VeroGuard Systems

Absolute Trust

Maintaining a Trusted Identity in the Digital Economy

The transition to a digital economy requires a trusted, efficient and unified secure method for accessing online services. As organisations battle the increasing cyber threat, the new hybrid IT environment and the end to the corporate network perimeter, identity and access management is more challenging than ever.

Traditional castle-and-moat security models do not meet with the needs of increasingly mobile users, and has seen move to Zero Trust models, where every new action requires re-authentication creating significant management overhead.

The alternate solution to this Absolute Trust. This model can be achieved by breaking down the silos of identity across business units and organisations, and enabling never before seen levels of collaboration and control.

VeroGuard Systems

Absolute Trust

The breakthrough for maintaining a Trusted Identity

Identity theft remains the number one attack vector for hackers, currently representative of more than 8 out of every 10 data breaches due to hacking. This should not be surprising, given the way in which we access systems and networks has changed little in the past 30 years; with a username and password still being used by the vast majority for user authentication. Add to this the traditional castle-and-moat security strategy which is still being employed and a hacker, once through a company's perimeter defences, can then freely access systems and resources.

The journey through user Access Management thus far, has seen the creation of policies for complex passwords, one-time-password tokens, use of biometric authentication devices and other multi factor authentication (MFA) techniques – none of which has led to a totally secure and trusted user access experience.

It all boils down to trust.

If trust could be easily established, then access management and network security policies would be far simpler to architect. However, just as trusting another human in a face-to-face interaction is far from a perfect science, there is no way to know if a digital credential has been stolen and is normally accepted without first establishing trust. Given the number and growing sophistication of phishing practices, organisations should be concerned.

It is for this reason that a model of **Zero Trust** is now becoming a popular policy employed for User Access Management. Zero Trust is a holistic IT security model that requires strict identity verification for every person and device trying to access a network, regardless of whether they are sitting inside or outside of the network perimeter. A core principal is to minimise access to the least amount required to perform the tasks a user needs to accomplish, meaning that every request for more resources is met with a re-authentication request.

Another option is to move to **Absolute Trust** where a user's identity can be irrefutably confirmed and non-repudiable. A model of Absolute Trust can break down the Access Management challenge and offers a single identity layer for any system regardless of the network, access point, device or application which would bring significant control and simplicity to Access Management policies.

Why don't existing access management solutions meet the needs of today's systems and networks?

Access management systems and policies have been developed in line with the technology platforms they support, however with the current hybrid of cloud and on premises IT environments most organisations use, maintaining control over who can access what is becoming a complex and time-consuming task.

Traditional access management solutions were developed to reduce the inefficiencies and increase control and security when provisioning user accounts across multiple systems. The first era was born in the late 90's to support on premises applications. Around 2010, a new generation of access management was required to cater for cloud applications, however this has led to fragmentation as the two environments are distinct from one another and users are managed separately and redundantly.

The third era is what analysts and industry see as the future: Unified Access Management - secure access management for all devices and applications, regardless of where they're hosted. Unified access management is the basis for which an Absolute Trust policy can be achieved removing the need to maintain multiple access management systems and policies for users internally, on their own devices and accessing systems remotely.

Everyone must be implementing Zero Trust more locks mean a stronger safe – Right?

The complexities of applying Zero Trust to a company's legacy and existing environments are equally matched by the ongoing effort required to maintain and update configurations across network services and resources, which can actually contribute to making the network more brittle.

A Zero Trust policy forces users and devices to strongly authenticate on any request and provide only minimal resource access. In this model requests for any new system or data access is met with a new authentication check every time. This way it is seen to protect an organisation from lateral movement and exposure due to identity theft. The theory being that the entry point for an attack is often not the target location. Zero Trust works by enabling policies giving users the least amount of access required to perform the tasks they need to accomplish, and is enabled by

technologies such as multifactor authentication, IAM, orchestration, analytics, encryption, scoring and file system permissions.

Some organisations have opted for a multi-layered approach, minimising password entry by implementing Single Sign On (SSO), applying hardware token, geolocation and device risk-based techniques to apply two-factor (2FA) and multifactor authentication (MFA) approaches across systems. SSO without other layers of authentication does become a single point of failure, as once the 'master password' has been obtained, an attacker gains access to all of that user's systems.

Zero Trust policies, therefore, build a trust profile based on the resources and systems a user is trying to access, where they are (network and location) and from which device they are on. For a user, this can mean a multitude of different experiences depending on these factors, and combinations of passwords, tokens, one-time passwords and MFA; depending on their access point and requirement. With each layer, yet another solution requires management and user support, adds to complexity and increases costs. The loss of oversight on any one layer becomes a point of susceptibility.

Even with strong operational controls in place, a major barrier for Zero Trust is the inability to apply a consistent and highly secure user authentication solution across legacy, on-premises and cloud systems, which provides a simple and frictionless experience for users regardless of how they connect.

Further, Zero Trust extends only as far as the reach of the organisation and cannot be applied in the same way to customer facing solutions or shared across corporate boundaries when collaborating with other organisations.

"More locks mean more keys, which all need to be rigorously managed from a user and system perspective to maintain the network hardening intended."

If you get it set up correctly Zero Trust works doesn't it?

Many experts agree that Zero Trust is a strong security posture for any organisation to employ; however, the reason it is necessary is to defend against the weakest element in the whole cyber security framework the "***Human Element***". What a Zero Trust User Access Management policy boils down to is that the CIO does not trust ***you.*** Too many employees still use the same weak password on multiple systems, get caught by phishing attacks and have malware on their personal devices. What this means is that cyber criminals can easily guess or collect user credentials and then impersonate an employee leading to the IT department limiting access to everything or implementing Zero Trust.

This methodology works well for modern cloud-based systems and greenfield environments, as network access can be designed from the inside out, rather than the traditional castle-and-moat strategy which builds security into the perimeter and trusts everything once it has successfully traversed the drawbridge and raised the portcullis.

However, a key drawback is the reliance on a password which leaves the gate open for attack. Therefore, even with a Zero Trust framework in place, organisations must continue to keep adding context, ensure user roles are up-to-date and add more authentication methods to counter credential-based attacks.

Zero Trust works, but it's complex to set up and a lot of work to maintain, and there is still no guarantee of blocking unauthorised access due to use of stolen credentials.

Can you realistically achieve Absolute Trust?

Absolute Trust appears on the surface to fly in the face of everything we have ever been told about the online world. Hackers and other nefarious actors continue to bombard our personal, business systems and devices with both full frontal and behind the scenes attacks, seeking more often that not the user credentials that provide access to the systems we use. Yes – your username and password.

So, what if we removed passwords completely? If you were able to securely access any system or device without needing a password, then there would be nothing to be stolen. Hackers could not access systems or networks via a username and password as this channel would be closed off, and therefore authenticated users could be immediately trusted.

To achieve this, one must be able to quickly and simply prove you are who you are

VeroGuard has created a system to do exactly that – essentially a solution to the problem of not knowing who or what is at the other end of an online transaction, and therefore the authenticity of the interrogation, communication and associated data.

VeroGuard's technology works by removing passwords and replacing them with a single and

fast login experience for all user authentications via a portable Digital ID. Security is assured with Hardware Security Modules (HSM's otherwise known as 'Black Boxes') at both ends of every authentication, communication and data transaction.

The VeroGuard Systems solution has been designed to reduce and remove many of the risks of being a victim of identity related cyber-crime and at the same time reduce integration costs, improve the user experience and address many of the issues associated with privileged access.

The VeroCard provides a single gesture, out of band, multi-factor authentication solution based on existing proven bank to bank protocols and can provide hardware encrypted and verified security access across platforms regardless of device, network or location.

VeroGuard can provide the infrastructure to enable an ***Absolute Trust*** policy for any organisation including Governments, Corporate, Large and Small Business and Individuals.

Surely Absolute Trust just creates a single point of attack. Once compromised everyone using the system is compromised?

Absolute Trust when implemented using VeroGuard's technology does not create a single point of failure, as the system is secured end to end with HSM's and all authentication transactions are encrypted. Private keys are never exposed to software where they can be harvested or broken by malware or applications.

The VeroCard device is an HSM level Digital Wallet which is tamper proof and if lost, the card has no accessible data on it and can be remotely disabled. Unlike a mobile phone, a VeroCard cannot have any user applications loaded, protecting the device from malware and other malicious applications.

In the unlikely event that the VeroGuard server is breached no card can be compromised, no user credentials can be stolen. In the unlikely event that a VeroCard is compromised it cannot affect any other user.

My organisation is driving an aggressive digital transformation program….

An Absolute Trust model with Unified Access Management is a cornerstone to digital transformation as a transformed company can't be concerned with where applications are hosted. Hybrid cloud and on premises IT environments are likely to remain for some time, therefore solutions to unify application access across these environments are required for an organisation to be truly effective.

Driving a Zero Trust policy is counter intuitive to user adoption and ongoing useability. The mantra of ***"security is more important than useability"*** must make way to ***"security with useability"*** and will see more organisations implement a unified universal identity that can be anchored to the user and not the application and provide the trusted secure access to any system expected by users and the security required by businesses, governments and individuals.

Absolute Trust

Absolute Trust delivers on the promise of digital transformation, removes the most common attack vector and the cause of more than 80% of data losses (passwords) and offers unprecedented ability to authenticate, collaborate and integrate. Absolute Trust is achieved by enabling systems to release the shackles of outdated, complex and restrictive user access and security policies, embrace a holistic unified universal digital identity layer for the connected world.

VeroGuard Systems Pty Ltd
ABN 25 617 573 001

P / +61 (03) 9558 3090
admin@veroguard.com.au

veroguard.com.au