ZERO TRUST – DEMYSTIFIED

UNISYS | Securing Your Tomorrow®

Everyone seems to be talking about Zero Trust in the security world at the moment. Unfortunately, there seems to be multiple definitions of this depending on which vendor you ask. To help others understand what Zero Trust is, this white paper covers the key aspects of a Zero Trust model.

What is Zero Trust?

Zero Trust is a *philosophy* and a related *architecture* to implement this *way of thinking* founded by John Kindervag in 2010. What it isn't, is a particular technology!

There are three key components to a Zero Trust model:

1. **User/Application authentication** – we must authenticate the user or the application (in cases where applications are requesting automated access) irrefutably to ensure that the entity requesting access is indeed that entity.
2. **Device authentication** – just authenticating the user/application is not enough. We must authenticate the device requesting access as well.
3. **Trust** – access is then granted once the user/application and device is irrefutably authenticated.

Essentially, the framework dictates that we cannot trust anything *inside* or *outside* your perimeters. The Zero Trust model operates on the principle of *'never trust, always verify'*. It effectively assumes that the perimeter is dead and we can no longer operate on the idea of establishing a perimeter and expecting a lower level of security inside the perimeter as everything inside is trusted. This has unfortunately proven true in multiple attacks as attackers simply enter the perimeter through trusted connections via tactics such as phishing attacks.

Enforcing the Control Plane

In order to adequately implement Zero Trust, one must enforce and leverage distributed policy enforcement as far toward the network edge as possible. This basically means that granular authentication and authorisation controls are enforced as far away from the data as possible which in most cases tends to be the device the user is using to access the data. So in essence, the user and device are both untrusted until both are authenticated after which very granular role based access controls are enforced.

In order to achieve the above, a **control plane** must be implemented that can coordinate and configure access to data. This control plane is technology agnostic. It simply needs to perform the function described above. Requests for access to protected resources are first made through the control plane, where both the device and user must be authenticated and authorised. Fine-grained policy can be applied at this layer, perhaps based on role in the organization, time of day, or type of device. Access to more secure resources can additionally mandate stronger authentication. Once the control plane has decided that the request will be allowed, it dynamically configures the data plane to accept traffic from that client (and that client only). In addition, it can coordinate the details of an encrypted tunnel between the requestor and the resource to prevent traffic from being 'sniffed on the wire'.

Components of Zero Trust and the Control Plane

Enforcing a Zero Trust model and the associated control plan that instructs the data plane to accept traffic from that client upon authentication requires some key components for the model to operate. The first and most fundamental is **micro-segmentation and granular perimeter enforcement** based on:

- Users
- Their locations
- Their devices and its security posture
- Their behaviour
- Their context and other data

The above aspects are used to determine whether to trust a *user, machine or application* seeking access to a particular part of the enterprise.

In this case, the micro-segmentation technology essentially becomes the control plane. Per the above section, encryption on the wire is a key component of Zero Trust. For any micro-segmentation technology to be an effective control plane, it *must*:

- Enforce traffic encryption between endpoints
- Authenticate the user and machine based on their identity and not the network segment they are coming from

Zero Trust Technologies

As stated earlier, Zero Trust is an architecture. Other than microsegmentation, the following key technologies and processes are required to implement Zero Trust:

- **Multifactor authentication** – to enforce strong authentication.
- **Identity and access management** – to irrefutably authenticate the user/application and the device.
- **User and network behaviour analytics** – to understand the relative behaviours of the user and the network they are coming from and highlight any unusual behaviour compared to a pre-established baseline which may indicate a compromised identity.

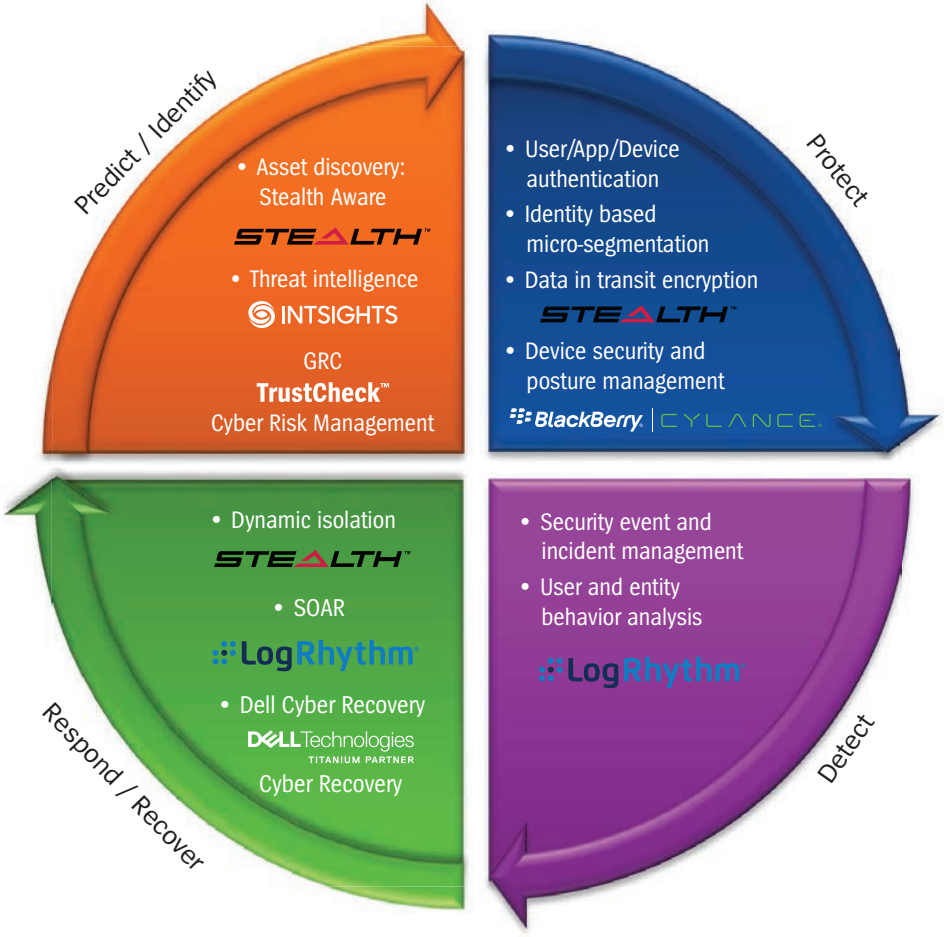
- **Endpoint security** – to ensure that the endpoint itself is clean and will not act as a conduit for an attacker to gain unauthorised access to data.
- **Encryption** – to prevent sniffing of traffic on the wire.
- **Scoring** – establishing a 'score' based on the perimeters above that will then determine whether access can be granted or not.
- Apart from the above key components, the following are needed as well:
  - *File system permissions* – needed in order to implement role based access controls.
  - *Auditing and logging* – to provide monitoring capabilities in case unauthorised access is achieved.
  - *Granular role based access controls* – to ensure access is on a 'need to know basis only'.
  - *Supporting processes* – all of the above needs to be supported by adequate operational procedures, processes and a conducive security framework so that the model operates as intended.
  - *Mindset and organisational change management* – since Zero Trust is a shift in security thinking, a mindset change managed by robust change management is required to ensure the successful implementation of Zero Trust in an organisation.

Challenges with Zero Trust

So Zero Trust sounds pretty awesome, right? So why haven't organisations adopted it fully?

As with any new technology or philosophy, there are always adoption challenges. Zero Trust is no different. At a high level, the key challenges in my experience are:

- **Change resistance** – Zero Trust is a fundamental shift in the way security is implemented. As a result, there is resistance from many who are simply used to the *traditional perimeter based security model*.
- **Technology focus as opposed to strategy focus** – since Zero Trust is a model that will impact the entire enterprise, it requires careful planning and a strategy to implement this. Many are still approaching security from the angle that if we throw enough technology at it, it will be fine. Unfortunately, this thinking is what will destroy the key principles of Zero Trust.
- **Legacy systems and environments** – legacy systems and environments that we still need for a variety of reasons were built around the traditional perimeter based security model. Changing them may not be easy and in some cases may stop these systems from operating.
- **Time and cost** – Zero Trust is an enterprise wide initiative. As such, it requires time and investment, both of which may be scarce in an organisation.



Zero Trust Model – Integrated and Delivered by Unisys

Suggested Approach to Zero Trust

Having discussed some challenges to adopting a Zero Trust model above, let's focus on an approach that may allow an organisation to implement a Zero Trust model successfully:

1. **Take a multi-year and multi-phased approach** – Zero Trust takes time to implement. Take your time and phase the project out to spread the investment over a few financial years.
2. **Determine an overall strategy and start from there** – since Zero Trust impacts the entire enterprise, a well-crafted strategy is critical to ensure success. A suggested, phased approach is:
   a. *Cloud environments, new systems and digital transformation are good places to start* – these tend to be greenfield and should be more conducive to a new security model.
   b. *Ensure zero trust is built into new systems, and upgrades or changes* – build Zero Trust by design, not by retrofit. As legacy systems are changed or retired, a Zero Trust model should be part of the new deployment strategy.
   c. *Engage a robust change management program* – mindset adjustment through good change management.
3. **Take a risk and business focus** – this will allow you to focus on protecting critical information assets and justify the investments based on ROI and risk mitigation.
4. **Ensure maintenance and management of the new environment** – as with everything, ensure your new Zero Trust deployment is well maintained and managed and does not degrade over time.

To summarise, Zero Trust is a security philosophy and architecture that will change the way traditional perimeter based security is deployed and helps organisations move from crisis to confidence.

Micro-segmentation is a key technology component of Zero Trust implementation and this paper provided an approach to implementing Zero Trust which included taking a phased approach based on a sound strategy underpinned by a risk and business focused approach to ensure your security is Always On.

About the Author

Ashwin Pal

Ashwin Pal is the Unisys Director of Security Services responsible for the delivery of Unisys' security business in the Asia Pacific region.

Contact Ashwin at Ashwin.Pal@au.unisys.com or connect with him at LinkedIn.

To learn more about how to implement Zero Trust to have ALWAYS ON security, visit www.unisys.com/zt-implemented.

For more information visit www.unisys.com

08/20 20-0380