

# Hardening your Identity Layer

October 2011

Ronny Bjones  
Senior Architect  
Directory, Access & Information Protection  
Microsoft Corporate

Copyright © Microsoft Corporation. All Rights Reserved.

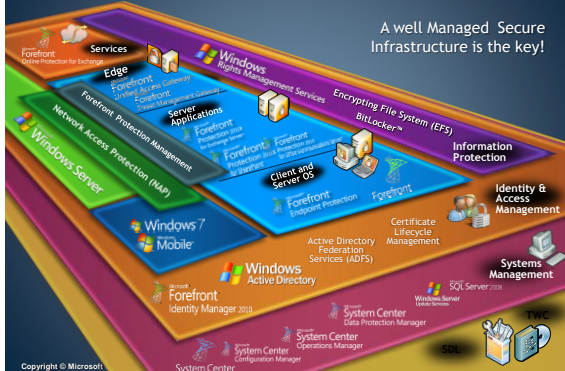
# Agenda

- Microsoft Hardening
- Cloud Hardened by Default
- Identity is key
- Join the TDL Authentication and Cybercrime pilot
- Conclusions

Copyright © Microsoft Corporation. All Rights Reserved.

# Microsoft Security: Defense In Depth

A well Managed Secure Infrastructure is the key!



Copyright © Microsoft

# Multi-Layered Defense

Strategy: employ a risk-based, multi-dimensional approach to safeguarding services and data

Security Management	Threat and Vulnerability Management, Monitoring and Response
Data	Access Control and Monitoring, File/Data Integrity
User	Account Management, Training and Awareness, Screening
Application	Secure Engineering (SDL), Access Control and Monitoring, Anti-Malware
Host	Access Control and Monitoring, Anti-Malware, Patch and Configuration Management
Internal Network	Dual-factor Auth, Intrusion Detection, Vulnerability Scanning
Network perimeter	Edge Routers, Firewalls, Intrusion Detection, Vulnerability Scanning
Facility	Physical Controls, Video Surveillance, Access Control

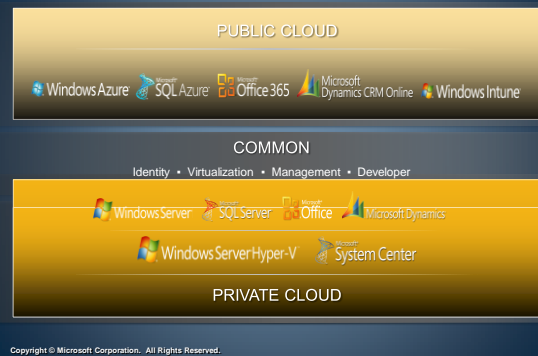
Copyright © Microsoft Corporation. All Rights Reserved.

# Agenda

- Microsoft Hardening
- Cloud Hardened by Default
- Identity is key
- Join the TDL Authentication and Cybercrime pilot
- Conclusions

Copyright © Microsoft Corporation. All Rights Reserved.

# Microsoft Cloud for Enterprise



Copyright © Microsoft Corporation. All Rights Reserved.

## Hybrid Becomes the Norm

- Public Cloud(s)
  - Many cloud providers and services
- Private Cloud
  - Within the enterprise or partner data center
- Hybrid will be the default
  - Mixture of private & public cloud(s)

Copyright © Microsoft Corporation. All Rights Reserved.

## Cloud is hardened by default

- <http://www.globalfoundationservices.com>

Copyright © Microsoft Corporation. All Rights Reserved.

## Agenda

- Microsoft Hardening
- Cloud Hardened by Default
- **Identity is key**
- Join the TDL Authentication and Cybercrime pilot
- Conclusions

Copyright © Microsoft Corporation. All Rights Reserved.

## Identity is common between Public or Private Cloud

- Identity will play a crucial role
- Can we still have different identity management systems for hybrid clouds?
  - Different cloud providers
  - Enterprise IDs
  - Partner IDs
- Federation is the norm
- What is the attack surface when identities get compromised?

Copyright © Microsoft Corporation. All Rights Reserved.

## Privacy is a key Property

Copyright © Microsoft Corporation. All Rights Reserved.

Microsoft

## Claims-Based Identities

- Federation based on open standards
- Externalize authentication
  - Support for different Levels Of Assurance (multi-factor)
  - Fine-grained authorization decisions
- Build for scalability

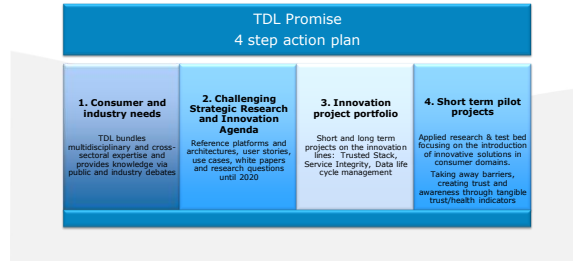
Copyright © Microsoft Corporation. All Rights Reserved.

Microsoft



**TDL Trust in Digital Life Trust in Digital Life shared vision**

*Trust in Digital Life is a challenging ecosystem bringing tangible trust in digital services supporting new ways of living and working. Trust will become an intrinsic property of any transaction. People should be able to recognize trustworthy services, transactions and data.*

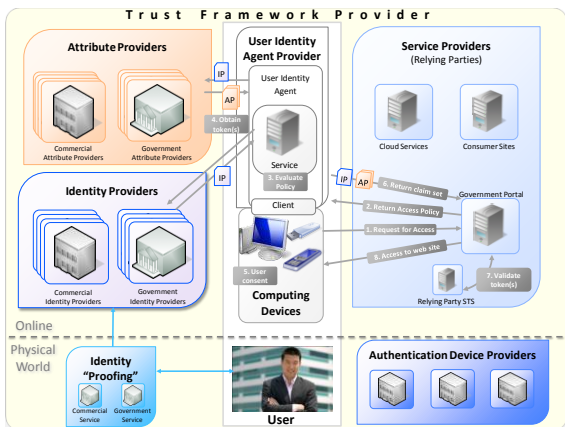


**TDL Trust in Digital Life Storyline**

- Introduction
- **Identity Architecture Principles**
  1. Composable Architecture
  2. Technology and Standards evolution
  3. Attributes remain with the owner of the data
  4. User Consent
  5. Privacy
  6. Correctness and accountability

**TDL Trust in Digital Life Storyline**

- Introduction
- Identity Architecture Principles
- Claims-based Application Architecture
- **Architecture**
  - Learn about the different components of the architecture
  - And how these components interact with each other
  - See the huge opportunity to turn legacy systems into components of the architecture as e.g. Attribute Providers



**TDL Trust in Digital Life TDL Authentication & Cybercrime Pilot**

- Hybrid: Mixing public sector credentials/services with public sector
- Build the infrastructure and validation with user groups
  - Usability of identity, privacy and security
- State of the Art authentication infrastructure
- Innovative cybercrime concepts
  - How can we be sure of the identity when the device is unhealthy?
  - Produce Device Health Claims
- Project is kicked-off
- Several "sprints" add new capabilities to the infrastructure
- Ronny.Bjones -> [microsoft.com](http://microsoft.com) to join the project

## Conclusions

- Hybrid is the norm
- Design for scale with Claims-based Identities
- Call to Action: Follow or join the TDL Pilot

Copyright © Microsoft Corporation. All Rights Reserved.

Microsoft

## Questions?

Copyright © Microsoft Corporation. All Rights Reserved.

Microsoft

**Microsoft**<sup>®</sup>  
*Your potential. Our passion.™*

© 2011 Microsoft Corporation. All rights reserved. Microsoft, Windows, Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. This document contains information that may be subject to change without notice. Microsoft makes no warranties, expressed or implied, as to the accuracy or reliability of the information provided in this document.

Copyright © Microsoft Corporation. All Rights Reserved.