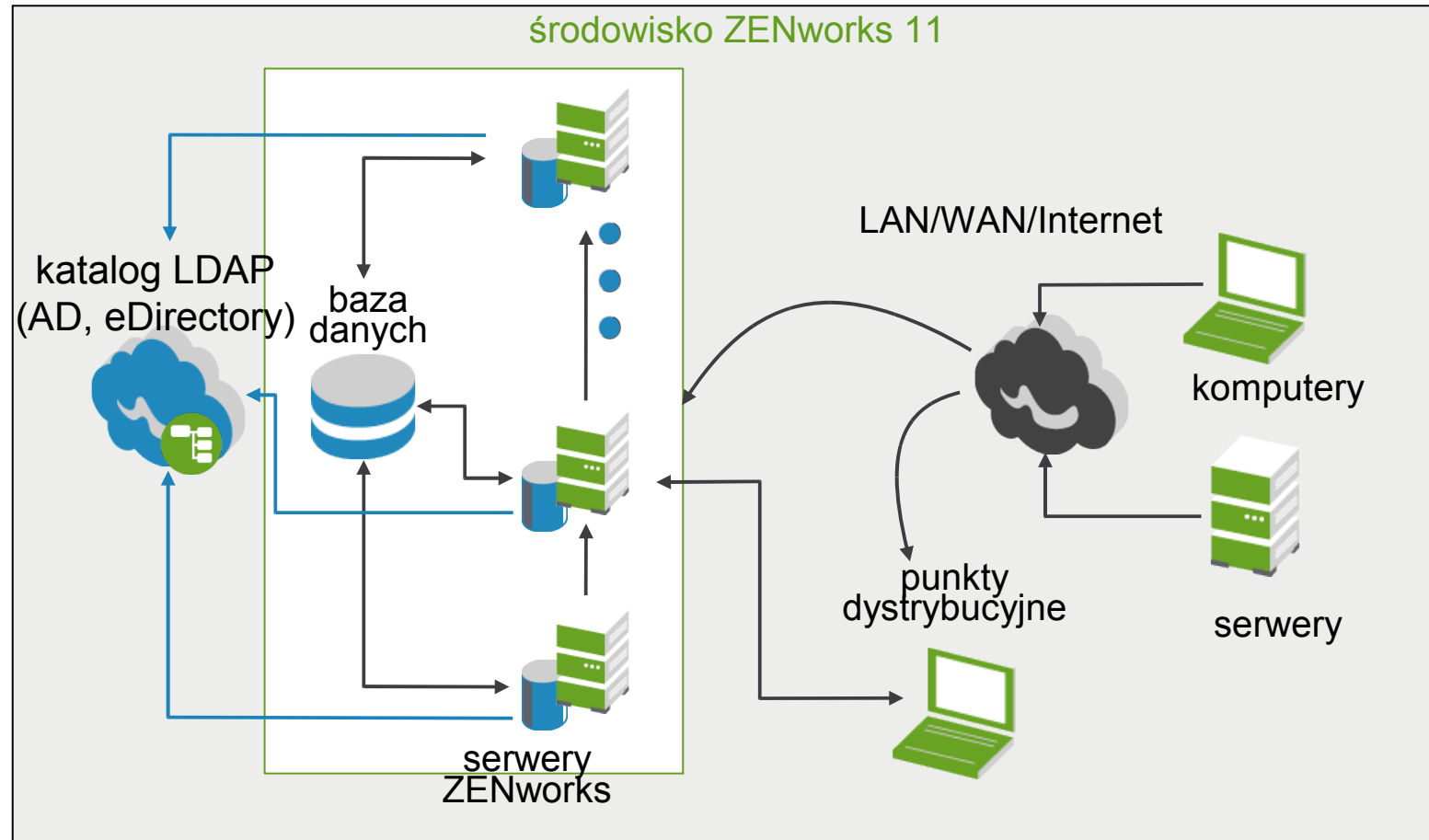
Frequently Used

Done

Rodzina produktów wspólnej platformy ZENworks 11:

- ZENworks Configuration Management 11 (Windows/Linux)
- **ZENworks Endpoint Security Management 11 (Windows)**
- ZENworks Asset Management 11 (Windows/Linux/Macintosh)
- ZENworks Patch Management 11 (Windows/Linux)

Architektura systemu ZENworks 11



Platformy systemowe serwerów ZENworks 11

- Systemy operacyjne serwerów ZENworks 11:
 - Linux
 - > SUSE Linux Enterprise Server 10 SP3 x86/x86-64
 - > SUSE Linux Enterprise Server 11 SP1 x86/x86-64
 - > Novell Open Enterprise Server 2 SP2/SP3 x86/x86-64
 - > Red Hat Enterprise Linux 5.0, 5.3, 5.4, 5.5 x86/x86-64
 - Windows
 - > Windows 2003 Server Standard/Enterprise SP2 x86/x86-64
 - > Windows 2008 Server Standard/Enterprise SP1/SP2 x86/x86-64
 - > Windows 2008 R2 Server Standard/Enterprise x86-64
 - VMware ESX/ESXi 3.5u4, 4 i 4.1 (ZENworks 11 Appliance – **nie wymaga licencji na system operacyjny!**)

Platformy systemowe serwerów ZENworks 11

- Bazy danych:
 - Sybase SQL Anywhere 10.0.1 (**darmowa licencja OEM dostarczana wraz z produktami ZENworks 11!**)
 - Oracle 10g Standard Release 2
 - MS SQL Server 2005 Standard/Enterprise
 - MS SQL Server 2008 (tryb kompatybilności 2005)

Platformy agentów ZENworks 11

- Systemy operacyjne dla agentów ZENworks 11:
 - Systemy serwerowe Windows
 - > Windows 2003 Server Standard/Enterprise SP2 x86/x86-64
 - > Windows 2008 Server Standard/Enterprise SP1/SP2 x86/x86-64
 - > Windows 2008 R2 Server Standard/Enterprise x86-64
 - **Systemy desktopowe Windows**
 - > **Windows XP Professional, Embedded, Tablet SP2/SP3 x86**
 - > **Windows Vista SP1 Business, Enterprise, Ultimate x86/x86-64**
 - > **Windows 7 Professional, Enterprise, Ultimate x86/x86-64**
 - Systemy terminalowe
 - > Windows Server: 2003 SP2, 2008 SP2, 2008 R2
 - > Citrix: XenApp Metaframe XP, XenApp 5.0, XenApp 6.0

ZENworks Endpoint Security Management 11

Ochrona punktów końcowych

Twój dział IT też ma z tym problem?



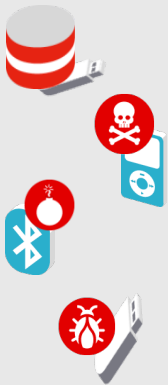
- Większość ważnych danych znajduje się na urządzeniach użytkowników, dlatego należy dbać o ich właściwą **konfigurację i bezpieczeństwo**



- Coraz więcej urządzeń jest **mobilnych** i nie zawsze dobrze chronionych. Mają jednak kontakt z firmową siecią i mogą przenosić zagrożenia



- Sieci bezprzewodowe są powszechnie stosowane, są też **łatwe do złamania i podatne na ataki**



- Urządzenia użytkowników potrafią zmieścić olbrzymie ilości danych
- Pojawiają się nowe zagrożenia jak iPod slurping, Thumbsucking (kradzież danych), snarfing (atak przez WiFi lub Bluetooth)

Bezpieczeństwo punktów końcowych

- **Co to jest?**

- Wymuszanie stosowania reguł zdefiniowanych przez organizację w celu ochrony posiadanych zasobów, w szczególności danych

- **Do czego służy?**

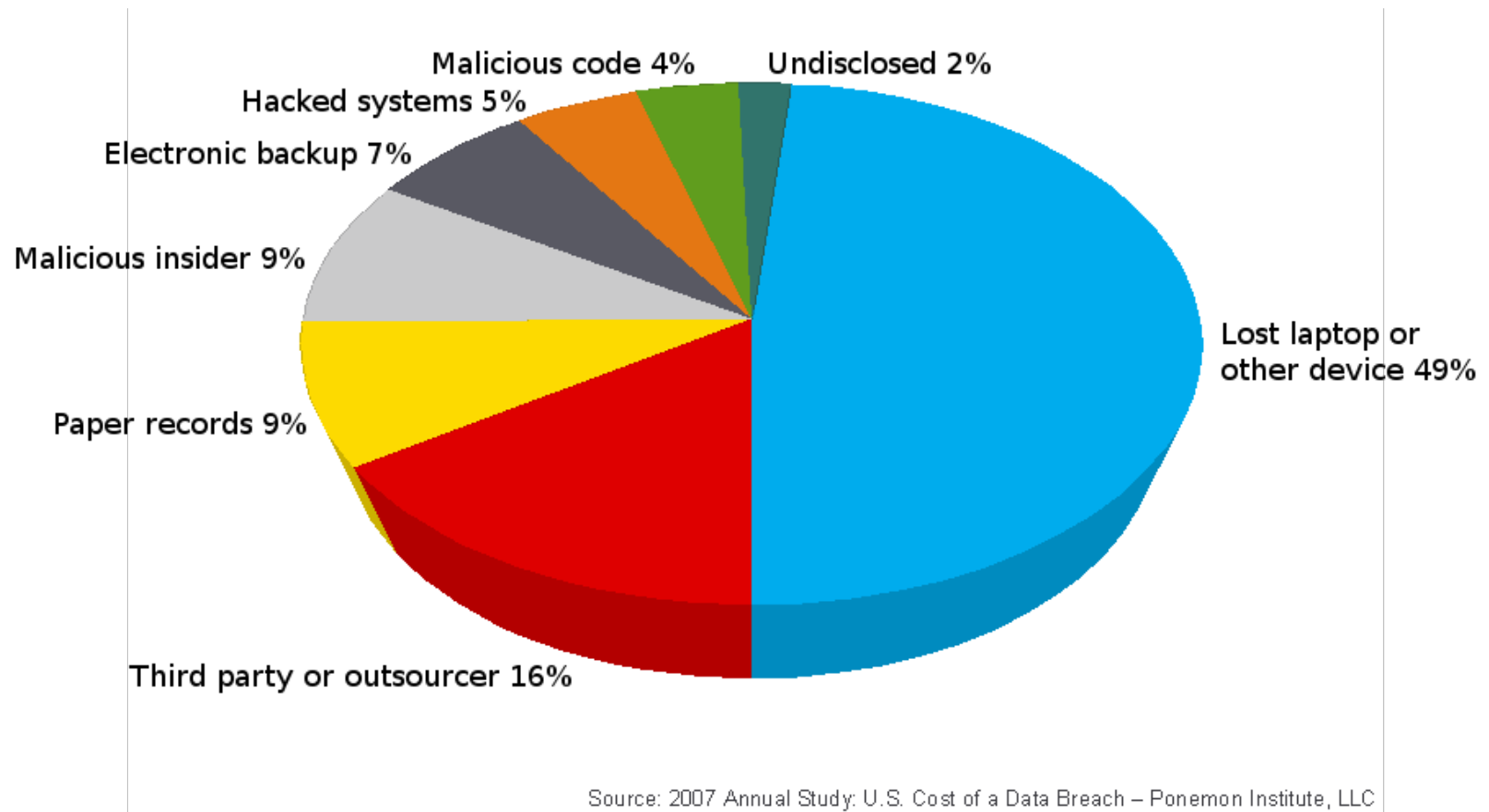
- zapewnia ochronę danych
- pozwala utrzymać sprawność systemów i produktywność użytkowników
- zapewnia zgodność z wymogami prawnymi (regulacje, przepisy)

- **Dlaczego należy stale zabezpieczać punkty końcowe?**

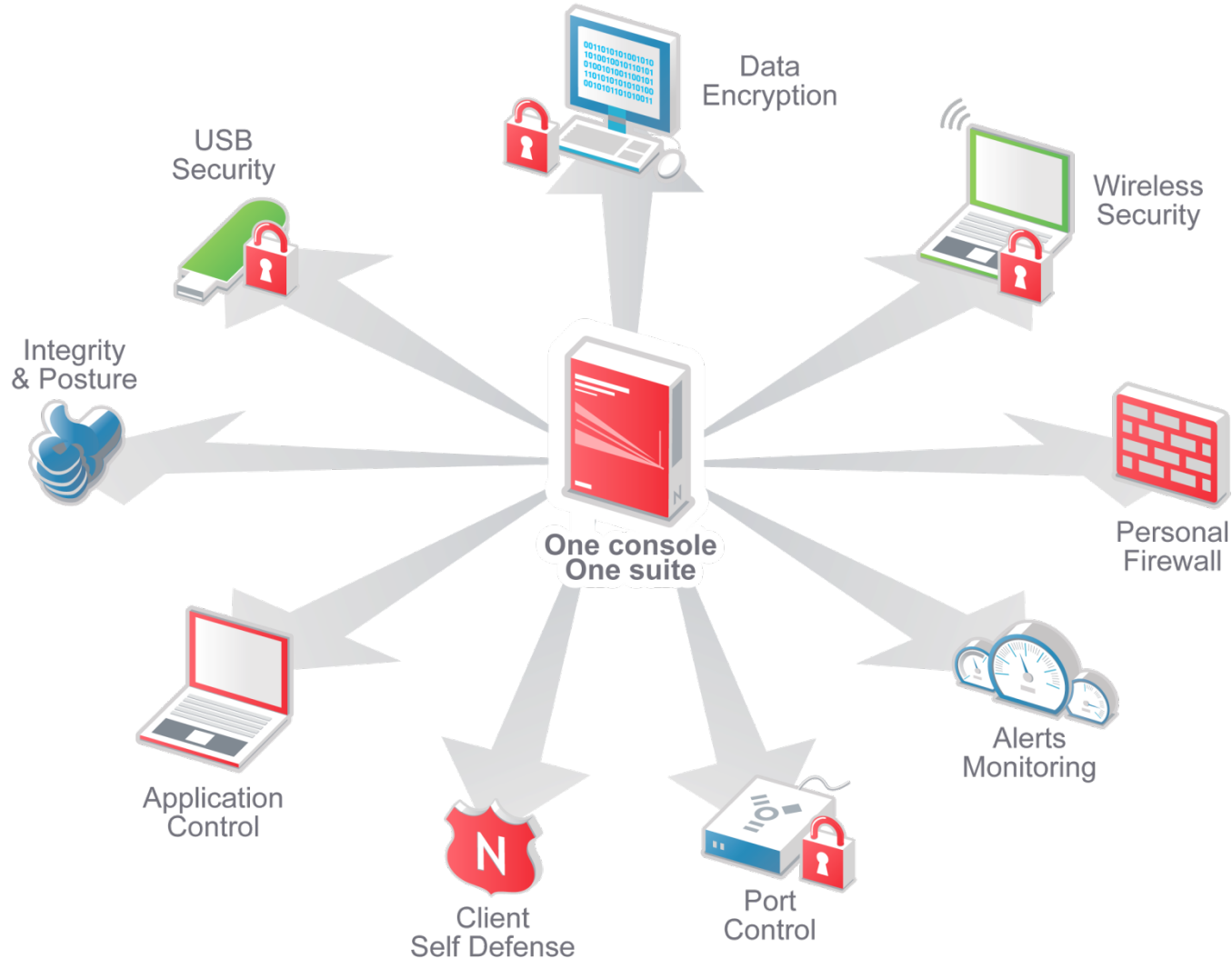
- Zmiany w sposobach prowadzenia działalności, duża szybkość zmian technologii IT, wzrost mobilności środowiska pracy użytkowników
- Z wieloma zagrożeniami można sobie poradzić działając wyłącznie na punktach końcowych:
 - > zagrożenia wynikające ze stosowania urządzeń przenoszących dane (odtwarzacze mp3, pendrive'y, tel. komórkowe)
 - > zagrożenia wynikające ze stosowania sieci bezprzewodowych
 - > kontrola wykorzystywanych aplikacji
 - > integralność zabezpieczeń 24/7, a nie tylko przy podłączeniu do firmowej sieci
 - > kontrola punktów końcowych poza biurem



Przyczyny wycieku firmowych danych



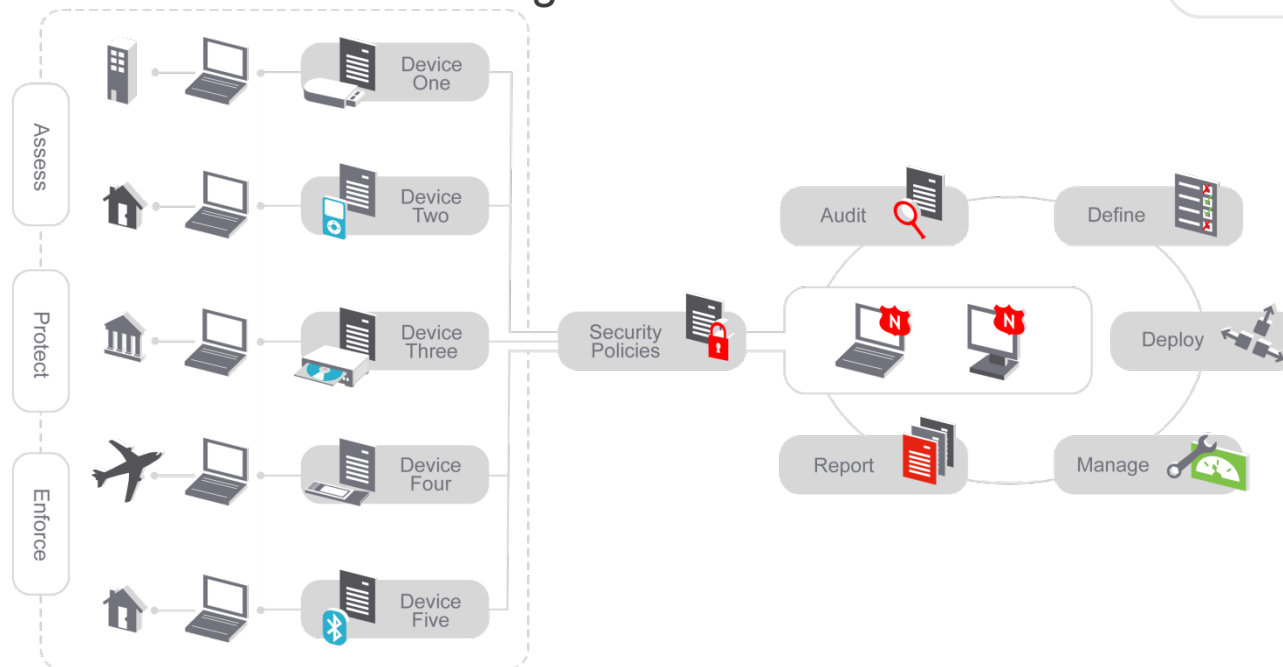
Novell zapewnia kompletne bezpieczeństwo punktów końcowych



Działanie w oparciu o informację o miejscu przebywania

Lokalizacje

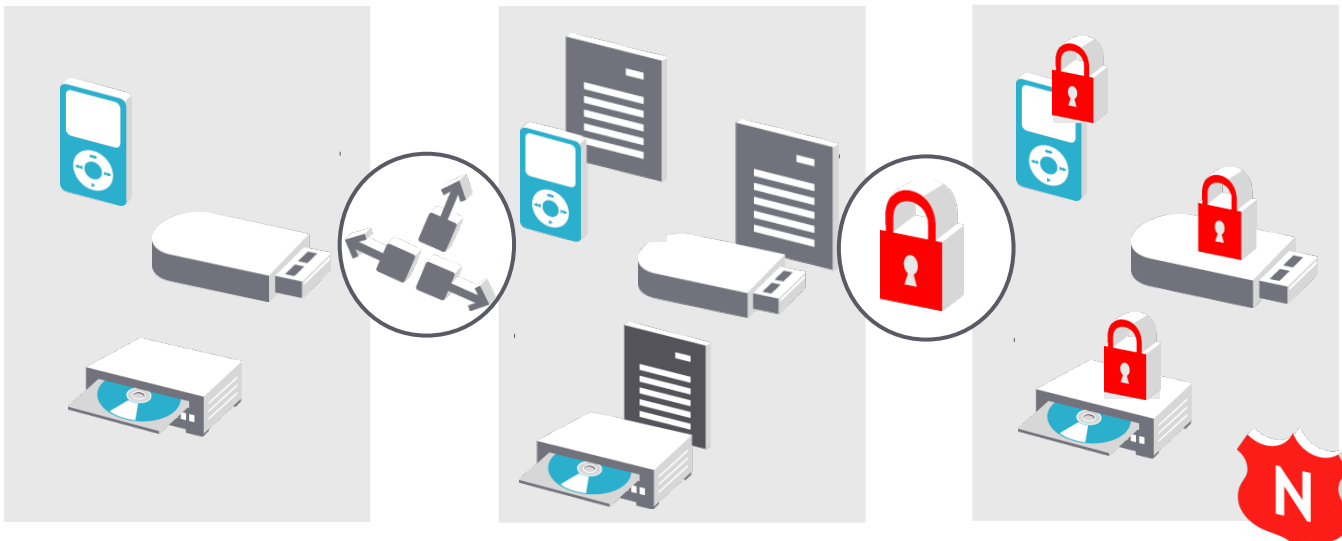
- Specyficzne zestawy ustawień dla każdej z lokalizacji, w której może znaleźć się urządzenie
- Lokalizacja jest ustalana na podstawie środowiska sieciowego



Kontrola urządzeń pamięci i USB



- Wyłączenie (w całości lub zapisu) urządzeń wymiennych, nagrywarek, napędów optycznych, wyłączenie funkcji AutoPlay i AutoRun, lista dopuszczonych wyjątków
- Wyłączenie (w całości lub zapisu) urządzeń prezentujących system plików (np. telefony, aparaty fotograficzne, ale bez myszek, klawiatur i innych nieplikowych urządzeń USB)
- Wyłączenie innych urządzeń USB (np. klawiatur, drukarek)



Szyfrowanie danych

- Przezroczyste dla użytkownika i w organizacji, silny algorytm (AES-256)
- Pliki w wybranych katalogach (wskazane przez administratora lub definiowane przez użytkownika)
- Pliki w wybranych urządzeniach (np. USB)
- Pliki w folderze Moje Dokumenty użytkownika
- Szyfrowanie wymuszone w oparciu o reguły
- Proste i bezpieczne zarządzanie kluczami szyfrującymi, dodatkowe zabezpieczenie hasłem
- Bezpieczne udostępnianie danych poza organizację



Kontrola aplikacji i sprzętu

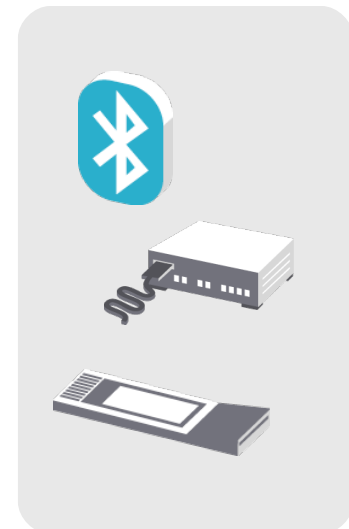
Kontrola i blokowanie oprogramowania

- blokowanie uruchamiania programów
- blokowanie programom dostępu do sieci
- sterowanie na podstawie lokalizacji



Sprzęt komunikacyjny

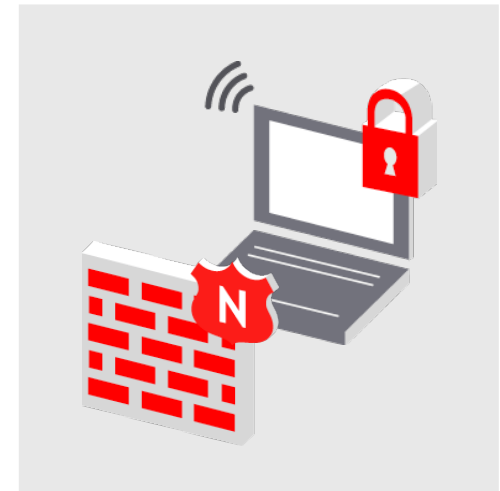
- Blokada urządzeń w określonych lokalizacjach:
 - podczerwień
 - Bluetooth
 - 1394 (*Firewire*)
 - porty szeregowe/równoległe
 - modemy



Kontrola sieci WiFi

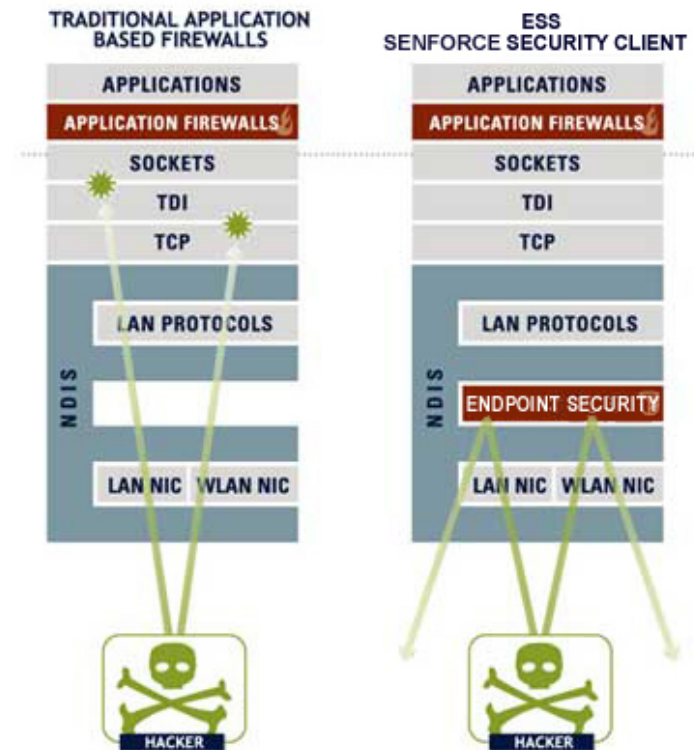


- Wyłączenie sieci WiFi
- Wyłączenie sieci WiFi, gdy jest aktywne połączenie kablowe
- Blokada połączeń mostkowych
- Blokada sieci „ad hoc”
- Ograniczenie dostępu na podstawie SSID, MAC i karty sieciowej
- Ustawienie minimum zabezpieczeń (brak zabezpieczeń, WEP 64, WEP 128, WPA)



Osobisty firewall zarządzany centralnie

- Działa na poziomie warstwy NDIS
- Chroni przed atakami na protokoły sieciowe
- „Access Control Lists” (ACLs) dla zaufanej komunikacji
- Ustawienia definiowane centralnie, szybka propagacja
- Ustawienia zależne od lokalizacji
- Brak możliwości wyłączenia przez użytkownika, nawet z prawami administratora
- Reguły TCP/UDP/IP/MAC
- Wymuszanie kwarantanny urządzenia



Ochrona (samoobrona) agenta

- Ochrona plików wykonywalnych, polis, bibliotek agenta
- Ochrona wpisów w rejestrze
- Ochrona sterowników
- Ochrona procesu
- Ochrona serwisu (usługi)
- Ochrona hasłem przed odinstalowaniem
- Ochrona (samoobrona) agenta, nawet przed użytkownikiem z prawami administratora



Inne funkcjonalności

Środowisko skryptowe JavaScript i VBScript do tworzenia zaawansowanych reguł integralności i naprawy (Integrity and remediation) – w ZESM11 SP1 – już wkrótce

Chwilowe wyłączenie/obejście polity

- Hasło administratora
- Wygenerowane dla użytkownika hasło jednorazowe



Wymuszenie połączenia VPN

- Automatyczne łączenie się przez VPN z siecią firmową w nieznannej lub zagrażającej bezpieczeństwu lokalizacji
- Wymuszenie szyfrowania/tunelowania całego ruchu ze stacji roboczej



Dziedziczenie polity i ustawień

Ochrona na poziomie sterowników

Sterownik systemu plików

- Może blokować dostęp i uruchamianie dowolnego pliku



Sterownik-filtr urządzeń przechowujących dane

- Obsługuje każde urządzenie, które udostępnia system plików
- Tryb tylko do odczytu lub całkowita blokada



Sterownik-filtr TDI

- Blokowanie aplikacjom dostępu do sieci



Firewall warstwy NDIS

- Oparty na stanie połączenia (stateful) i sesjach
- Obsługuje ruch sieciowy, zanim dotrze do systemu operacyjnego



Licencjonowanie i ceny

ZENworks Endpoint Security Management – licencjonowanie

- Po jednej licencji na każdy komputer użytkownika (urządzenie)
- Ceny
 - € 80 za licencję z roczną asystą techniczną (maintenance)
 - € 245 za licencję z roczną asystą techniczną w przypadku zakupu zestawu **ZENworks Configuration Management Enterprise Edition**

Dostępność w zestawach...

W cenniku firmy Novell produkty z linii ZENworks są dostępne samodzielnie oraz w następujących zestawach:

Produkty dostępne samodzielnie w cenniku:	Dostępne zestawy:			
	ZENworks Configuration Management Standard Edition	ZENworks Configuration Management Advanced Edition	ZENworks Configuration Management Enterprise Edition	Novell Endpoint Lifecycle Management Suite
ZENworks 11 Configuration Management	•	•	•	•
ZENworks 11 Patch Management		•	•	•
ZENworks 11 Asset Management			•	•
ZENworks 11 Endpoint Security Management			•	
ZENworks Application Virtualization 8				•

UWAGA: ZENworks 11 Configuration Management w wersji Standard jest dostępny w Polsce w ramach **promocyjnego zestawu Novell Open Workgroup Suite**

Sprawdź: www.novell.pl/promocje

ZENworks Endpoint Security Management w Twojej organizacji

- Mamy specjalne ceny dla różnych grup odbiorców (np. administracja, edukacja, szpitale)
- Skorzystaj z indywidualnej wyceny i formularza zamówienia oferty:
 - www.novell.pl/formularz.html
- Więcej informacji o produkcie
 - www.novell.com/products/zenworks/endpointsecuritymanagement
 - infolinia 800 22 66 85

Demonstracja systemu

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.