cloud security alliance®

ZERO TRUST Advancement Center

Demystifying Zero Trust

For the C-Level (and the rest of us)

PRESENTED BY

cloud security alliance®

Paul Simmonds

Director, CSA (Europe) & CEO, Global Identity Foundation

Agenda

1 What is Zero Trust (and what it should be)?

2 Let's talk about "risk"

3 (Not) Communicating Zero Trust to the Board

4 Your Zero Trust "sanity" check-list (things to think about)

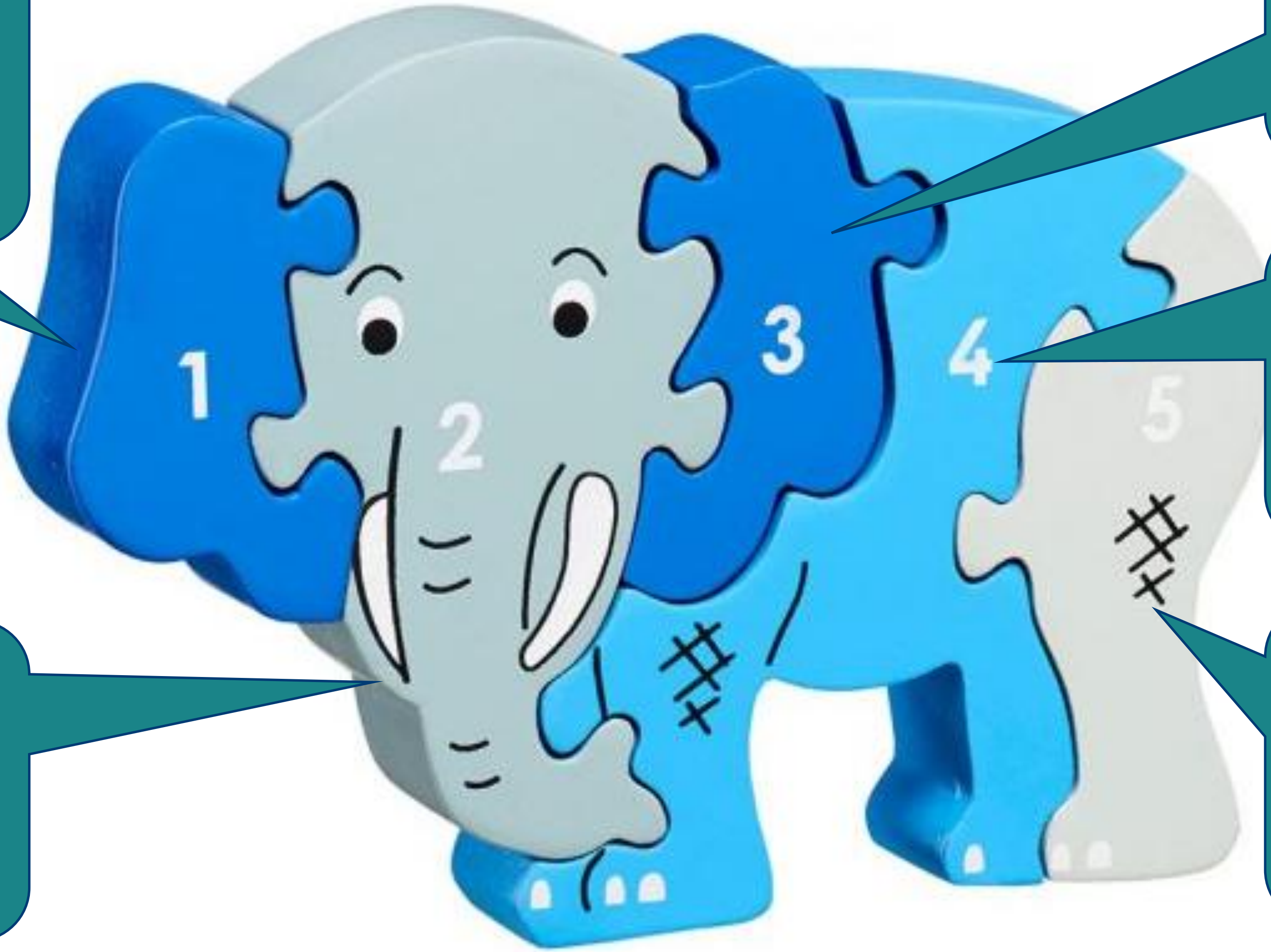
Lets start with . . .

A parable!

Public Domain, https://commons.wikimedia.org/w/index.php?curid=4581243

I'm a network security engineer
the solution to ZT is …
a Software Defined Perimeter

I'm a desktop security specialist
the solution to ZT is …
a hardened endpoint



I'm an identity specialist
the solution to ZT is …
an IAM solution

I'm web specialist
the solution to ZT is …
cloud access security broker (CASB)

I'm a cloud specialist
the solution to ZT is …
everything outsourced to SAAS

Elephant © www.lankakade.co.uk

Castle & Moat Security Inc
Our old technology product
Now with added "Zero Trust"
"We couldn't make it work in our existing network, so what chance do we have with 'Zero Trust'?"
FTSE 100 CISO

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

Zero Trust & Vendor PR?

So many vendors, so many "Zero Trust" products!

So many vendors selling you "Zero Trust"

- 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

So it's important you select your Zero Trust products & solutions with care!

Zero Trust – A History

From hardened perimeter to evaluate risk and work anywhere

Time

1990's

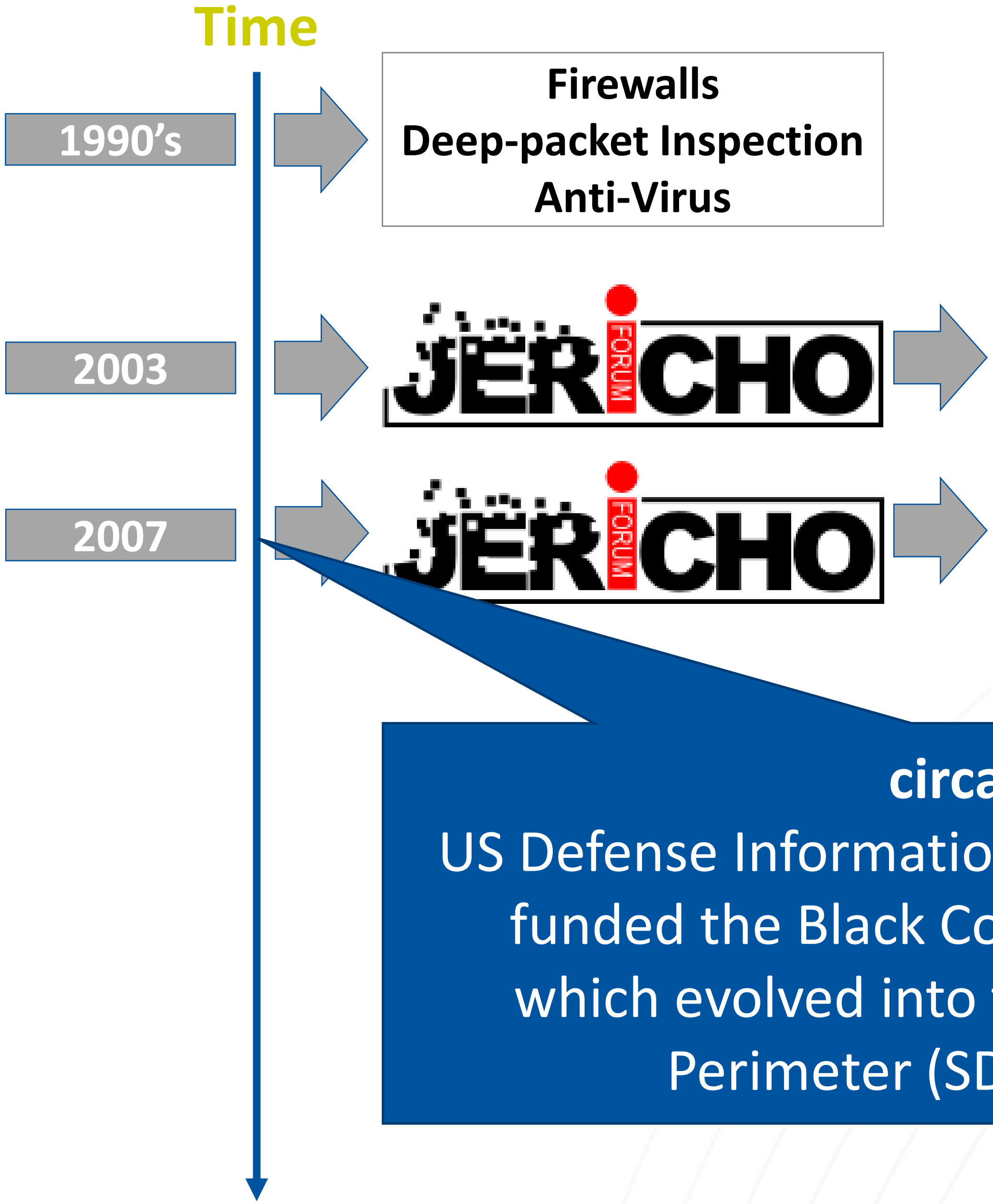
Firewalls
Deep-packet Inspection
Anti-Virus

1994

The term "Zero Trust" was coined within Stephen Paul Marsh's PhD thesis "Formalizing trust as a computational concept"

Zero Trust – A History

From hardened perimeter to evaluate risk and work anywhere



Firewalls
Deep-packet Inspection
Anti-Virus

De-perimeterisation & the Jericho Forum "Commandments"

- The firewall has limited use as a security boundary, and it's only getting worse
- Hard borders are inhibiting business and business strategy

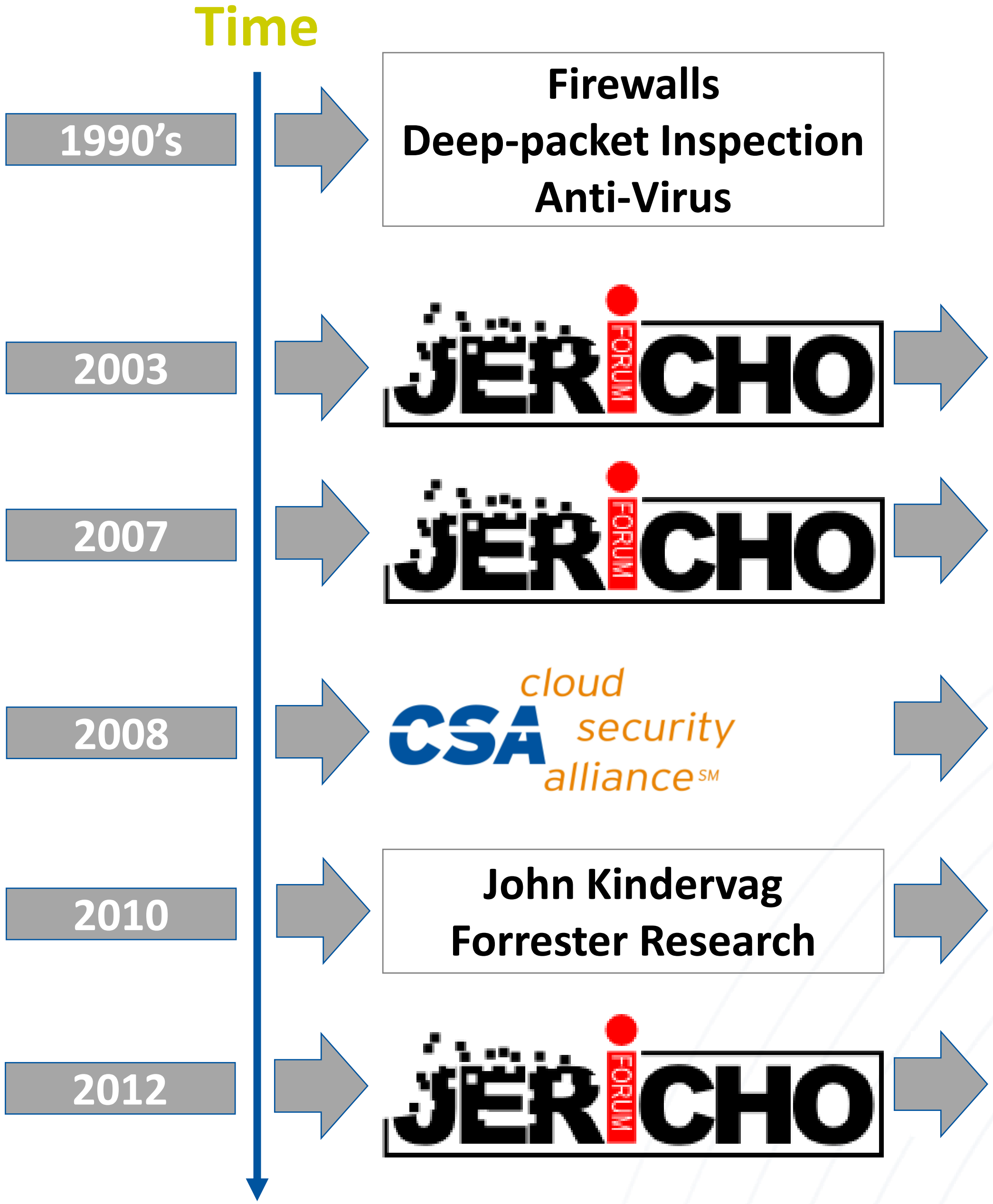
Computing outside of your perimeter

- If your border is irrelevant, then you can outsource your computing servers
- Developed the "Cloud Cube" model for "cloud" outsourcing

circa-2007
US Defense Information Systems Agency (DISA) funded the Black Core Network initiative; which evolved into the Software-Defined Perimeter (SDP) framework"

Zero Trust – A History

From hardened perimeter to evaluate risk and work anywhere



De-perimeterisation & the Jericho Forum "Commandments"

- The firewall has limited use as a security boundary, and it's only getting worse
- Hard borders are inhibiting business and business strategy

Computing outside of your perimeter

- If your border is irrelevant, then you can outsource your computing servers
- Developed the "Cloud Cube" model for "cloud" outsourcing

How do you secure "Cloud Computing"

- Ingested Jericho Forum concept work on "computing outside your perimeter"
- Developed the "Guidance" documents, based on industry best practice

Zero Trust Network Architecture

- Presented a document called "Zero Trust Network Architecture"
- Proposed "Segmented, Parallelized, and Centralized" internal networks

Jericho Forum "Identity Commandments"

- Consume trusted identity and attributes to drive "entitlement"
- Ensure the entity taking the risk fully understands the risk of all components

2003 “De-Perimeterisation”	2010 “Zero Trust Networking”	2017 “Zero Trust”
● The scope and level of protection should be specific & appropriate to the asset at risk ● Security mechanisms must be pervasive, simple, scalable & easy to manage ● Devices and applications must communicate using open, secure protocols ● All devices must be capable of maintaining their security policy on an untrusted network	● "We have to know what's going on in our networks, Users can't have willy-nilly access” ● [Proposes] a network segmentation gateway. "It's like a UTM [unified threat management] tool or firewall on steroids" ● [Proposes] “Segmented, Parallelized, and Centralized” internal networks	● “We no longer determine who you are based on your IP address” ● “We treat every network in the world as untrusted; Whether it’s physically inside our building, [or] whether you’re at a Starbucks”
Jericho Forum “Commandments”	*John Kindervag Forrester paper “Zero Trust Network Architecture”*	*Heather Adkins, Director of Information Security Google*

[1] https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf
[2] https://www.darkreading.com/perimeter/forrester-pushes-zero-trust-model-for-security
[3] https://www.youtube.com/watch?v=d90Ov6QM1jE

So what is "Zero Trust"?

Is it?

- Strategy?
- Design Principles?
- Architecture?
- Products?

Zero Trust is an overarching **security philosophy**

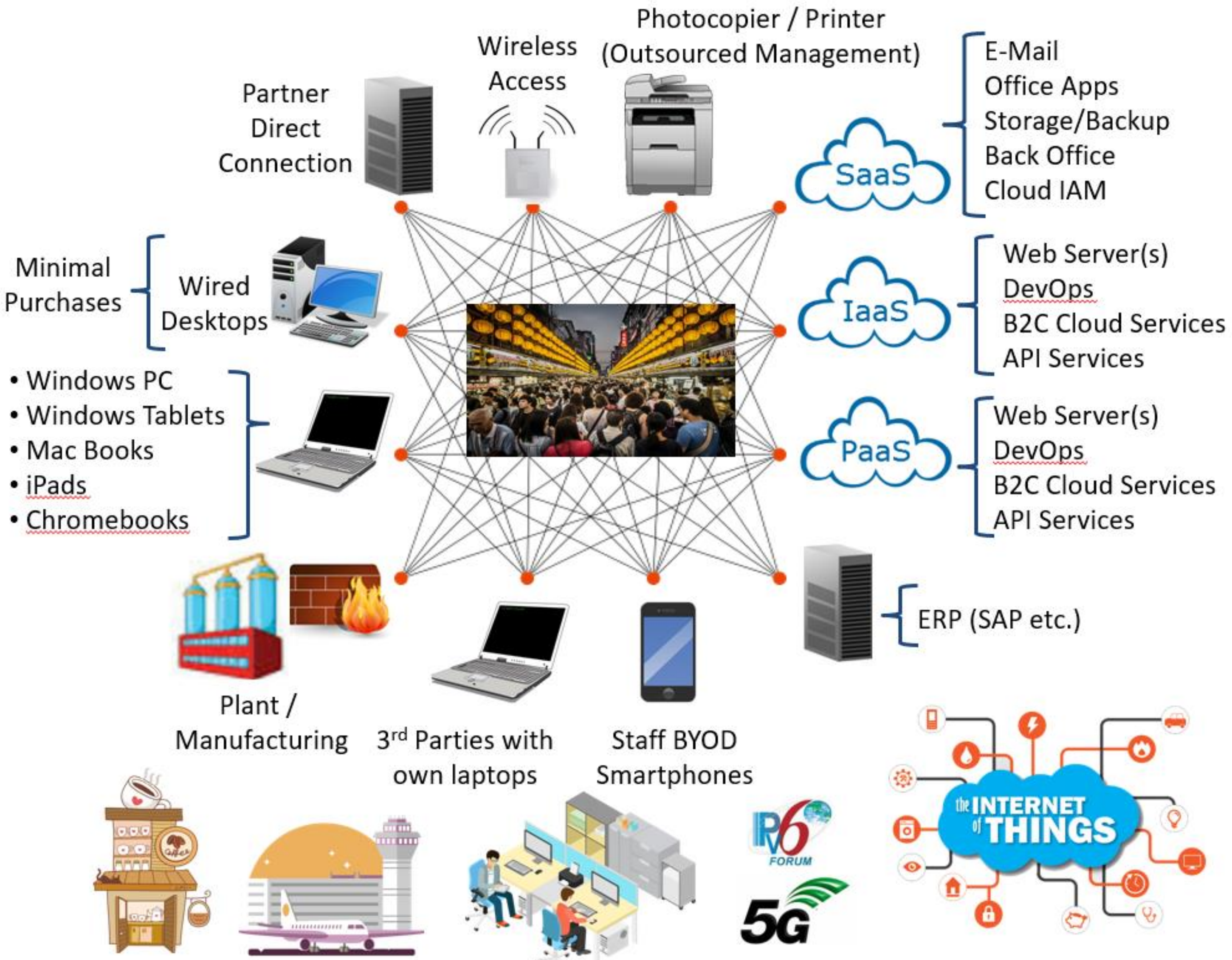
Zero Trust as a philosophy

It's delivering business flexibility for todays modern business

Replacing "trust in the network" with;

- Trust inferred from devices, users, organisations and end-point trust agents
- An "entitlement" decision about access to data and to devices, whatever the location
- Network control (where still required) based on entitlement using technologies such as SDN

And in some cases, no corporate network whatsoever!



So what is “Zero Trust”?

Is it?

- Strategy?
- Design Principles?
- Architecture?
- Products?

Zero Trust is an overarching **security philosophy**

Dictating that any/all access requests to systems or data should be **risk-based** and start from a position of zero trust

Agenda

1. What is Zero Trust (and what it should be)?

2. ***Let’s talk about “risk”***

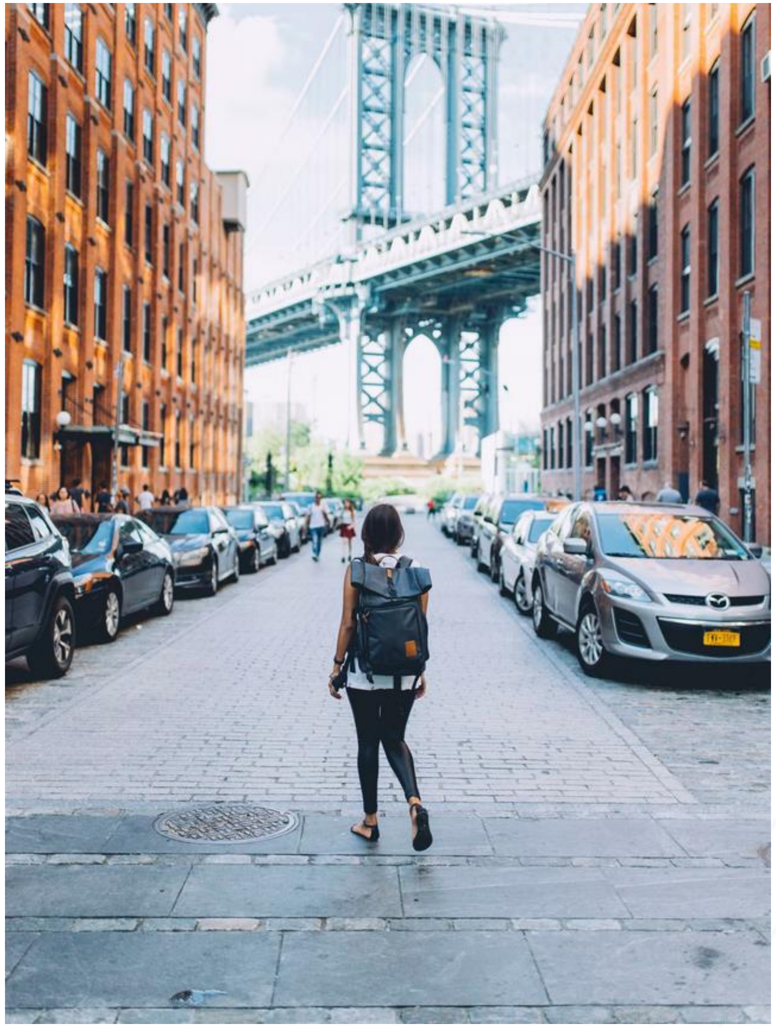
3. (Not) Communicating Zero Trust to the Board

4. Your Zero Trust “sanity” check-list (things to think about)

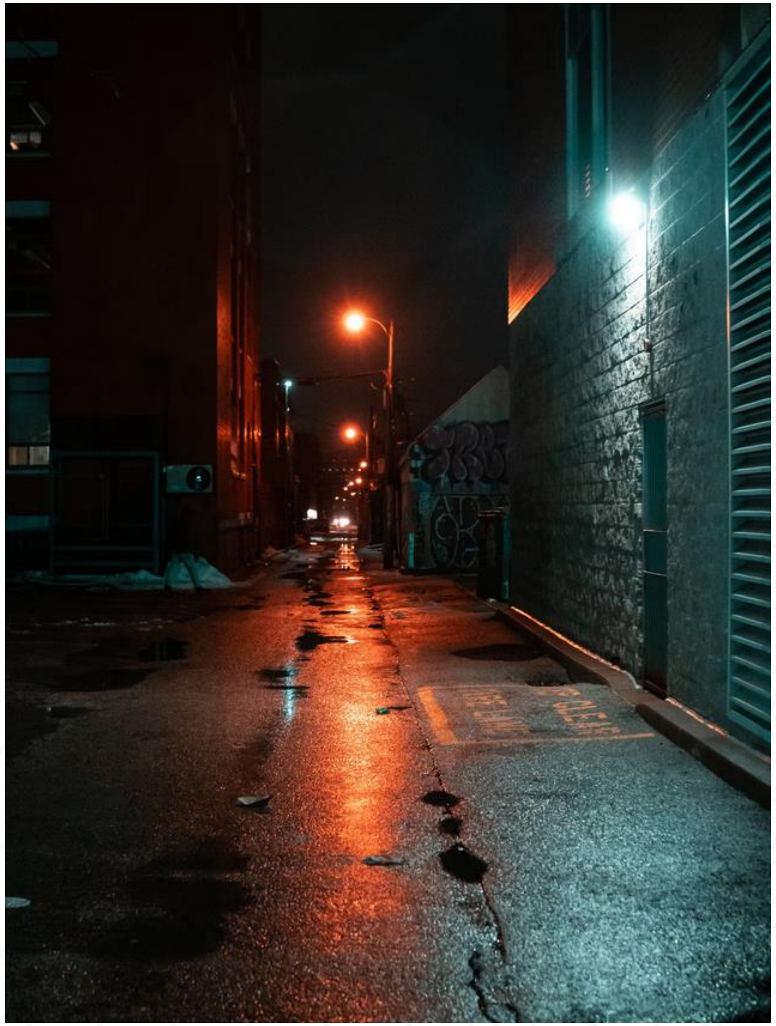
Risk

Risk = Impact ($) x Probability (%)

Risk, environment & context



Source: Unsplash – Brevitē (@brevite)



Source: Unsplash - Boden Deplaedt

Risk Equation:

- Who am I?
- Am I alone?
- Time of day?
- Alternative routes?
- Area history?
- Street lighting?
- Policing & presence?
- Am I a target?

Risk & Zero Trust

Risk is a contextual

How to we deal with risk?

1. Eliminated

You design it out

2. Mitigated

You add compensating controls

3. Transferred

Another party takes on the risk, e.g.; Insurance

4. Accepted

The risk remains as a cost of doing business

The entity taking the risk must be able to evaluate all Identity and Attribute information

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

“Entitlement”

Making a risk-based decision

★

About ***access to data*** and/or ***systems***

★

Based on the ***trusted identity*** and ***attributes***

★

Of ***all the entities*** and ***components***
in the transaction chain

Risk & Zero Trust

Risk must be a contextual decision!

Context

- Access to data
- Access to system
- Trusted identity (and level of trust)
- Attributes asserted (and level of trust)
- All the entities in the transaction chain
- All the components in the transaction chain
- *History*

Agenda

1 What is Zero Trust (and what it should be)?

2 Let’s talk about “risk”

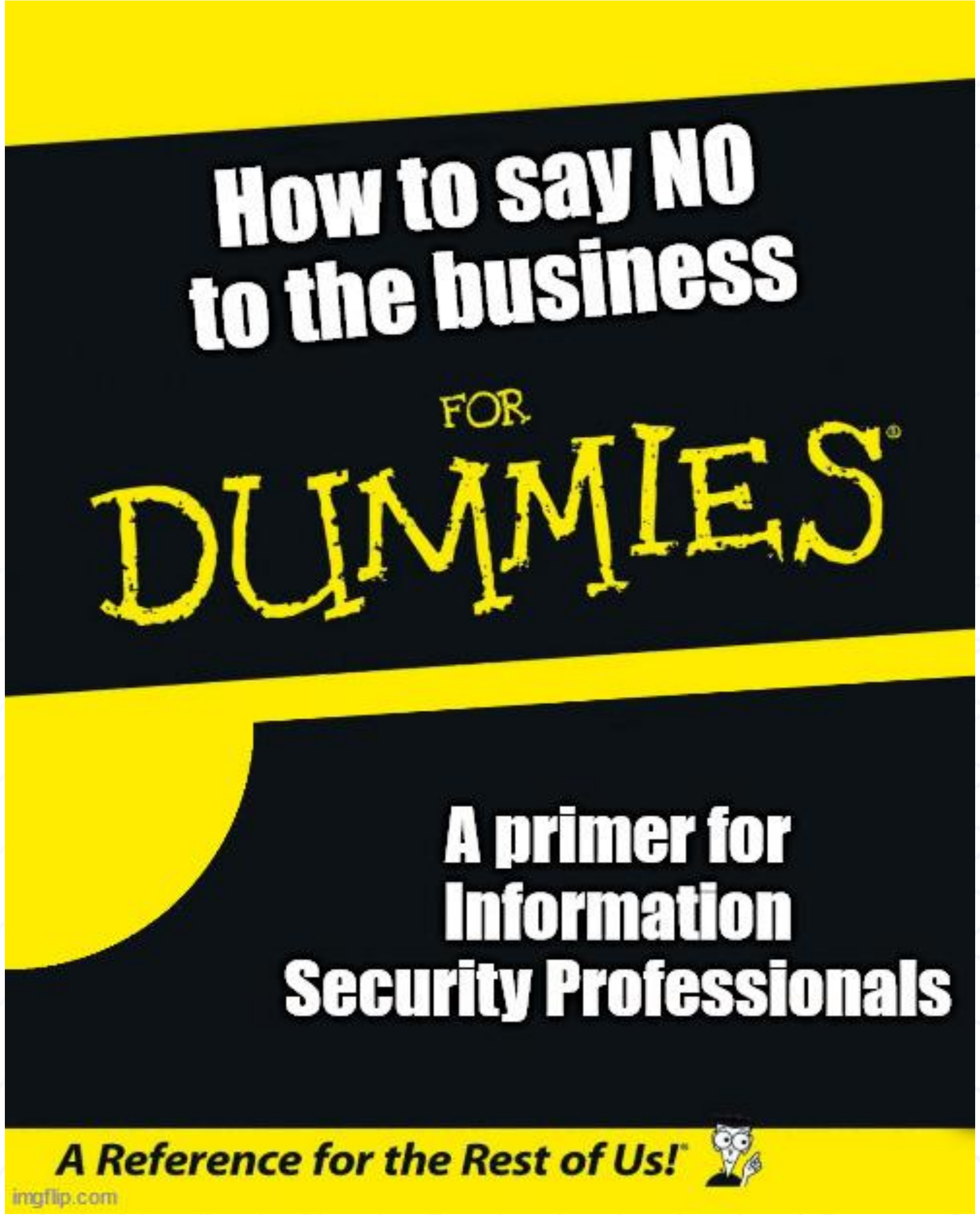
3 ***(Not) Communicating Zero Trust to the Board***

4 Your Zero Trust “sanity” check-list (things to think about)

Security & IT inhibit the business

Proof:

- The rise of shadow IT
- Security a top 5 priority
  Yet no board level CISO’s
  and rarely any CIO’s
- Outsourcing of IT functions
  Seen to be a commodity
- Rarely consulted on strategic decisions
- Resulting in a rear-guard action
- And thus are perceived as saying “no”


How to say NO to the business
FOR
DUMMIES
A primer for Information Security Professionals
A Reference for the Rest of Us!
imgflip.com

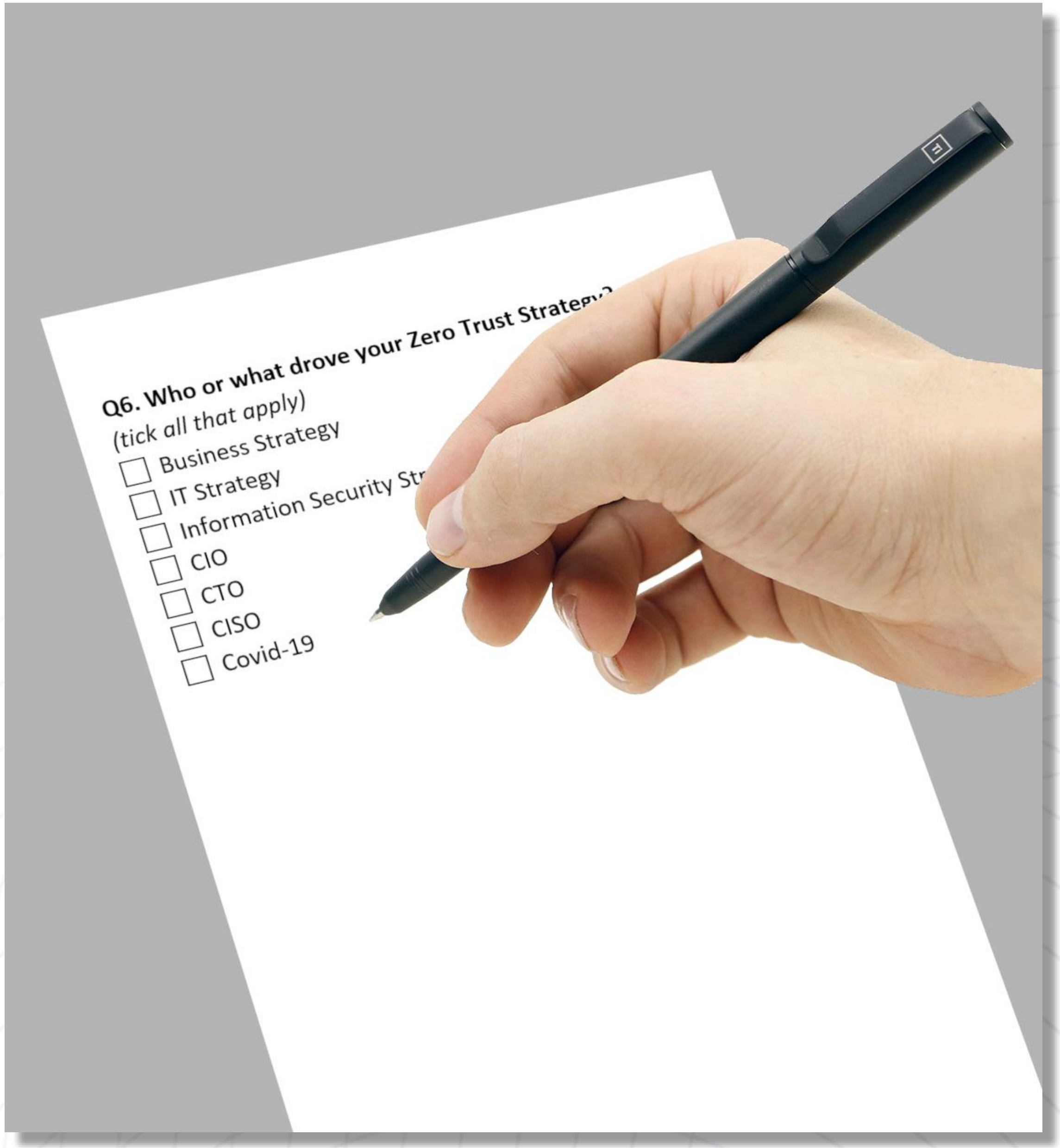
The pandemic re-enforced the stereotype

We made it work for the business

And the sky did not fall down ….

If fact (in many cases) it worked better

So now explain why you need $$$$$ for Zero Trust?



Q6. Who or what drove your Zero Trust Strategy?

(tick all that apply)

□ Business Strategy
□ IT Strategy
□ Information Security Str
□ CIO
□ CTO
□ CISO
□ Covid-19

www.time.com/asia JANUARY 18, 1999

TIME

THE END OF THE WORLD !?!

Y2K insanity! Apocalypse Now! Will computers melt down? Will society? A guide to MILLENNIUM MADNESS

PANIC
DONT
PANIC
LENNIUM CLOCK
DOWN TO THE YEAR

Jan. 18, 1999, cover of TIME

What everyone should know about the Millennium Bug

FACTS NOT FICTION

About the bug 1
At home 3
Business as usual 5
Personal computing 6
Services to the home 7
Personal finance 9
Health 11
Emergency services 13
Shops and service stations 15
Your local area 17
Travelling overseas 19
International 21

Keep this booklet for future reference

Published by HM Government

UK Government

So what do the board care about?

- **Faster**
- **Better**
- **Cheaper**

Justified with quantifiable risk!

Aligned to business aims and objectives

Secure is YOUR job, and should be a given!

A Zero Trust "philosophy" is neither a technology, security, or an identity issue

Alignment to the busiess

Strategic alignment of the business roadmap & strategy with the technology needed to support it.

Do you understand what the strategic vision of the board / business is?

Delivering value to the business

How will it enable the business to:

- Move Faster
  (time to implement)
- Reduce Costs
  (return on investment)
- Be More Secure
  (but at no additional cost)

Zero Trust “themes” for the board

Agility

Enables the business to move, faster
Enables the use of new (cheaper) technologies for example, IoT, 5G, Cloud

Collaboration

Easier collaboration, especially with other organizations
(Partners, JV’s, Outsourced partnerships etc.)

Alignment

IT, Networking and Information Security (perceivably) better aligned to business need

Risk Reduction

Aligned with the boards risk-appetite

Focused on business-critical assets

A risk-based approach to securing assets

Agenda

1 What is Zero Trust (and what it should be)?

2 Let’s talk about “risk”

3 (Not) Communicating Zero Trust to the Board

4 ***Your Zero Trust “sanity” check-list (things to think about)***

Zero Trust; and things that make you go Aargh!

- Identity is the new perimeter
- Zero Trust is a network security concept
- You must install "my product" / solution / corporate standard
- All access must be authenticated
- Trust but verify
- Anything with a buzzword

Two critical flaws in architectural thinking

Binary Trust

A system (*refer to rule* 2)
authenticates the entity,
turning a "maybe" (a variable) into
a "certainty" (binary)

Rule 1
Never turn a variable into a binary

The "locus of control"

I can make it all work,
as long as EVERYTHING
plays in my system.

Rule 2

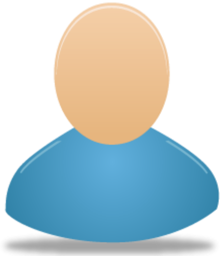
You must be able to trust
(*refer to Rule 1*)
entities that you do not manage

Questions to ask yourself?

- Am I enrolling entities I don't employ, manage or vet; into my Identity system?
- Can I support (real) BYOD?
- It my external auditors turn up needing access (for their laptops) can I simply give it to them?
- How do I set up a collaboration between ten disparate people / organizations?

Any ZT ecosystem must encompass all entity types

Entities enable context!



People

- Humans

Devices

- Computers
- Phones
- IoT
- Vehicles
- Printers
- PVR’s
- BYOD

Organizations

- Legal Organizations
- Families
- Organization Groupings

```
  post-<?php the_ID(
lass="entry-featured">
php x_featured_gallery(); ?>
div>
<div class="entry-wrap">
  <header class="entry-header">
    <?php if ( is_singular() ) : ?>
    <h1 class="h-entry"><?php the_title(); ?
    <?php else : ?>
    <h2 class="h-entry">
      <a href="<?php the_permalink(); ?>" tit
    </h2>
    <?php endif; ?>
    <?php x_integrity_entry_meta(); ?>
  </header>
  <?php if ( is_singular() ) : ?>
  <div class="entry-content">
    <?php the_content(); ?>
```

Code

- Code
- Executable Programs
- Self-Protecting Data
- DRM
- Signed Data

Agents

- Human agents
- Delegations
- AI Programs
- Learning programs

Risk & Context

(Flawed) binary trust implies flawed risk assessments

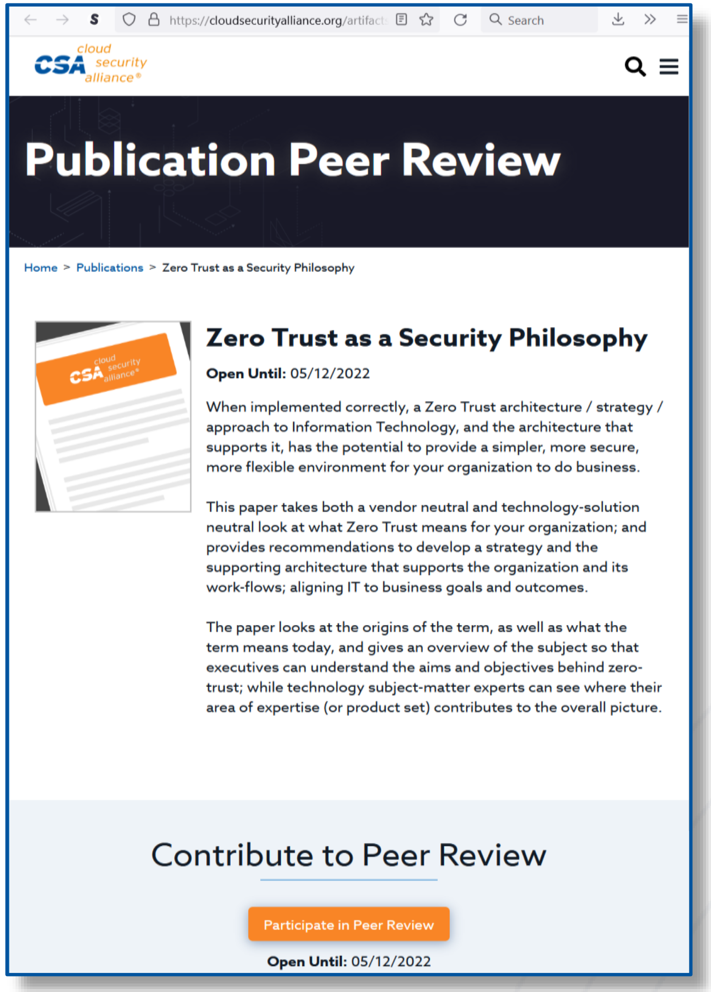
- "They are trusted because they are on the Intranet", or "They are who they claim to be because they (eventually) gave a correct password", or "they passed security vetting"

Risk, especially when moving to a more granular approach demanded by a Zero Trust architecture, must also be variable;

- Based on understanding all the entities involved (context), and;
- A situational understanding of what the entity is requesting, (additional context) and;
- Continually assessed as the context changes (temporal trust)

In conclusion

Have your say on the CSA document


https://cloudsecurityalliance.org/artifact
Search
Participate in Peer Review

Publication Peer Review

Home > Publications > Zero Trust as a Security Philosophy

Zero Trust as a Security Philosophy

Open Until: 05/12/2022

When implemented correctly, a Zero Trust architecture / strategy / approach to Information Technology, and the architecture that supports it, has the potential to provide a simpler, more secure, more flexible environment for your organization to do business.

This paper takes both a vendor neutral and technology-solution neutral look at what Zero Trust means for your organization; and provides recommendations to develop a strategy and the supporting architecture that supports the organization and its work-flows; aligning IT to business goals and outcomes.

The paper looks at the origins of the term, as well as what the term means today, and gives an overview of the subject so that executives can understand the aims and objectives behind zero-trust; while technology subject-matter experts can see where their area of expertise (or product set) contributes to the overall picture.

Contribute to Peer Review

Open Until: 05/12/2022

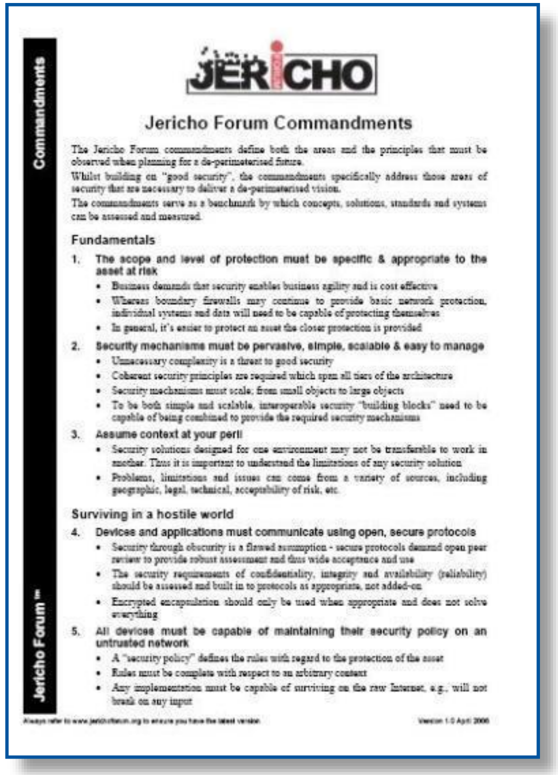
Zero Trust as a Security Philosophy

https://cloudsecurityalliance.org/artifacts/zero-trust-security-philosophy/

CSA Public Peer Reviews

https://cloudsecurityalliance.org/research/contribute#peer-reviews

Free Resources & Further Reading



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

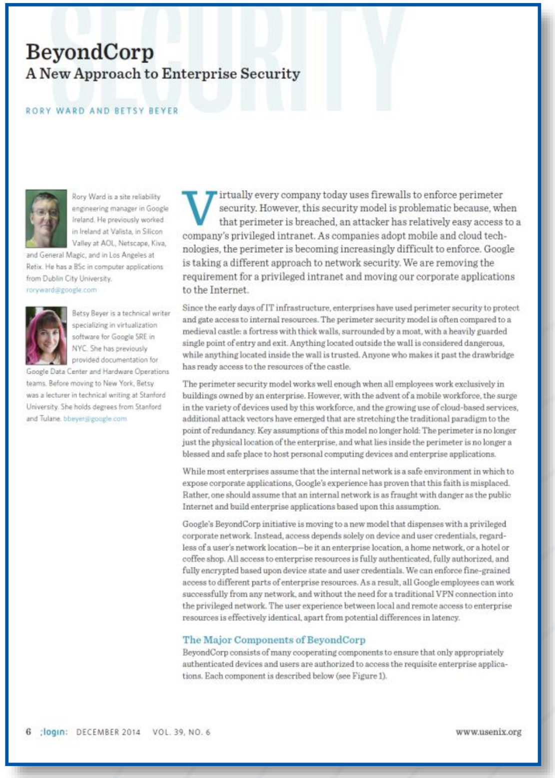
4. **Devices and applications must communicate using open, secure protocols**
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and 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



SECURITY

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.

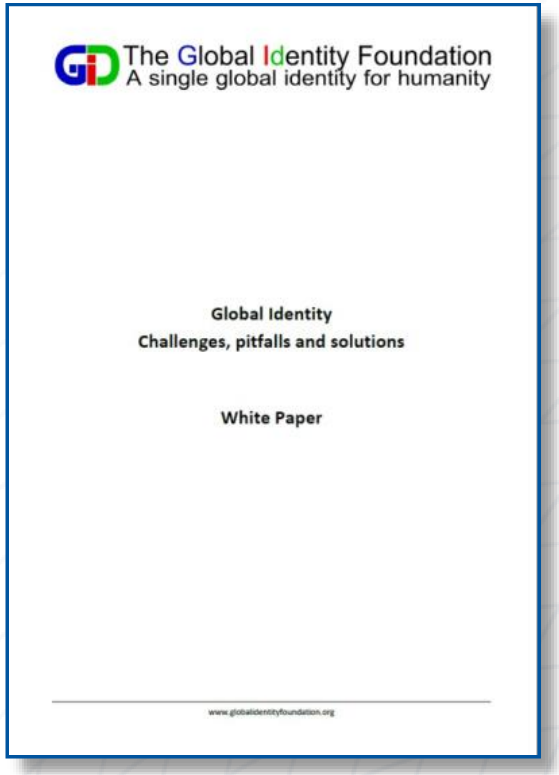
Google's BeyondCorp initiative is moving to a new model that dispenses with a privileged corporate network. Instead, access depends solely on device and user credentials, regardless of a user's network location—be it an enterprise location, a home network, or a hotel or coffee shop. All access to enterprise 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



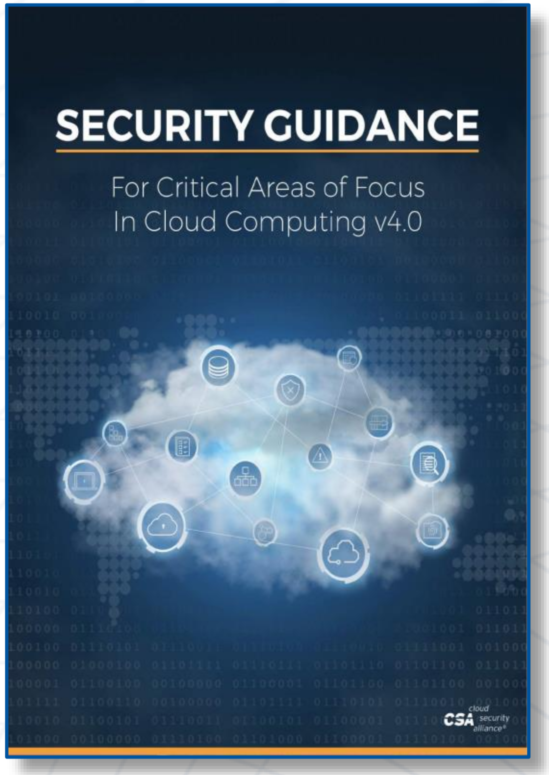
The Global Identity Foundation
A single global identity for humanity

Global Identity
Challenges, pitfalls and solutions

White Paper

www.globalidentityfoundation.org

Global Identity – "Challenges Pitfalls & Solution"



SECURITY GUIDANCE

For Critical Areas of Focus
In Cloud Computing v4.0

CSA cloud security alliance

CSA Guidelines

All freely available

Thank you!

Paul Simmonds

paul.simmonds@cloudsecurityalliance.org.uk

Twitter: @simmonds_paul

https://www.linkedin.com/in/psimmonds/