RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: STR-W12

The fallacy of the "Zero Trust Network"

Paul Simmonds

CEO & CISO
The Global Identity Foundation
@simmonds_paul

#RSAC

Agenda

- How we got here!
- A little background – and a history lesson
- What Zero Trust is not, and what it may be
- Reacting to a Zero Trust strategy
- What you should be doing when you go back to work

RSAConference2019

How we got here!

Our industry loves marketing Buzzwords

- Early 90's – Viruses (are they real?)
- Mid-90's – Wardialing
- Late 90's – "Deep Packet Inspection" Firewalls
- Early 2000's – The year(s) of PKI
- Mid 2000's – Deperimeterization (thank you Jericho Forum)
- Late 2000's – "Next Generation" Firewalls
- Early 2010's – "Defence in depth" & APT's
- Mid 2010's – AI & Big Data
- And now ..... – Zero Trust

So many vendors, so many “Zero Trust” products!

Therefore; Select your products with care!

Is it just the marketing department jumping on the buzzword-bandwaggon?

So many vendors, so many “Zero Trust” products!

- Akamai
- AlgoSec
- Amazon AWS
- Aporeto
- Centrify
- Cloud Harmonics
- Cloudflare
- Cymbel
- Cyxtera
- Double Octopus
- Duo Security (Cisco)
- ForgeRock
- Google (BeyondCorp)
- Guardicore
- Jump Cloud
- Luminate
- Microsoft
- Netronome
- Okta
- PaloAlto Networks
- Panda Security
- Plixer
- ScaleFT
- SecureCircle
- Tripwire
- Zentera
- Zscaler

... and many more

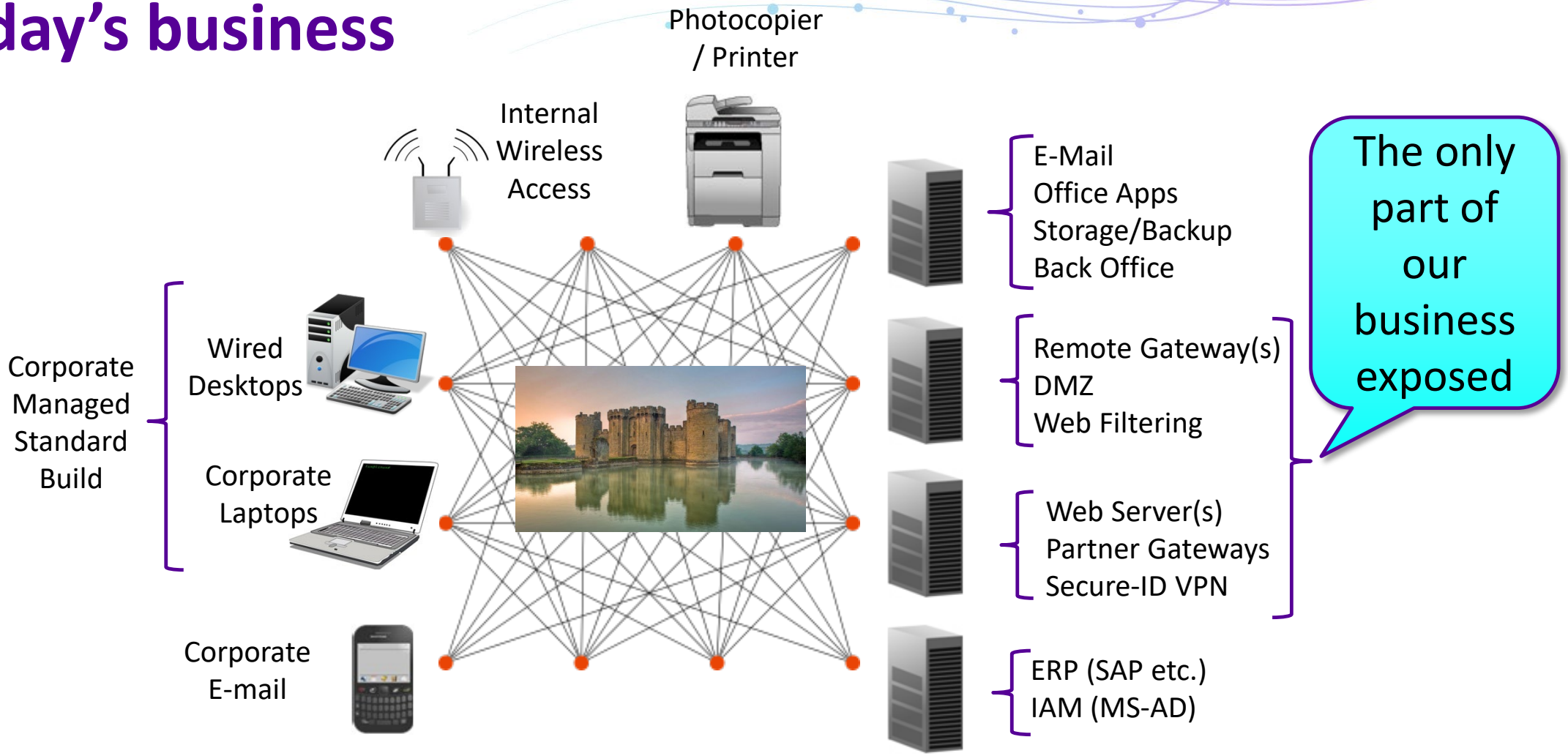
So on to the history . . .

RSAConference2019

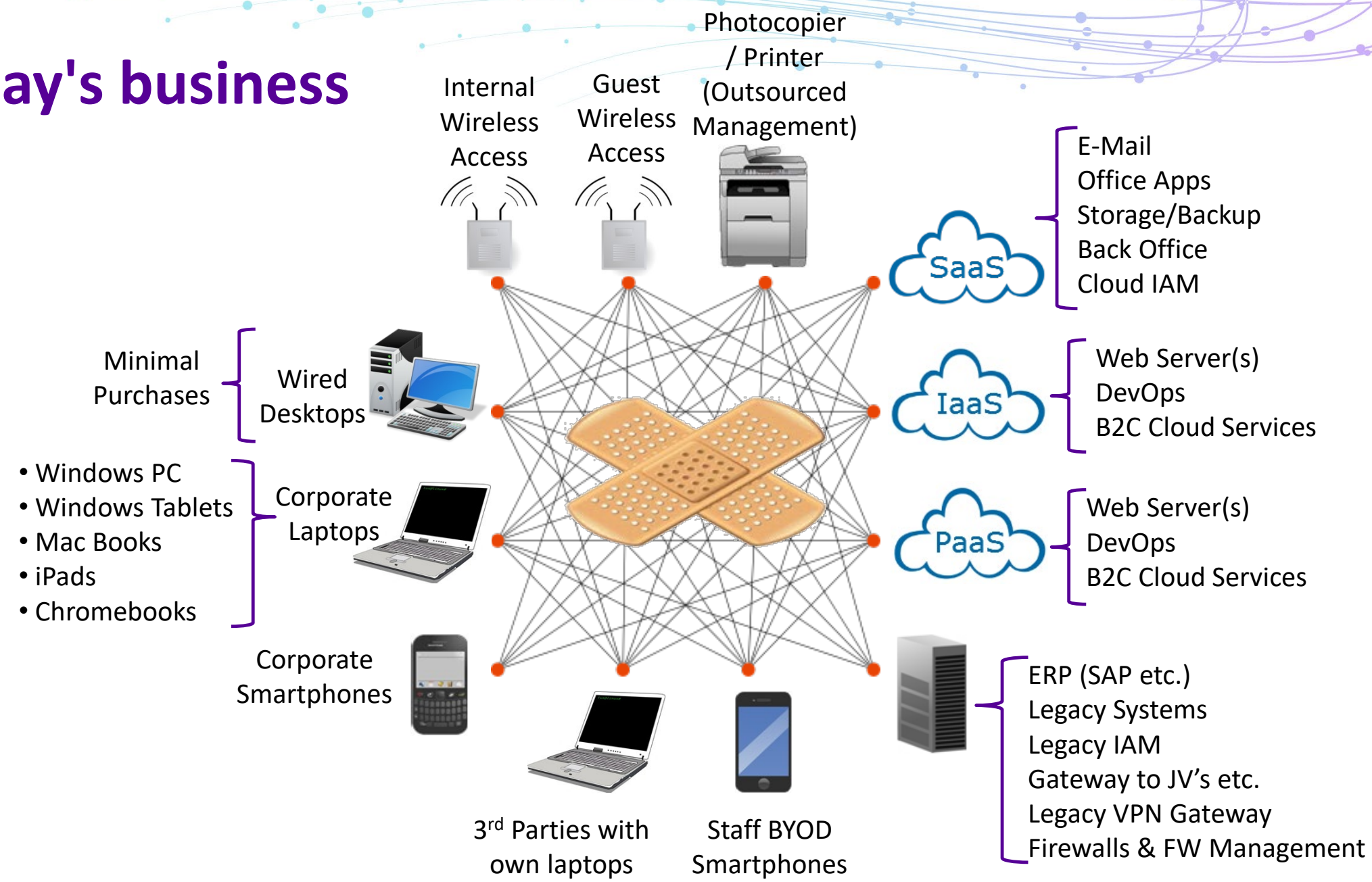
A little background

…. and a history lesson

Yesterday's business



Today's business



Tomorrow's business

Zero Trust

Minimal Purchases

Wired Desktops

Corporate Laptops

- Windows PC
- Windows Tablets
- Mac Books
- iPads
- Chromebooks

Partner Direct Connection

Wireless Access

Photocopier / Printer (Outsourced Management)

SaaS

- E-Mail
- Office Apps
- Storage/Backup
- Back Office
- Cloud IAM

IaaS

- Web Server(s)
- DevOps
- B2C Cloud Services
- API Services

PaaS

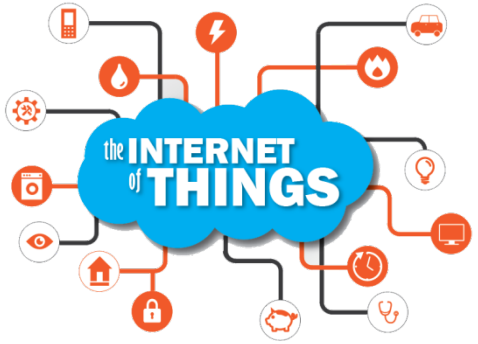
- Web Server(s)
- DevOps
- B2C Cloud Services
- API Services

Plant / Manufacturing

3rd Parties with own laptops

Staff BYOD Smartphones

ERP (SAP etc.)

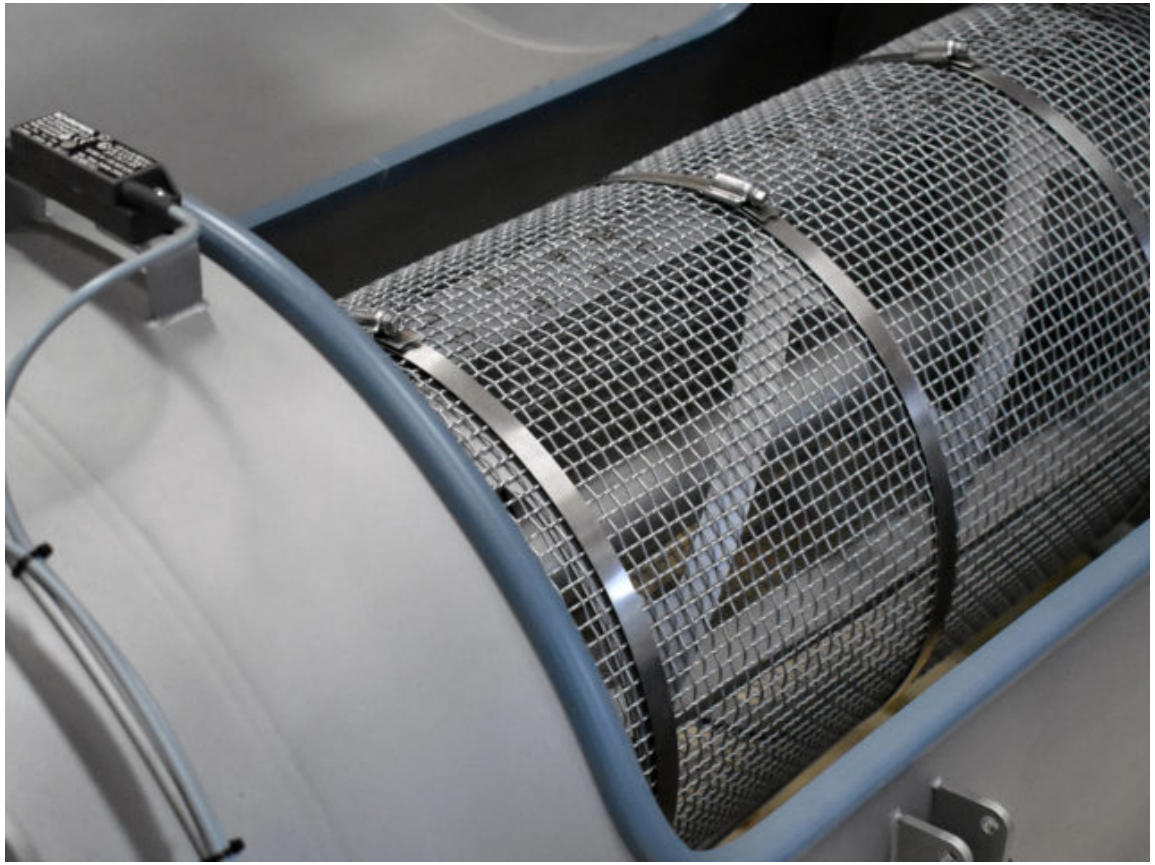


IPv6 FORUM 5G

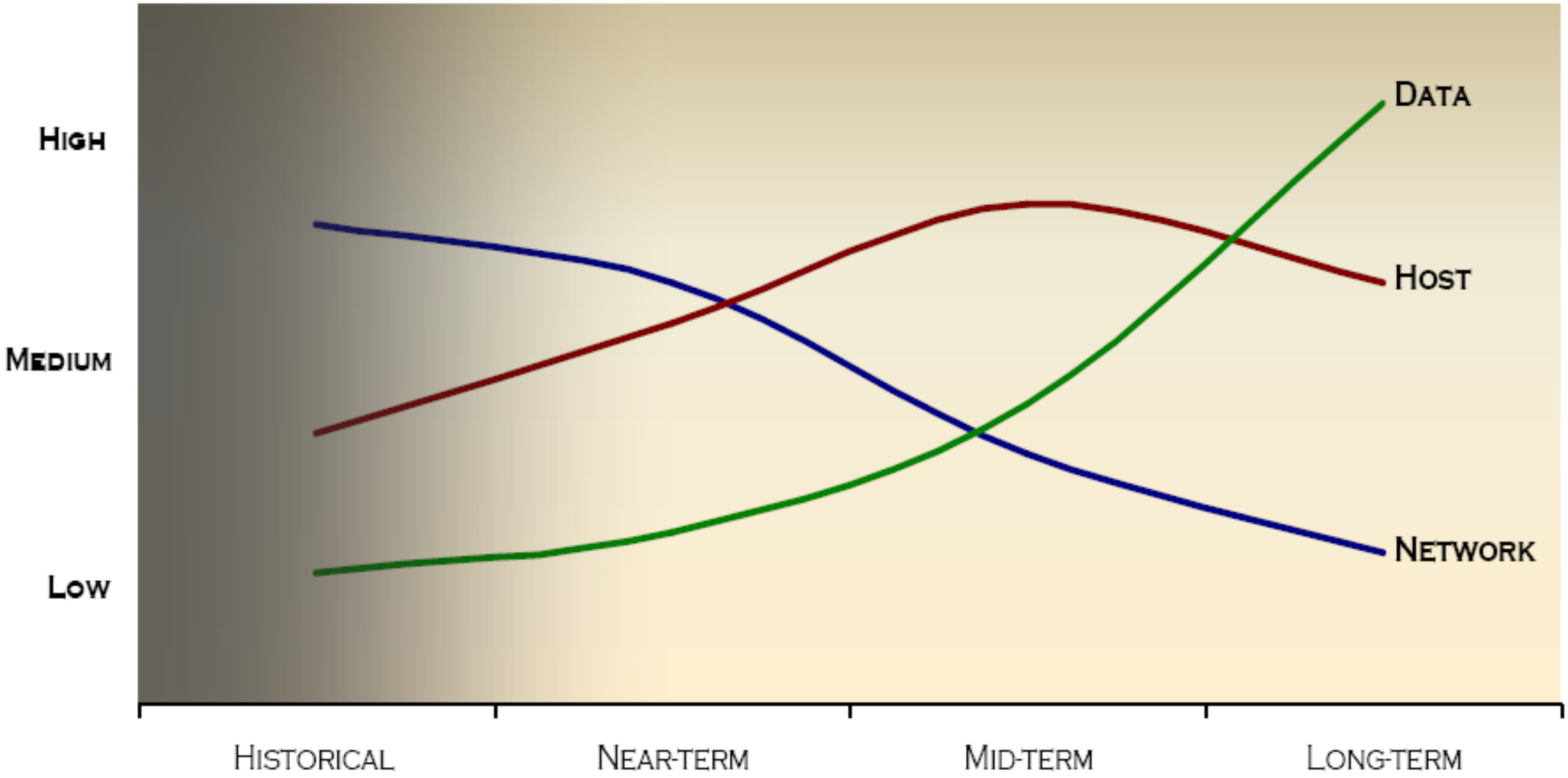
… and our border?

This is what we fool ourselves into thinking we deliver

But at best - this is what we actually deliver



Evolution of Information Security Technology

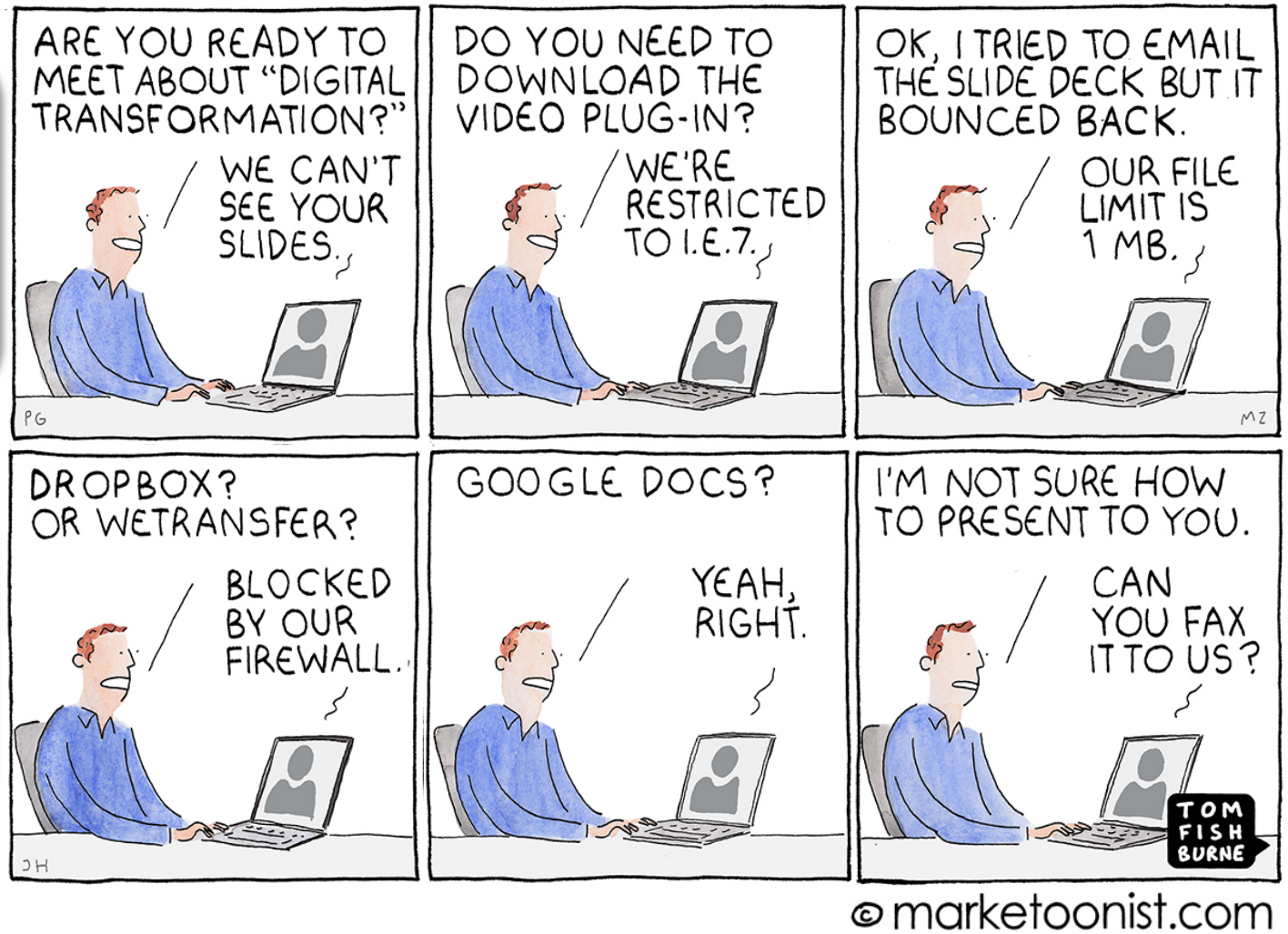


Source: Dan Hitchcock
https://movetheworld.files.wordpress.com/2008/01/evolutionofinformationsecuritytechnologies.pdf

And this is how the business see us . . .

"Digital Transformation is about collaboration"

"But YOU stop us from working effectively"



"How do I collaborate with what my partners are using?"

"It works just fine from my home PC"

Right problem, wrong solution

Symantec.

Enabling location awareness for a client

HOWTO81170

June 21st, 2018

https://www.symantec.com/docs/HOWTO81170

Technical Support

Support / Enabling location awareness for a client

Description

To make the policies that are assigned to clients contingent on the client's connection location, you can enable location awareness for the client.

If you check **Remember the last location**, then when a client connects to the network, it is assigned the policy from the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the client can manually switch between any of the locations even when it is under server control. If a quarantine location is enabled, the client may switch to the quarantine policy after a few seconds.

If you uncheck **Remember the last location**, then when a client connects to the network, it is assigned the policy from the default location. The client cannot connect to the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the user can manually switch between any of the locations even when the client is under server control. If a quarantine location is enabled, the client may switch to the Quarantine Policy after a few seconds.

To enable location awareness for a client

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to implement automatic switching of locations.

- We need to run insecure protocols on the Intranet
- We've made it secure, but ..... let's downgrade the security when "inside" the Intranet!
- D'oh!

RSAConference2019

What Zero Trust is not

. . . and what it may be

What Zero Trust is not . . .

- About “trusting no one”
- A “next-generation perimeter”
- And certainly not “VPN modernization”
- An off-the-shelf product
- An IT-only project
- A one-off project
- About eliminating your Intranet (but could be!)

What Zero Trust should be in your organization . . .

- A business ENABLER!
- An (architectural) state of mind
- When there is no (security) difference between the Internet and Intranet
- A combination of processes and technologies
- Reduced complexity
- A unified experience - greater flexibility and productivity for staff and partners

RSAConference2019

Reacting to a Zero Trust strategy

Zero Trust: Network

- There is no “DMZ” or “VPN” anymore: no security perimeter
- The “Intranet” may be retained for QoS (but not security)
- It’s application and user-centric, not infrastructure-centric: dynamic, evolving
- All network sessions must have authentication and authorization
- Enforce the network to only allow encrypted protocols
- There is more than one way to implement it:
  - Network Micro-segmentation (lots of tiny firewalls)
  - Software-Defined Perimeter (lots of tiny VPN tunnels)
  - Identity-Aware Proxy (next-gen Web Access Management)

  And you’ll probably end up using all of these

Zero Trust: Legacy

- Identifying legacy will be key to any Zero Trust transformation
- Once identified then have a strategy for dealing with it:
  - Plan to replace it
  - Upgrade it
  - Put it on a totally isolated network
  - Isolate it (possibly using Network Micro-segmentation)
  - Use an identity aware firewall
  - Encapsulate insecure protocols
  - Use a data-diode

  Or some mix of all the above!

Zero Trust: Access Management

- Least Privilege
  - every access limited to a specific user, device, and app or resource only
- Centralized
  - policies are standardized across common IT systems
  - policies are defined by the business (with the support of IT)
- Dynamic
  - access decisions are made in real-time
  - common requirements, individual attributes and context influence each decision
- Adaptive
  - open to support new authentication methods
  - constantly evolving, reacting to environment changes (machine learning, AI, etc.)

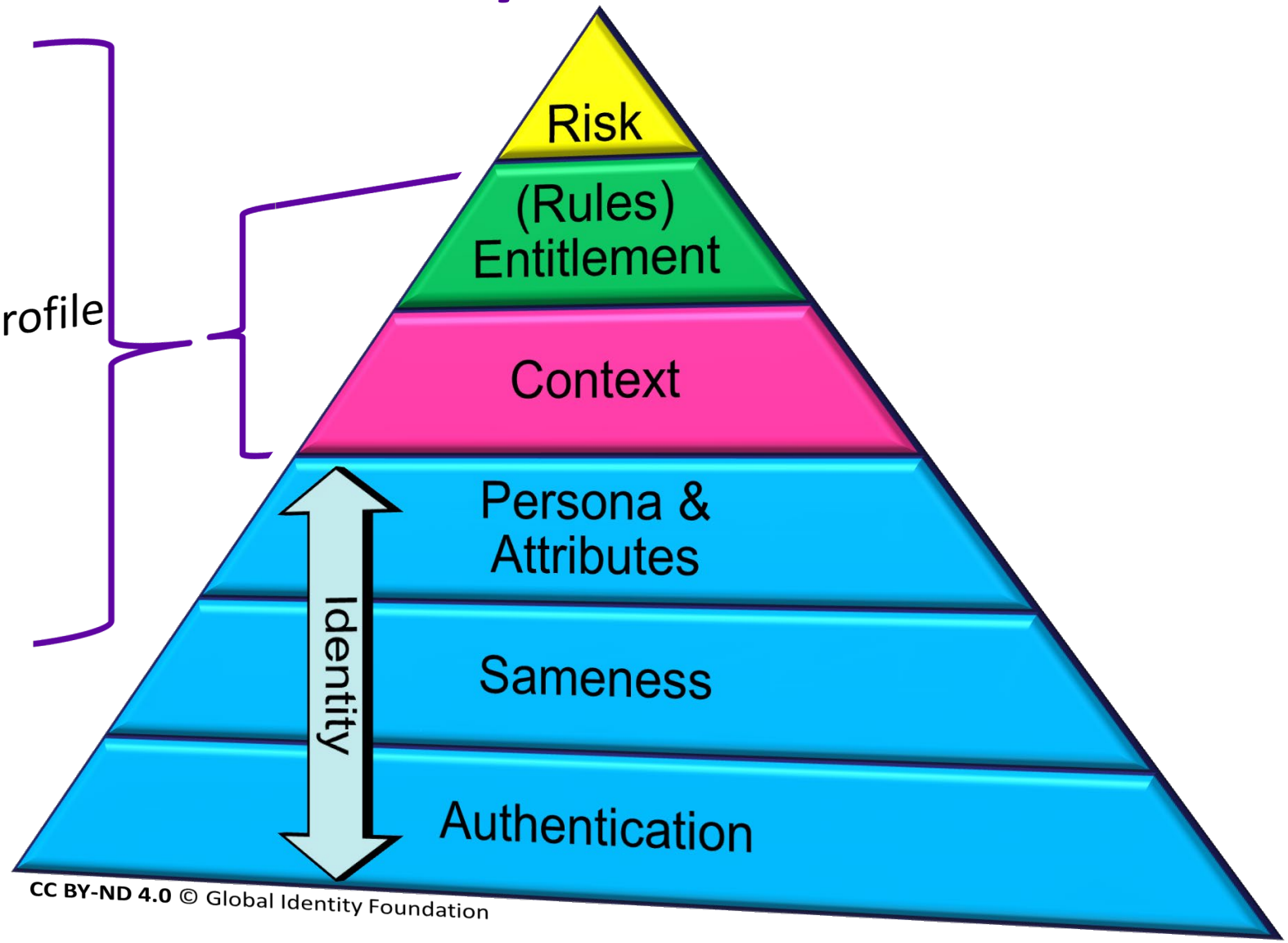
Zero Trust: Data

- Asset Discovery
  - You cannot protect what you don't even know exists
- Data Discovery & Classification
  - Not all data is created equal, and every organization has its own data taxonomy
- Data Flows
  - Identifying sensitive data flows & protocols between apps, users, external parties, frenemies, partners & the devices is the foundation for securing them
- Data Protection
  - All sensitive data must be encrypted at rest and in transfer [and preferably in processing – but that's a whole separate talk . . . .]

Zero Trust: Identity - CONTEXT is key

External Information

- Geo-spatial Location
- Geo-network Location
- Historic transaction info.
- Normative transactional profile
- Code-base trust-level
- Code-execution trust
- Device identity trust
- Organization identities
- Transaction risk level

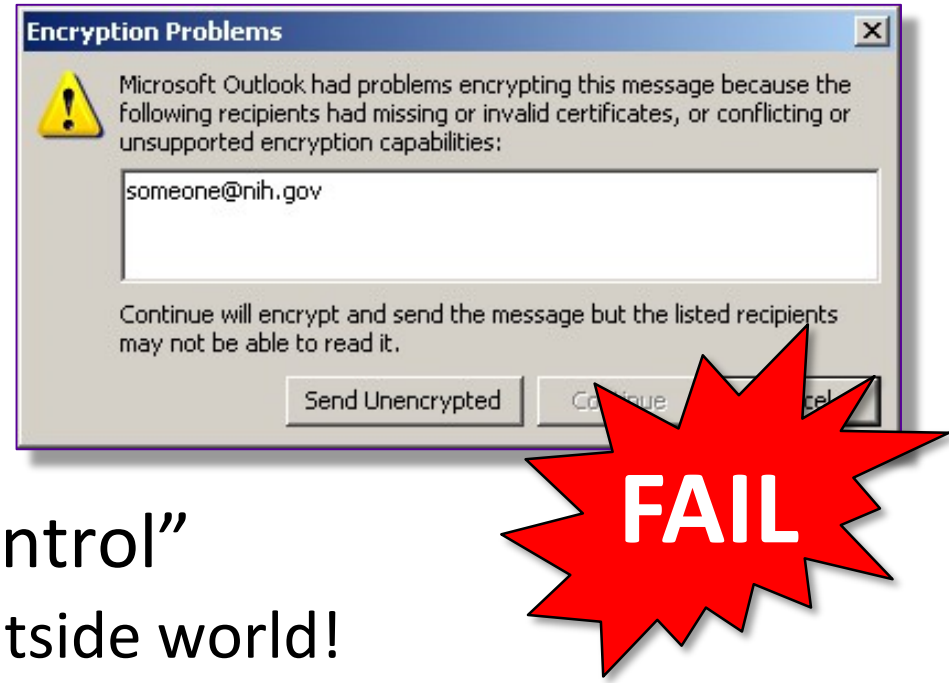


What strategies should I employ?

- Always start with a long-term, business-driven strategy
- “Rip and replace”: sounds good, doesn’t work
- Think beyond security, focus on business enablers
  - Reduction of infrastructure complexity
  - Hybrid-cloud ready
  - Enterprise mobility
  - Compliance
- Identify your key assets and biggest risks (don’t leave this to IT)
- Do not expect to achieve the goal in one step (or ever)
- Reuse and incorporate existing security, monitoring, orchestration tools

Zero Trust: Data

- Adopt the principle of Least Privilege
  - Data access should be limited to a specific user, device, and app or resource only
  - Think who/what needs access
    - then work out how to limit the access
- Contextual Access Control
  - Data access policies must be defined by the business (with the support of IT)
  - Access decisions should be made in real-time
- It must operate outside of your "locus of control"
  - Because businesses need to interact with the outside world!

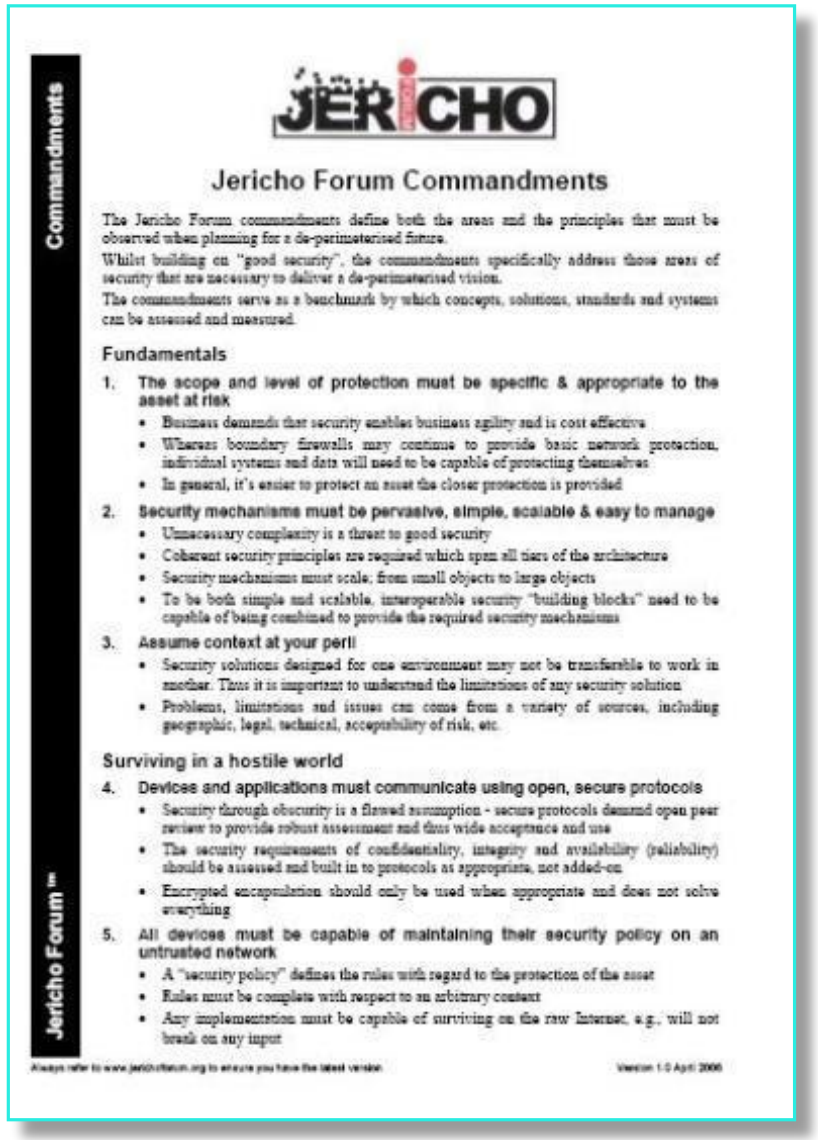


Get back to fundamentals

- Use only inherently secure protocols - JF#4
- Design for the Internet - JF#5
- Base your access control on multiple trust attributes (not just “user”) – JF#6
- Ensure data is secure by default – JF#11

Stretch goal;

- Be able to use trust attributes from outside of your “locus-of-control” – JF#8



Commandments

JERICHO

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on “good security”, the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

1. **The scope and level of protection must be specific & appropriate to the asset at risk**
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it’s easier to protect an asset the closer protection is provided
2. **Security mechanisms must be pervasive, simple, scalable & easy to manage**
   - Unnecessary complexity is a threat to good security
   - Coherent security principles are required which span all tiers of the architecture
   - Security mechanisms must scale; from small objects to large objects
   - To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms
3. **Assume context at your peril**
   - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
   - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

4. **Devices and applications must communicate using open, secure protocols**
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
   - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. **All devices must be capable of maintaining their security policy on an untrusted network**
   - A “security policy” defines the rules with regard to the protection of the asset
   - Rules must be complete with respect to an arbitrary content
   - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Jericho Forum™

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

RSAConference2019

What you should be doing when you go back to work

Summary

- “Zero Trust” is an (architectural) state of mind
- “Zero Trust” is not a product solution you can buy!

- There are quick wins, as well as long term strategy!
- You need to align security architecture with business strategy!

- Design for “Internet” and implement on the Intranet & Internet!

Easy wins . . .

- Simple strategy
  - Move to HTML5 delivered applications
  - Mandate those apps must deliver over HTTPS
- Only fight battles big enough to matter
  - Find and eliminate insecure protocols
  - Improve processes around user identity
- Only fight battles small enough to win
  - Only argue for change at a major upgrade or replacement
  - If PC/Windows/AD add device certificates (and leverage them . . .)

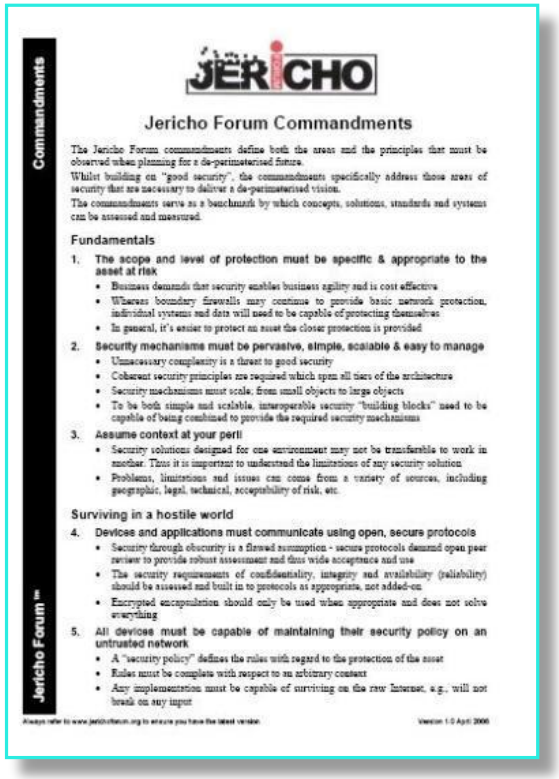
Apply What You Have Learned Today

- Next week you should:
  - Plan how you can identity all your devices and their locations
  - Develop an Internet mentality for your Intranet
- In three months following this presentation you should:
  - Have talked to the business to understand their strategy and needs
  - Understand and have plans / solutions for your legacy
  - Have a roadmap to eliminate insecure protocol
  - Worked with IT to understand the refresh strategy
  - Worked with purchasing to get a “heads-up” new systems

Apply What You Have Learned Today

- Within six months you should:
  - Have aligned medium term business strategy with a security strategy
  - Worked with business to provide ROI costing to drive security enablement
  - Develop a series of “cookie-cutter” approaches that people support
- Longer term
  - Work with business to ensure all new (and upgraded) systems use a “Zero Trust” or “De-perimeterized” approach to security
  - Develop metrics to demonstrate increased security and ROI

Free Resources & Further Reading



JERICHO FORUM

Commandments

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

1. The scope and level of protection must be specific & appropriate to the asset at risk
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect an asset the closer protection is provided
2. Security mechanisms must be pervasive, simple, scalable & easy to manage
   - Unnecessary complexity is a threat to good security
   - Coherent security principles are required which span all tiers of the architecture
   - Security mechanisms must scale, from small objects to large objects
   - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
3. Assume context at your peril
   - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
   - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

4. Devices and applications must communicate using open, secure protocols
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
   - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. All devices must be capable of maintaining their security policy on an untrusted network
   - A "security policy" defines the rules with regard to the protection of the asset
   - Rules must be complete with respect to an arbitrary context
   - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Jericho Forum ™

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.0 April 2006

Jericho Forum Commandments

BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. roryward@google.com

Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

While most enterprises assume that the internal network is a safe environment in which to expose corporate applications, Google's experience has proven that this faith is misplaced. Rather, one should assume that an internal network is as fraught with danger as the public Internet and build enterprise applications based upon this assumption.

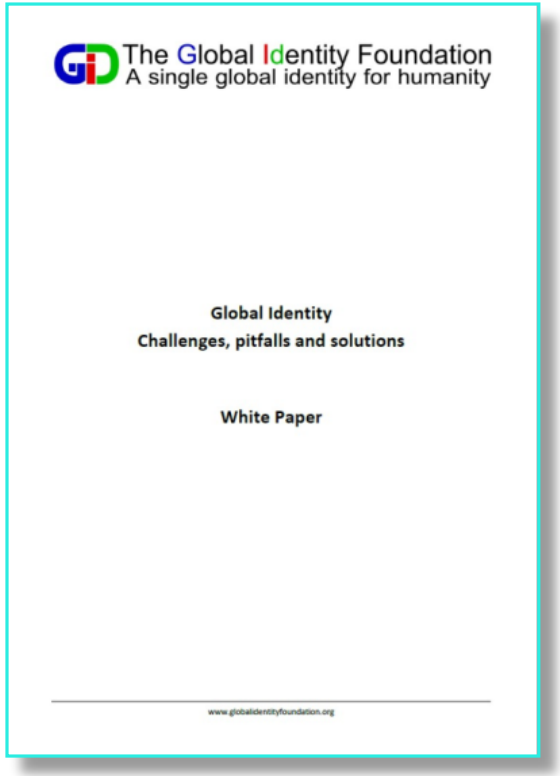
Google's BeyondCorp initiative is moving to a new model that dispenses with a privileged corporate network. Instead, access depends solely on device and user credentials, regardless of a user's network location—be it an enterprise location, a home network, or a hotel or coffee shop. All access to enterprise resources is fully authenticated, fully authorized, and fully encrypted based upon device state and user credentials. We can enforce fine-grained access to different parts of enterprise resources. As a result, all Google employees can work successfully from any network, and without the need for a traditional VPN connection into the privileged network. The user experience between local and remote access to enterprise resources is effectively identical, apart from potential differences in latency.

The Major Components of BeyondCorp

BeyondCorp consists of many cooperating components to ensure that only appropriately authenticated devices and users are authorized to access the requisite enterprise applications. Each component is described below (see Figure 1).

6 ;login: DECEMBER 2014 VOL. 39, NO. 6 www.usenix.org

Google BeyondCorp



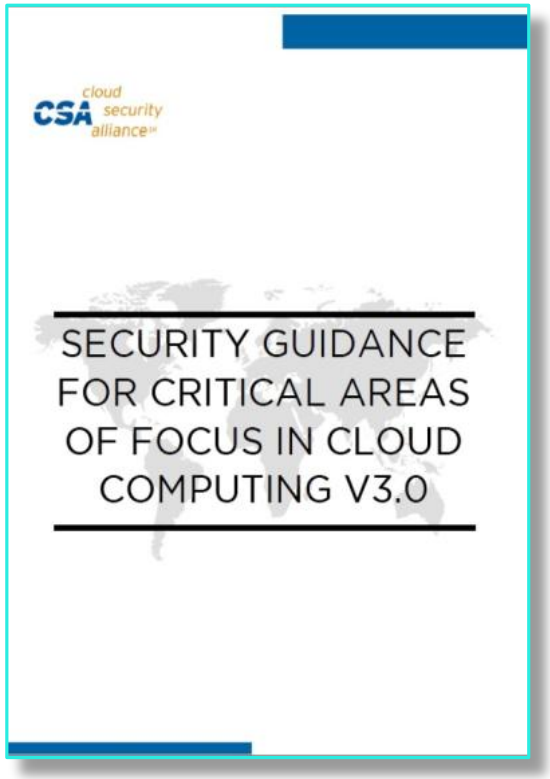
The Global Identity Foundation
A single global identity for humanity

Global Identity
Challenges, pitfalls and solutions

White Paper

www.globalidentityfoundation.org

Global Identity – "Challenges Pitfalls & Solution"



CSA cloud security alliance

SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

CSA Guidelines

***All freely available**: Use Google; or linked at: www.globalidentityfoundation.org*

Questions

Questions & Comment

omments

Questions & Comments

Questions & Commen

ions & Comments