

The Evolution of Data Center Security Architecture

“It’s not the appliances, it’s the data!”

Wallace Dalrymple
Chief Network & Security Architect
General Motors
May 21st, 2007

INTEROP[®]

BUSINESS. TECHNOLOGY.
ONE WEEK. ONE PLACE.

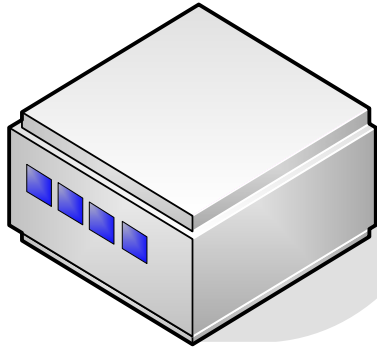
Agenda

- A Quick Story.....
- Data-Centric Security Model
- Re-architecting the Data-Center
- Emerging Data-Centric Technologies
- Data-Centric Timeline

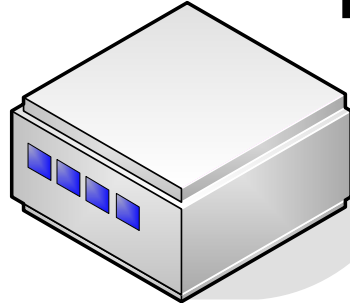
RSA Experience



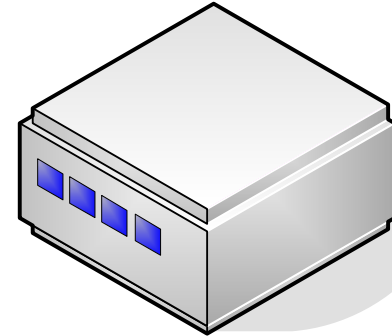
Attack of the Appliances!



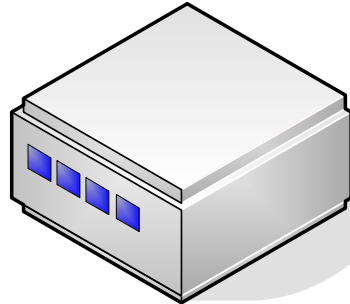
NAC



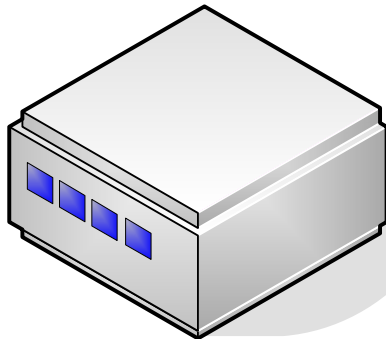
IDS



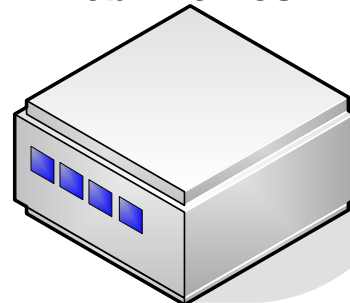
Vulnerability Scanning



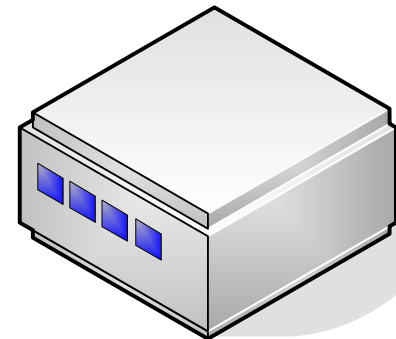
Web Proxies



IPS



Data Leakage



Wireless IPS

A person is walking through a server room, surrounded by rows of server racks. The room is brightly lit, and the racks are filled with various components. The person is wearing a light-colored shirt and dark pants. The overall scene is a typical data center environment.

A New Focus on Securing Data

- Many organizations are realizing that perimeter firewalls, anti-virus software, and intrusion detection systems are not enough to protect them from attacks on company data
- Data attacks have moved to the application level, databases level, storage/file level circumventing network-based firewalls
- The ideal form of protection requires new strategies and more focus on data-centric protection measures

The Future is Data-Centric

- Infrastructure-Centric mechanisms concentrate on:
 - Protecting information by securing the infrastructure components that store, transmit, or process data
 - Firewalls
 - Intrusion Detection & Prevention Systems
- Data-Centric mechanisms protect:
 - Information independent of the infrastructure components
 - Encryption solutions which encrypts data wherever that data travels
 - Access solutions which restrict access to only individuals who need to access the data



Data-Centric Mission Statement

A strategy that considers:

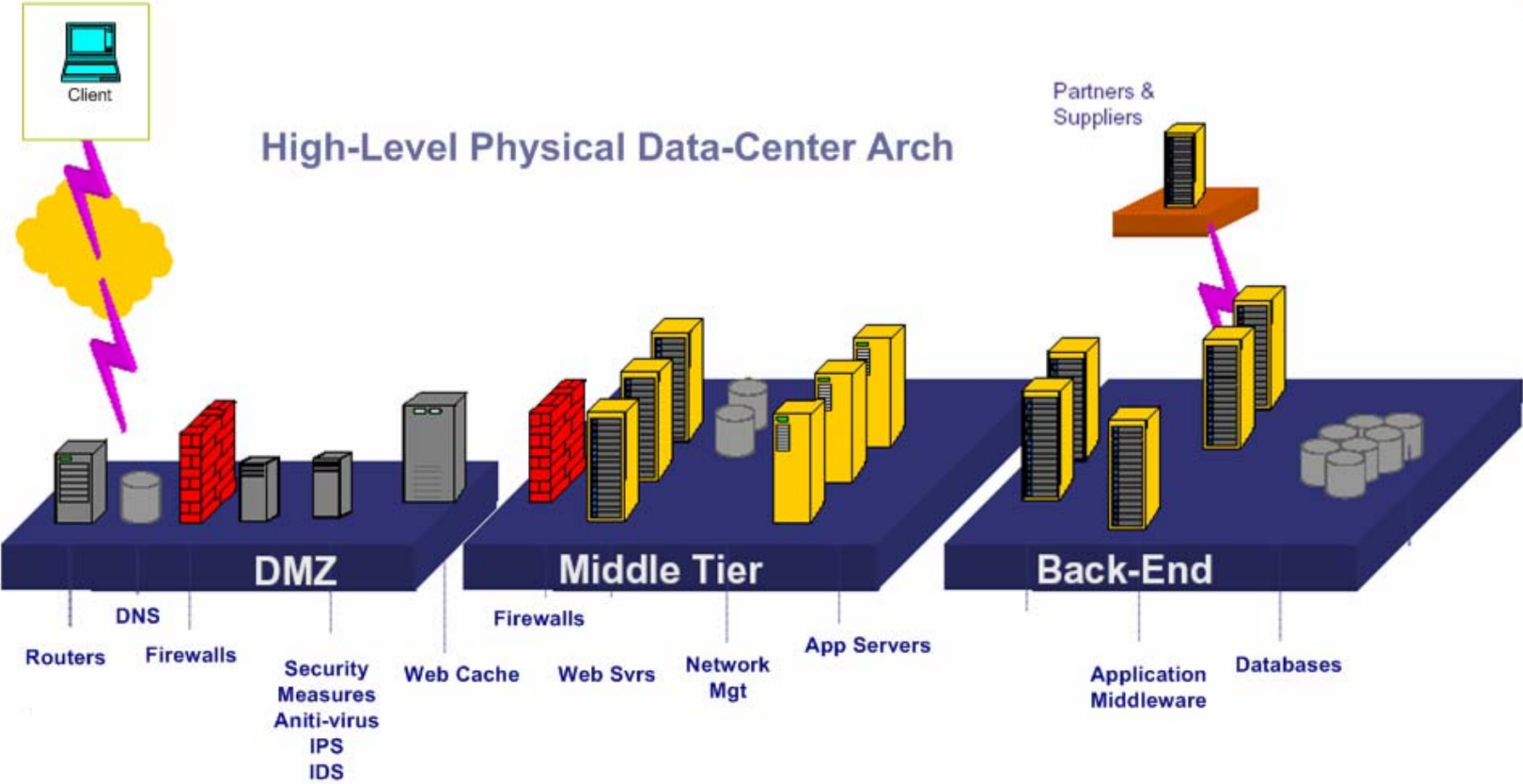
- Open, integrated platforms
- Strong access controls
- Encryption framework
- Integrate with complementary security products & technologies



Re-designing the Castle



Data Inside the Castle



Data Outside the Castle



Help Desk



Mobile Users



Employees



Suppliers/Contractors



Partners

Expanding the Boundaries

- Safely share data
- Provide access controls
- Prevent data theft
- Leverage existing security tools

The Move Towards Data-Centric

- Enterprise Rights Management
- Federated Identity
- Dynamic Data Encryption
- Redefining the “Data” Center Architecture

ERM/IRM

- It's not DRM – focused on entertainment media
- It is focused on:
 - Pre-access to data (pass-phrases, biometrics)
 - Post-access to data (forwarding of files, emails)
 - Securing of data (intellectual property)
 - Regulatory compliance & versioning of data
- Provides the ability to protect & manage data outside of your immediate control

ERM/IRM Challenges

- Encryption can impede document recovery, archiving, and search
- Accessing files outside the Corp FW
- No current standard for:
 - agent software
 - key management
 - common rights markup language
- Today ERM is very expensive

Federated Identity

- The process of a user's authentication across multiple IT systems or organizations
- The agreement of multiple organizations to agree on a common authentication tool
- Standardizing on methods of communication
 - SAML
 - SOAP

Challenges to Federated Identity

- Must work with existing controls
 - AD
 - LDAP
- There must be an industry standard adopted
 - Must work with 3rd parties
 - Must be able to interoperate with multiple vendors
- It's identity; Not “Data”

Dynamic Data Encryption

- Enforce consistent security policies across the enterprise
- Protect data-in-motion and data-at-rest
- Transparent to existing applications & infrastructure
- Minimal impact on performance

Challenges to Dynamic Data Encryption

- Enterprise solutions vs. point solutions
- Multiple encryption protocols
- Management of Keys
- Changes to COTS & legacy systems
 - Cost vs. Risk
- Performance!

Redefining the “Data” Center Architecture

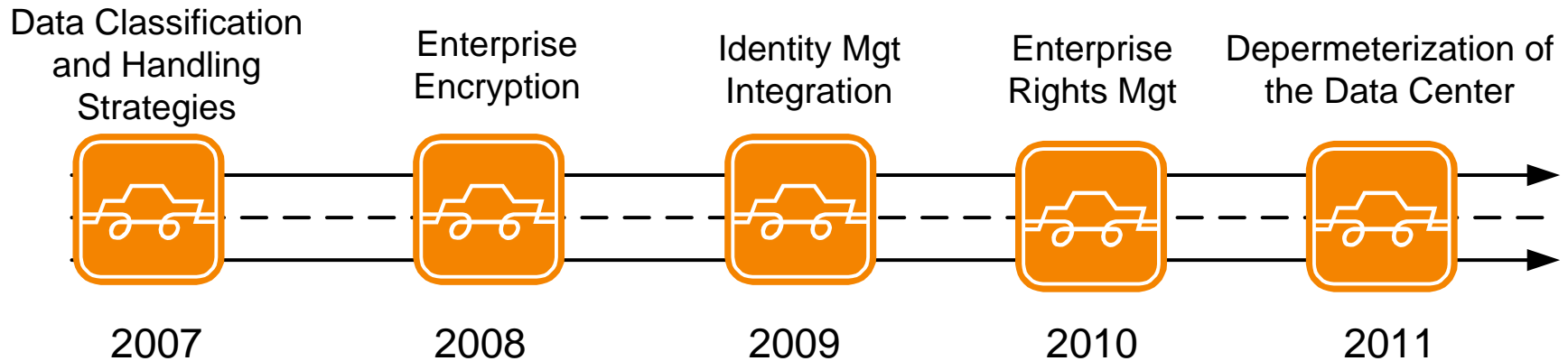
- Extending the data center architecture & securing data access to:
 - Suppliers
 - Joint Ventures/Partners
 - Customers
- Extends business boundaries & capabilities to allow for a more agile response to business needs

Defining the “Data” Center Architecture

- Security must be built-in from the ground up
- Access to data must be done holistically
- Must be part of the data center architecture & design
- Must enable greater business flexibility & show a cost reduction

Data-Centric Evolution

Data-Centric Timeline



Moving Forward.....

- Traditional defense-in-depth isn't sustainable
- Business requirements will continue to outpace IT capabilities to keep up
- Emerging technologies (ERM,F.I.)...coming soon to...start planning today!

Thank You!

Please feel free to contact me with any
comments or questions at

Wallace.Dalrymple@GM.com