Digital Transformation is to Business what Zero Trust is to a Security !

Vlad Klasnja – Director, Cloud Architecture Services

Agenda

- What it IS and What is NOT ?
- Past & Present
- Value, Benefits and Pillars of Zero Trust
- Where to start ?

Charlie CISO cartoon strip

Definition

“Forrester Research defines the Zero Trust Model as "a conceptual and architectural model for how security teams should redesign networks into secure micro perimeters, strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation."

Zero Trust’s main purpose is **Removal of Implicit Trust**

Zero Trust focuses on DATA centric and RISK based ACCESS approach

Zero Trust is **NOT**

- a quick win
- an “Off-the-shelf” product
- a one-off or IT only project
- a play for only identity or network vendors
- an idea where trust is removed completely

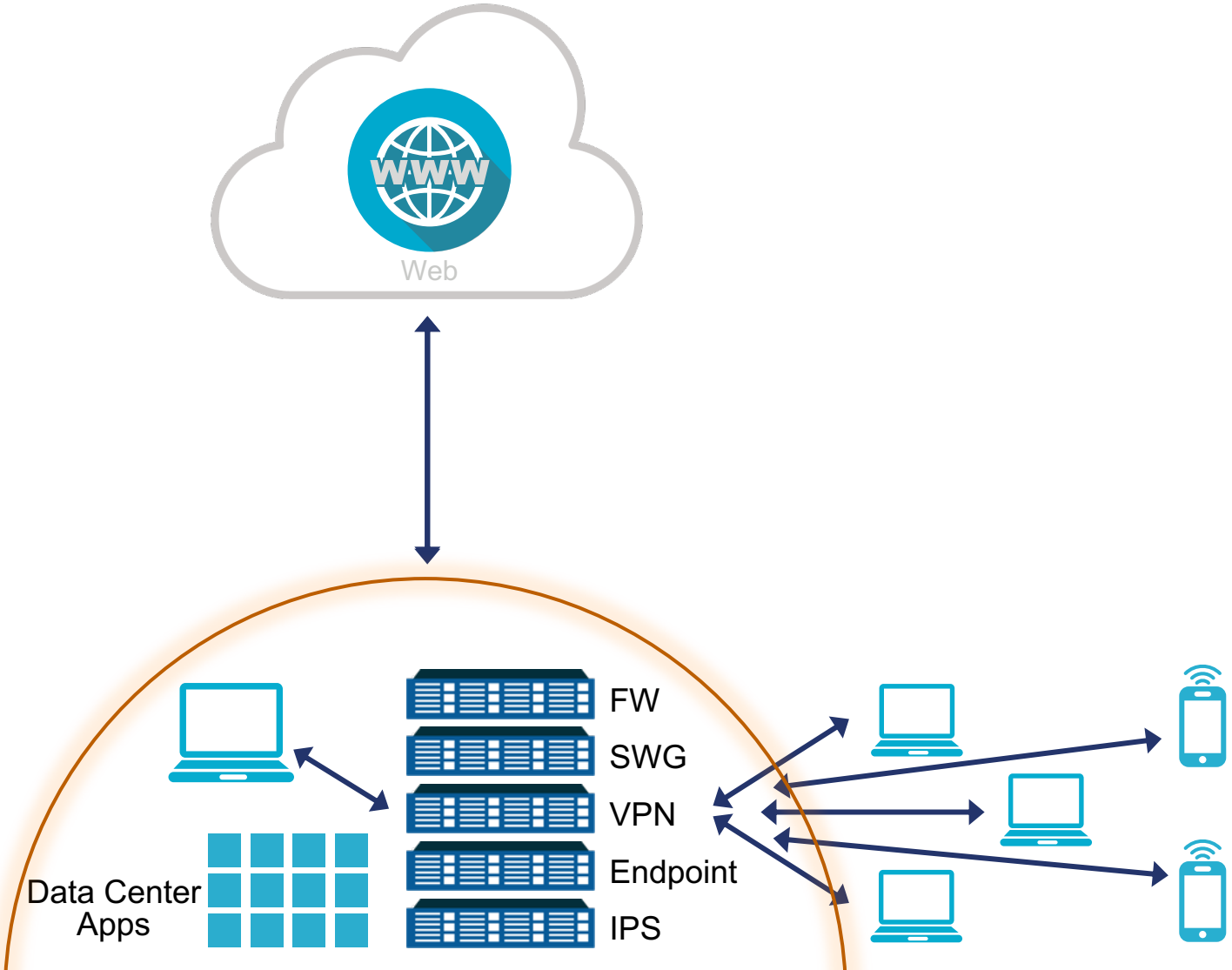
Zero Trust is

- requiring a programmatic approach
- a combination of process & technology
- helping with reduction of complexity
- application, identity and data focused
- contextual and dynamic in nature

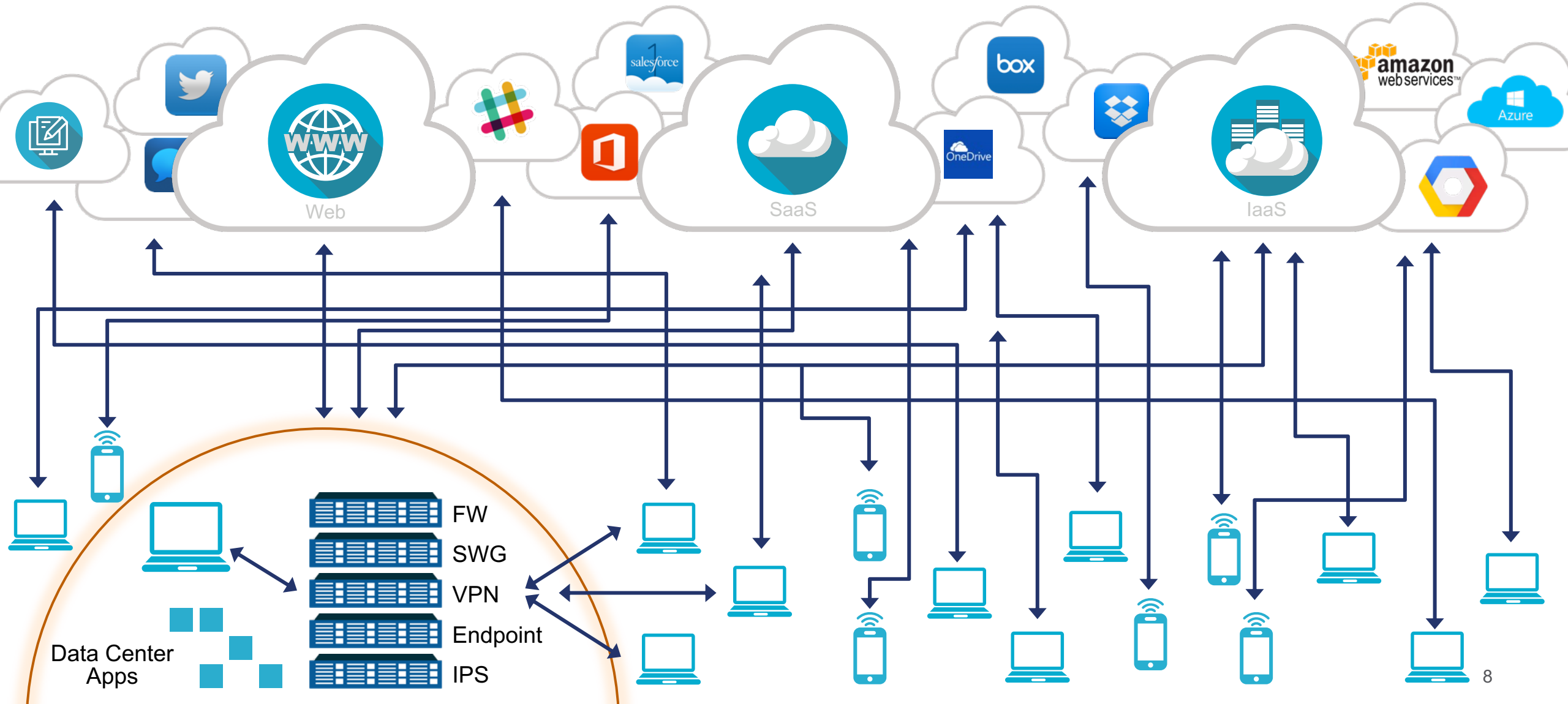
Past – How did we get here?

Zero trust started out as a networking concept with a specific perimeter in mind.

Controlled Access Design (Everything back hauled)



Direct to Internet



Mobilization of the Workforce

User, Group, OU

On Any Device

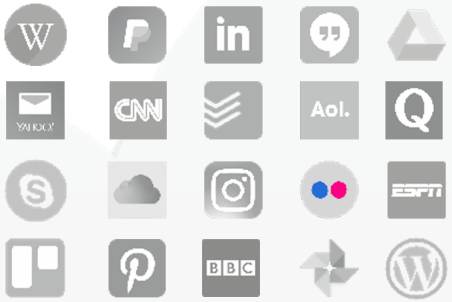
On Her Cell Phone

On Her Tablet

On Her Laptop

(Managed or Unmanaged)

To Any Application



From Any Location

At the Office

At Home

At the Cafe

Share Any Information

Financials

Ideas

Pictures

Content / Classification

Present

- Connectivity is ubiquitous
- Exponential growth of Cloud and Mobility
- Users demand instant access to applications and data

Digital Transformation

Disruption

New strategies and thinking

Growth

Transformation fuels growth

Consumerization

The workplace is no longer where people work.

Digital Business Opportunities

Digital Business Strategy

Digital Business Optimization		Digital Business Transformation	
▪ Sell More ▪ Reduce Costs ▪ Digitalize Workforce	▪ Optimize Client Experience ▪ Improve Efficiency	▪ New Digital Services, Products ▪ Autonomous Buying and Selling	▪ Seamless Partner Network Integration ▪ Create an Ecosystem

Existing Business Model | **New Business Model(s)**

New Privacy and Security Model(s)

Gartner

Zero Trust is a profound cultural transformation ~~that impacts all business and organizational activities~~

Digital Transformation is to business what Zero Trust is to a Security !

Value, Benefits & Pillars

Value

Building a Security program based on Zero Trust will *drastically* decrease an organization's risk exposure

Benefits

Prevention of lateral movement

Predefined application/ resource access governance

Provides strong authentication, conditional/ least privileged access

Gain full visibility and control within your ecosystem

(On-premises and Cloud)

Enables the ability for risk-based access decisions at scale

Protects your customer's data

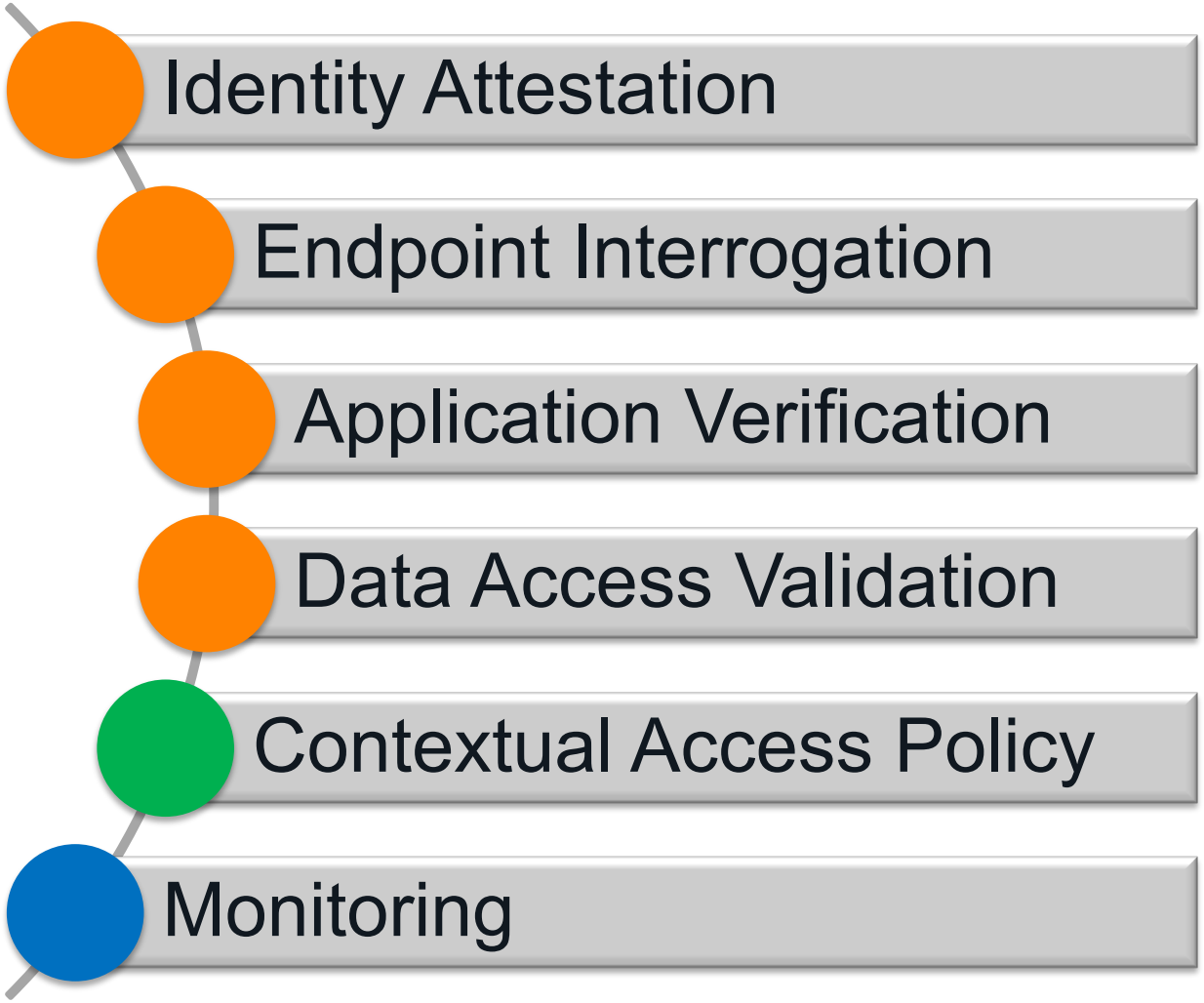
Minimizes loss of organizations intellectual property

Helps compliance audit initiatives

Supports the transition to the cloud

Aids in Security program transformation

Pillars



- Directory structure
- Federation
- MFA & PAM

- State of an endpoint
- Criteria satisfaction
- User to endpoint mapping

- Standard or NOT
- Application mapping
- Role assignment

- Classification
- Inspection & data flow
- Access relationship & patterns

- Risk score
- Adaptive enforcement
- Session isolation

- Detection
- Prevention
- Reporting

Trust is a Continuum

Trust	Level 1	Level 2	Level 3	Level 4	Level 5
Access Activity	Non-Sensitive Data (Read Only)	Non-Sensitive Data (Read & Write)	Limited Sensitive Data (Read)	Sensitive Data (Read & Write)	Sensitive Data (Read & Write & Store on Device)
Identity	Limited Access Validation	Multifactor Authentication	Multifactor Authentication	Multifactor Authentication	Multifactor Authentication
Endpoint	Unmanaged Device	Unmanaged Device	Unmanaged Device	Unmanaged Device	Managed Device
Application	Unsanctioned App	Unsanctioned App	Sanctioned App	Sanctioned App	Sanctioned App
Example	*Social Media*	*Google Drive, Box, Office365*	*Confidential Reports*	*Email*	*HR Data, Board Materials, Large Database*

Where to Start with Zero Trust

What to Consider Before Implementing Zero Trust

You must architect with your business in mind first (business outcome)

Understand your current process and deficiencies

Understand your threats and risk

Understand your technology stack

Map required capabilities, data and transaction flows

Understand your end user requirements (transparency, easy of use, availability)

Implementing Zero Trust

Document your model, architectural principles, patterns, and standards (Holistic Modular Architecture)

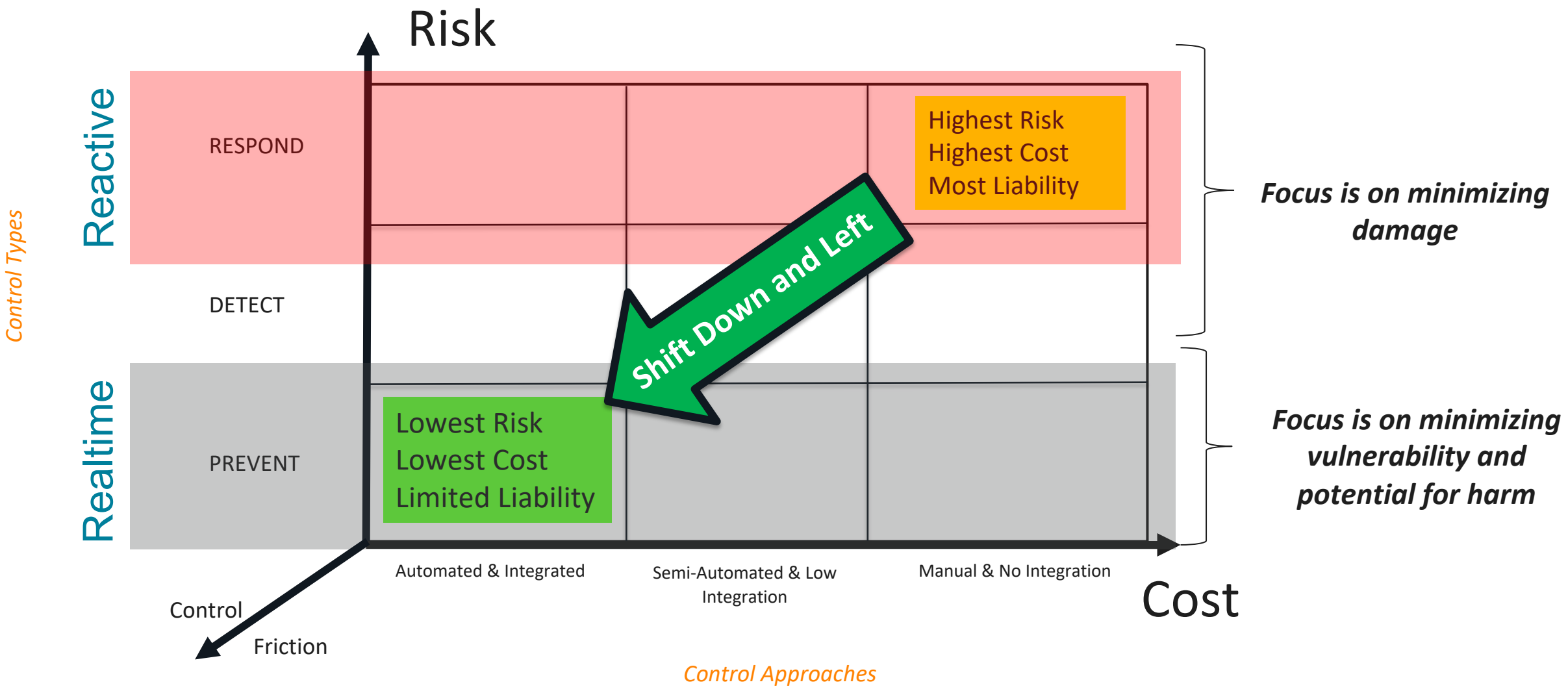
Start with idea of equalizing internet and intranet

Simplify your operating environment (remove redundancy)

Design, build, test, deploy rather than deploy and hope you got it right and integration exists

Think BIG and Start Small

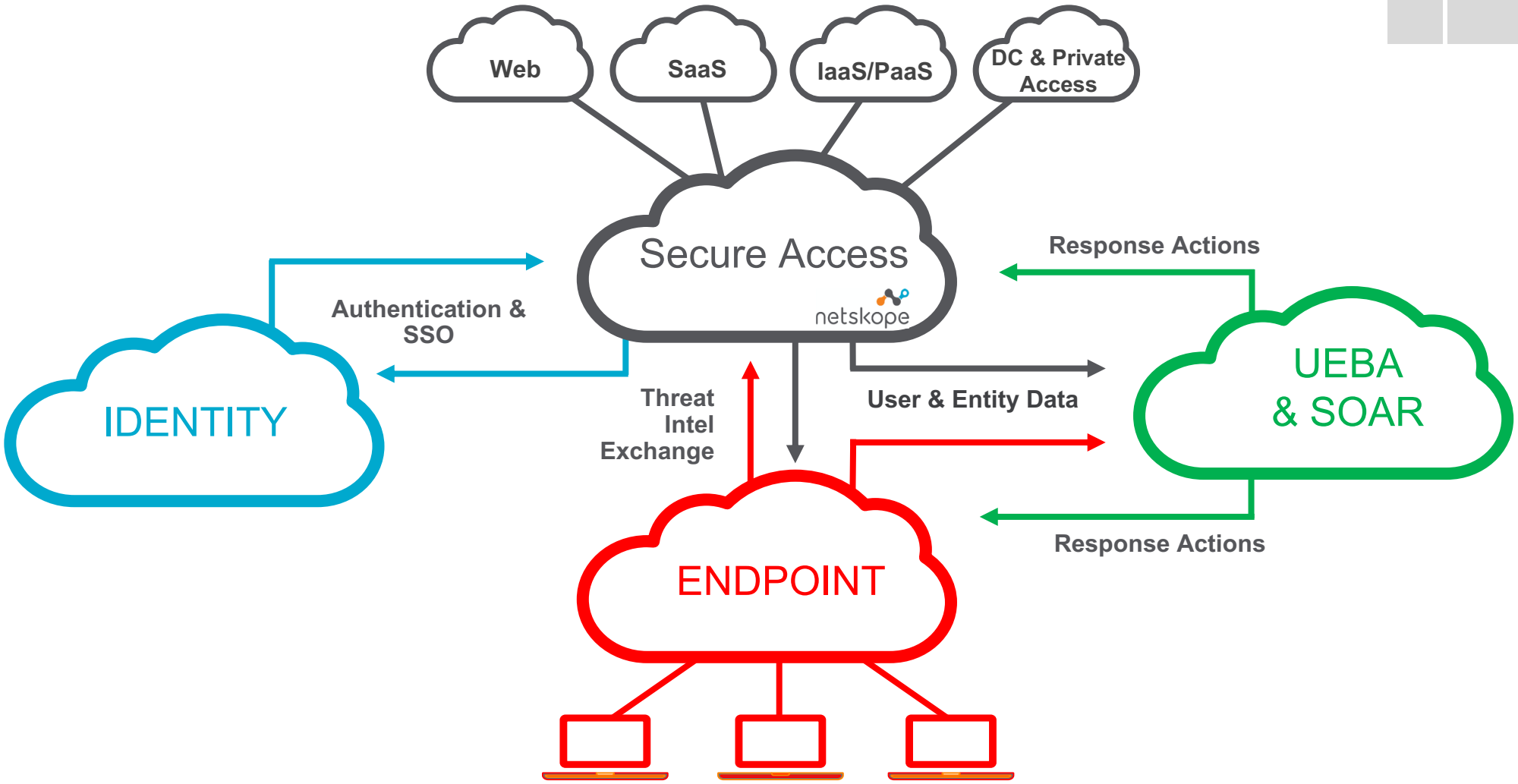
Re-Architect & Simplify



Source: Managing Risk and Information Security 2nd edition Malcolm Harkins

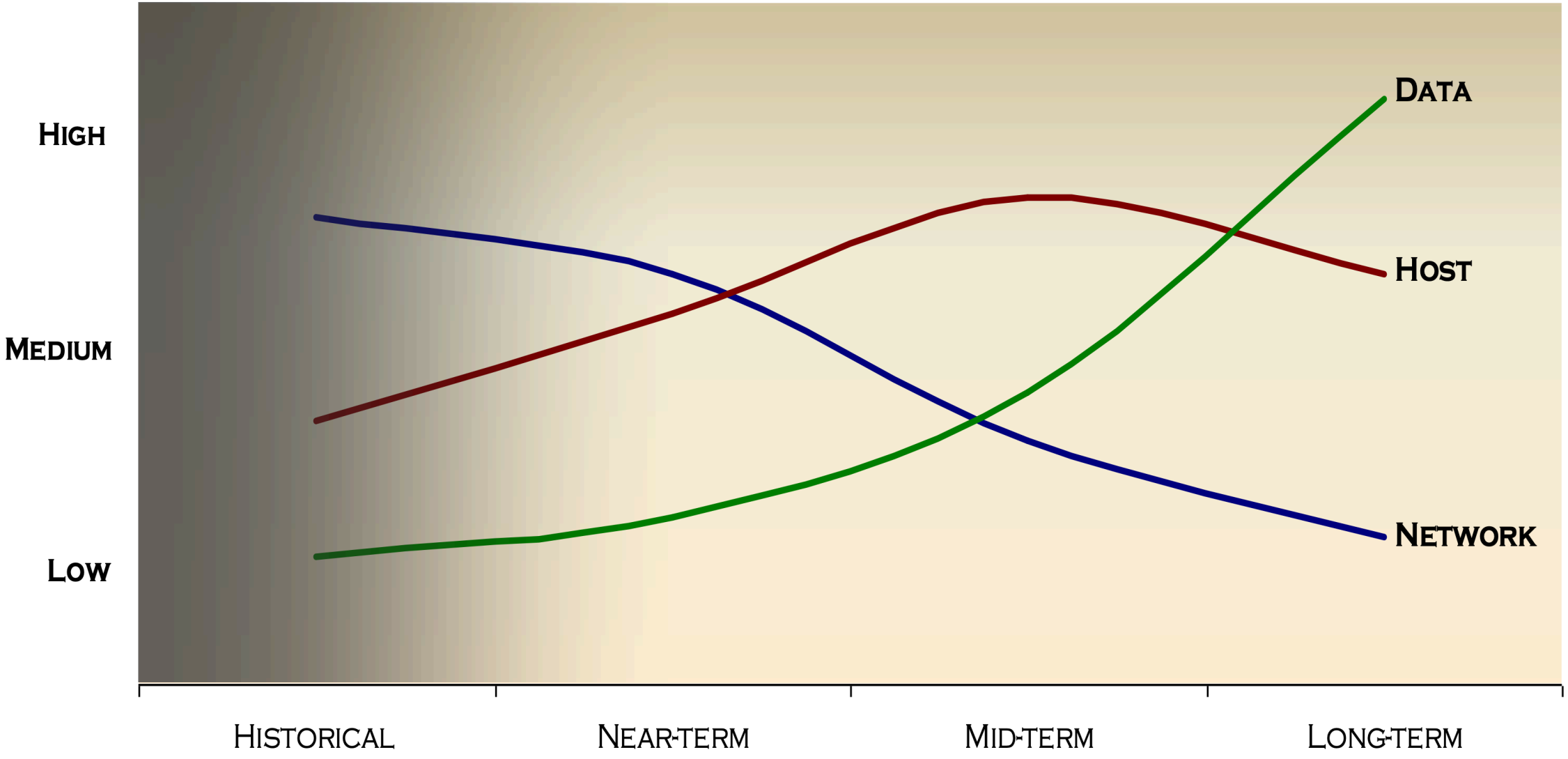
Security stack pillars

GRC		Ops
	AppSec	
	Secure Access	
	Identity	
	Endpoint	




Questions

Evolution of Information Security Technology



Created by Dan Hitchcock