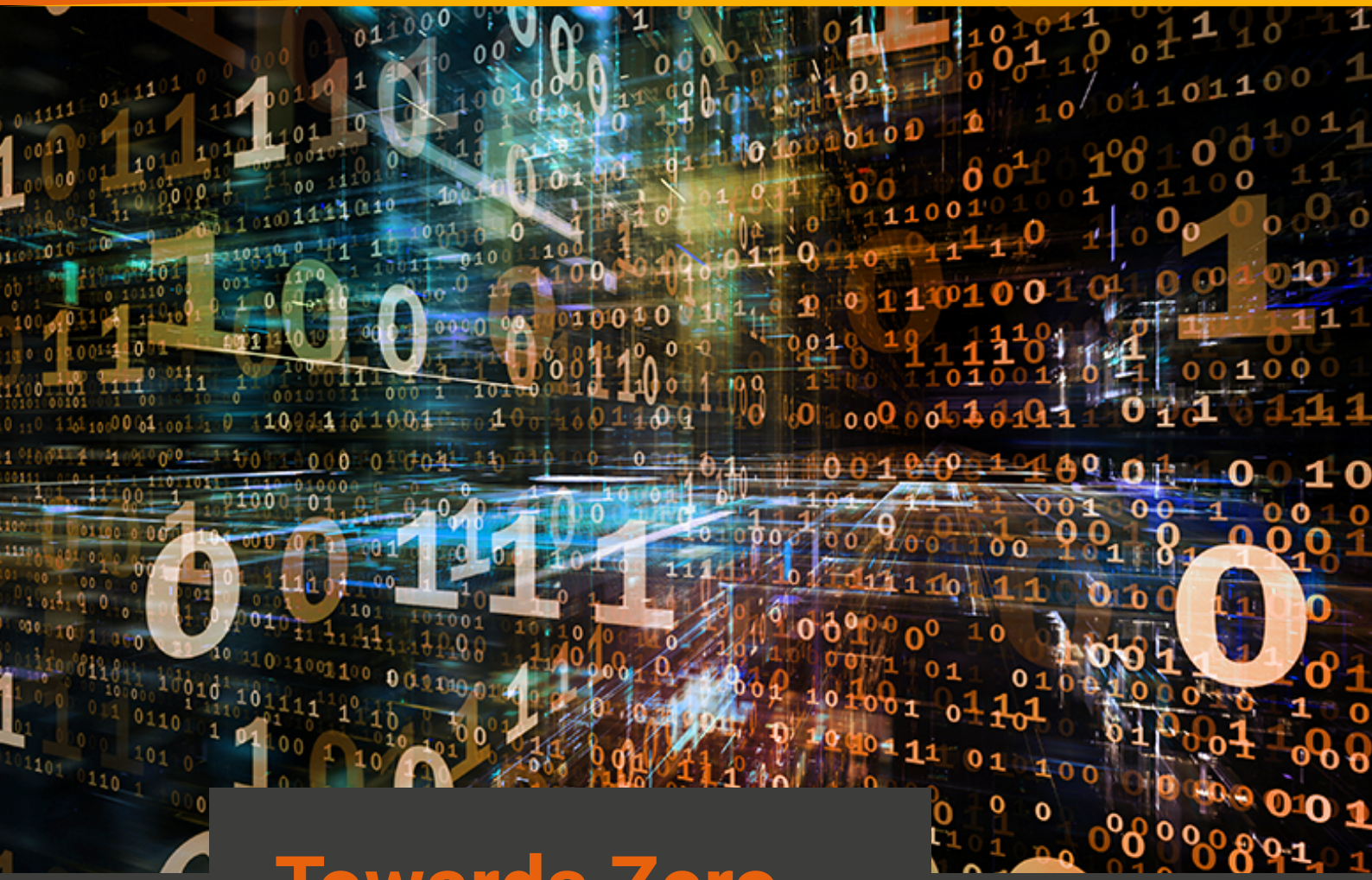
#becrypt



Towards Zero Trust

Approaching and Measuring Zero Trust Adoption

A Becrypt Whitepaper

Introduction - *It's all in the mind*

An organisation's journey towards Zero Trust is more about mind-set change than technology change. Zero Trust (ZT), according to NIST (US National Institute of Standards and Technology) [1], is

A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

ZT is the term for an evolving set of cybersecurity paradigms that move network defences from static, network-based perimeters to focus on users, assets, and resources. However, network perimeters do not themselves cause assets to be compromised. It is rather the often misplaced trust in the continued relevance and effectiveness of network perimeters where they exist.

Yet, as NIST highlight, many definitions of ZT stress the concept of removing wide-area perimeter defences (e.g. enterprise firewalls), while continuing to define themselves in relation to other, often smaller perimeters. This can lead to an over-emphasis on what should be absent when adopting ZT, as opposed to how existing environments may be augmented and evolved with new controls or architectures. This in turn may inhibit an organisation's adoption of ZT in the face of complex dependencies on existing legacy systems and applications.

Defining ZT

Consequently NIST attempt to define ZT and ZT Architectures (ZTA) in terms of basic tenets that should be involved, rather than what is excluded. ZTA forms the basis for a plan to implement ZT, and the tenets outlined below represent an ideal. In practice, not all tenets may be fully implemented in their purest form for a given strategy.

NIST Basic ZT tenets:

- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No asset is inherently trusted.
- All resource authentication and authorisation are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

The approach and technical controls supporting ZT adoption may vary substantially dependent upon use case, but at a high-level should focus on identifying organisational assets and their dependencies, and use authentication and authorisation to create and then ideally shrink implicit trust zones.
High level guidance to help organisations adopt ZT, and aligned with NIST, is usefully provided by the UK National Cyber Security Centre (NCSC) [2].

- Know your architecture including users, devices, and services
- Know your user, service and device identities
- Know the health of your users, devices and services
- Use policies to authorise requests
- Authenticate everywhere
- Focus your monitoring on devices and services
- Don't trust any network, including your own
- Choose services designed for zero trust

Avoiding a definition that requires specific exclusions (e.g. VPNs, Firewalls) or mandates specific inclusions (e.g. Public Cloud), makes it easier for organisations to readily adopt a ZT mind-set, and seek relevant opportunities to enhance or

augment existing infrastructure and services, which may or may not form part of a journey to a longer-term and a more complete migration to ZT.

Initial projects may include a review of corporate assets and approaches to data classification, reviewing user identity life-cycle management, introducing or enhancing device identity and health measurements, and greater network or service segmentation, all of which feed nicely in to a review of security monitoring. Projects may well assume that the corporate firewall and VPN will remain in place for the foreseeable, but the organisation's assumptions regarding their value in isolation has evolved.

Create Creating Zero Trust Architectures from scratch and removing implicit trust in disparate networks allows start-up or autonomous enterprises to impose robust security controls and risk management while reaping the benefits of diverse technologies.	**Augment** Where organisations see the value of adopting ZT principles for new projects or semi-autonomous environments that will run alongside and have some interaction with existing legacy systems. Often the first step to ZT migration.
Enhance Where organisation see the value of applying ZT principles where practical within existing legacy environments, seeking to improve cyber resilience without attempting to attain or approach full alignment with ZT.	**Migrate** Organisations formally set the strategic objective to migrate existing systems to align to Zero Trust principles as far as is practically possible.

ZT Project Catagorisation

Approaches to ZT

Well-resourced and competent organisations, such as Google with the well-publicised BeyondCorp initiative [3], have taken many years to approach their ZT goals. BeyondCorp represented a major business change programme, with senior organisational support to navigate a wide range of technical and process-related challenges. BeyondCorp relied on augmenting existing infrastructure with a new 'unprivileged' network that would run in parallel with legacy IT, while users and services that could be migrated across were carefully prioritised.

Today, Google recommend organisations identify constrained use cases for the commencement of ZT adoption. Use case selection may be on the basis of services that will be easy to either create with, or migrate to a ZT model, in order to gain early wins and momentum to carry forward. An example may be supporting direct access to cloud services, such as Office 365, that allows a better user experience than routing traffic via the corporate LAN. Microsoft's Conditional Access Control Policies, provide an extensible mechanism for integrating federated user and device identity management with dynamic security policies for Azure-based applications, allowing a robust security posture to be maintained for devices outside of the corporate LAN.

Alternatively, organisations may choose to identify where new planned services present significant IT-related business risk, and undertake the appropriate adoption of ZT principles to provide a mechanism for more effective risk management. A common scenario within the critical national infrastructure (CNI), has been improving protection of critical services by enhancing device health measurement and security monitoring with dynamic policy enforcement for privileged services, beyond that currently achievable across the broader organisation.

An architecture for robust device health and identity management, developed as part of the NCSC CloudClient project [4], allows an organisation to verify the integrity of all executing software components running on an organisational asset. Resource access decisions combine user identity, device identity and health, and can be implemented at an individual resource level (e.g. via a proxy server) or a network segment level dependent on architectural requirements.

Assessing ZT Maturity

Given the diversity of requirements and approaches to ZT adoption, assessing organisational maturity with respect to ZT must be done along the axes of both scope and effectiveness. Scope includes both defining the subset of organisational assets that are included, as well as the strategic objectives. As mentioned above, organisations may well target a subset of assets regarded as critical services, and be justified in ignoring low-value, low-risk assets that may be complex to migrate to ZT. In this context, the appropriate strategic objective to be measured against, will be successful augmentation of existing IT, as opposed to complete organisational migration to pure ZT.

Indicators of effectiveness of ZT adoption within defined scope will then include:

Completeness of asset inventory and dependencies

With many ZT architectures, inventory maturity is required before services are fully live, to allow relevant access policies to be defined. The BeyondCorp initiative used extensive network and system monitoring to identify and confirm assets and access requirements, with controls initially set to monitor mode, to inform service migration.

Assessment of the relative size of implicit trust zones

Implicit trust zones may range from policy enforcement points serving individual resources, through to gateways protecting secure enclaves that host multiple resources within a defined network segment. Assessing the size of a trust zone is a measure of maturity, with the ideal being access to individual enterprise resources granted on a per-session basis. However, where secure enclaves exist out of necessity, a key measure of maturity will be avoiding or minimising any variation of authentication and authorisation required for access to the enclave based on source or destination. For example, where secure enclaves support legacy applications, ACLs providing access from legacy IT should provide some form of equivalence to policy controlling access from external assets.

Granularity of access policies

As part of broader information security management, mature organisations will have undertaken an assessment of relevant threats and organisational risk appetite. The maturity of access control policies should be judged as relative to the resulting security objectives. For example in CNI elevated-threat environments, appropriate measures of device health increasingly involve robust mechanisms for validating the integrity of all software executing on an asset. Elsewhere, a policy that simply ensures devices are patched may be sufficiently mature given the relevant threat model.

Effectiveness of security monitoring

Within a ZT environment, the policies that define expected user and device behaviour provide the context for informed logging. Combining controls such as MFA and robust device health measurements should mean significant access policy violations will be low-volume and high-value events, making the detection and analysis of significant events easier than legacy IT systems, even on open or unprivileged networks.

Adaptability

As ZT policies need to evolve in line with environmental, process or people changes, the presence of automation, or at least minimised overhead in resource or time required to maintain ZT policy alignment will form important measures of maturity that effect both usability and security.

Usability

Usability is often a straightforward measure of maturity to track, as users will readily voice their views, and can be formally encouraged to do so. Many ZT implementations can deliver usability benefits, through more effective forms of user authentication or more efficient access to new (often cloud) services.

Summary

The increased adoption of cloud and mobile technologies, increasing network interconnectivity and the digital dependencies of today's organisations has led to the rise in popularity of the Zero Trust model. As a sign of maturity of ZT, both NCSC and US agencies recommend the ZT model as an approach for organisations to improve cyber resilience, and provide useful and evolving advice to help organisations do so. The diversity of requirements of individual organisations, means there is no single appropriate blue print for organisations to follow for ZT adoption. However, the core philosophy of reducing or removing implicit trust in networks provides common ground across the variety of architectural choices, and the value derived should be through explicit measurements made in the context of an organisation's strategic objectives.

References

[1] NIST Special Publication (SP) 800-207, Zero Trust Architecture, **https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207**

[2] National Cyber Security Centre, Zero trust principles - beta release, **https://www.ncsc.gov.uk/blog-post/zero-trust-principles-beta-release**

[3] Google, BeyondCorp, **https://cloud.google.com/beyondcorp**

[4] CloudClient – Origins of a Zero Trust Network deployment for UK Government, **https://www.enterprisetimes.co.uk/2018/11/29/cloudclient-origins-of-a-zero-trust-network-deployment-for-uk-government-2/**

About Becrypt

Becrypt is an agile London-based UK SME with 20 years cyber security expertise, established through the development and delivery of cloud, mobile and endpoint platforms. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services - from funded research, to commercially available products and flexible managed services. Becrypt have worked with UK Government and platform vendors to pioneer and deploy device health identity management products and services, based on the NCSC CloudClient Architecture.

https://www.becrypt.com/uk/products/paradox/

Becrypt Ltd
Artillery House
11-19 Artillery Row
London SW1P 1RT
UK Company Number 4328430
Tel: 0845 838 2050

#becrypt