Awingu.com®

One Workspace. Any Device. Anywhere.

Zero Trust: what, why and how

Written by

Dr. Chase Cunningham

NETWORK, NETWORK

When the Jericho Forum was founded in 2004, its mission was to define what cybersecurity would look like in a future where there was no perimeter, and cloud dominated the world's approach to architecture. The leaders and visionaries at the forum saw that coming transition nearly a decade before it was ever a real consideration for businesses. In 2009, Forrester analyst John Kindervag coined the term "Zero Trust" in his research, mainly due to his realization that "deperimeterization", which is what the Jericho Forum was calling their future cyber model, was not going to be a well received term in the market.

That original concept of Zero Trust was based on the thinking that a data-centric network design was capable of leveraging micro-segmentation via the firewall and network-connected assets to enforce granular rule sets and thereby limit lateral movement by attackers. As the concept of Zero Trust evolved, a more identity-centric approach started to gain prominence. This trend has accelerated with the adoption of mobile and cloud technologies and was further expedited as the Covid crisis and the move to remote work took place in 2020.

While Zero Trust has come to the main stage in the post-Covid year, the conversation around SASE has grown almost as quickly. While there are similarities and differences between these two approaches to cybersecurity it's worth our time to explore the realities of ZT and SASE with a bit more depth.

But while Zero Trust has grown in global adoption there are hindrances that have come to light for organizations that seek to adopt ZT as their strategic focal point. One of those main issues is that of command and control of disparate resources and the need for increased efficacy of resource allocation and use for the variety of tooling that is needed to make ZT possible.

The Network component of Zero Trust must include technology that aids in the grouping of host servers, data connections, interfaces between hosts, network segmentation, intrusion detection, cryptography of flows between hosts (e.g. SSL, VPNs), and can also include more useful telemetry data such as "time of day" and proximity of multi-factor mechanisms in relation to the network. Within the Zero Trust approach, it is important to understand that the network has an identity as well and that there is immense value in understanding how items of that identity are operating.

The academic definition for Zero Trust as stated by Forrester is that Zero Trust is strategically focused on addressing lateral threat movement within the network by leveraging micro-segmentation and granular enforcement, based on user context, data access controls, location, app, and the device posture. As you can see by looking at the Forrester ZeroTrusteXtended ecosystem framework Zero Trust is a multi-faceted approach to security strategy and is inclusive of a variety of technical components and capabilities.

John Kindervag, a.k.a.
the "Godfather of Zero Trust"

THE JERICHO FORUM

The Jericho Forum was basically a group of large, multinational user companies that were dedicated to the development of particular standards that hoped to help enterprises enable secure, boundaryless information sharing across disparate infrastructure..

According to one of the group's co-founders, namely Paul Simmonds, the idea for the group started in 2002. That's right nearly 20 years ago. The basic concept for the Jericho Forum was to support and further the idea of "de-perimeterization", a lengthy way of saying when businesses went beyond a network. The group realized that many different vendors and companies were tackling many of the same challenges of doing business and operating securely in a de-perimeterized world. Mainly these visionaries realized that they would need to look at the problem space differently as businesses were going to change how they operated.

Accepting that businesses were going to move to a world that embraced de-perimeterisation required that security architects and defenders to fundamentally re-think their approach to securing data. Securing data where the data was originated and used also was a change in thinking for the members of the Jericho Forum as it meant they had to truly recognize that the current state of infrastructure, in the early 2000s that is, was not secure by nature.

The Jericho Forum recognized emerging trends that were just showing up on the global stage nearly 20 years ago. Those early issues that the Jericho Forum identified are now part of our everyday lives, most people just aren't aware of the realities of operating in the perimeter-free world.

The Jericho Forum logo

CLOUD EMERGES

Cloud computing has mostly been pioneered by a few major firms, but the reach and power of the innovations from cloud have been the lever that has vaulted the world into its current era of digital innovation and acceleration. In reality, the term "cloud computing" was first exposed to the world way back in 2006 to refer to a business model in which data service and architecture reside in remote servers.

Since that early concept for cloud computing, cloud use has expanded globally and has been actively adopted by clients and vendors in both developed countries and emerging markets. Recently, the research company Forrester published the first industry report that offered a sizing of the cloud computing market. According to this report, the market is expected to reach $241 billion in 2020, compared to $40.7 billion in 2010.

Cloud computing and cloud-based resources are literally the technology that helped the world economy survive the Covid19 crisis. As the world moved almost overnight to a fully remote and totally connected model for a large percentage of work roles it was cloud computing and the availability of connectivity and resources that cloud offered which powered this massive transition. To be blunt, without the cloud and the world economy would have basically collapsed.

Cloud computing and cloud-based technologies are now the largest area of investment and growth in technology infrastructure globally at over 100 billion dollars by 2023 (Miltz). With the continued growth of cloud as the standard for infrastructure over the next decade it is logical to think that companies would be wise to move their resources and assets to leverage this powerful and dynamic infrastructure apparatus.

But as the cloud is so powerful and so useful there is a key transition that has also occurred. As more cloud has become a growth solution the reality that cloud access revolves around one pivotal gear in the machine. Identity and the user's accounts that are the crux of those access identities is the single most important mechanism for any organization to manage in the cloud space. If cloud is the infrastructure for the future, identity is the key that holds to the door for that cloud-based future.

IDENTITY TAKES HOLD

In the original concept for de-perimeterized security way back in 2003, the issue of identity was one that was essentially addressed with the idea that at that time a user often only had one login and one password on any system, and that system was administered in a controlled corporate enclave that was relatively bounded. That idea was fine in 2003, but now in 2021 that no longer holds water.

Consider that the average user has roughly 4 devices, over 90 personal accounts, and more than 20 business application accounts, each with their own usernames and passwords. The numbers get exponentially large for users and their identities when the move to a disparate and remote work scenario gets added into the equation. Users' identities are increasingly growing with the addition of cloud resources, cloud applications, and the variety of devices that are constantly coming online. Each of those identities and their associated usernames and passwords presents a potential avenue of compromise for any enterprise.

Added to this is the issue that with increased home usage and remote work every individual is essentially an administrator on their home network, which connects to the corporate resources, which accesses everything that user, and their potentially threatened home network, devices, and passwords have access to. Those usernames, passwords, and compromised accesses are tied to the identities that organizations must manage in the dynamic cloud space in order to keep their businesses operational and enable digital transformation.

While the cloud is the power that is driving digital transformation forward, it is the user and their ability to access those cloud resources that actually makes everything work. Without users there is no value to these systems and businesses would digitally die overnight. But managing those users and their likely compromised identities becomes increasingly important and if a business ignores that reality, they knowingly introduce compromise into their cloud infrastructure and ultimately their corporate network.

Managing the user and their identity became increasingly pivotal for organizations as the Covid19 crisis unfolded and has proven both difficult and necessary. As remote work became the global standard for businesses due to the crisis the world awoke to the reality that these issues were not a “one and done” but are now part of any business that wishes to be viable in the future.

"The point is that remote work is here to stay and is a competitive business advantage for the foreseeable future. But enabling remote work is not "easy", especially when the need for security is tossed into the mix."

Dr. Chase Cunningham

REMOTE WORK AND THE FUTURE

Remote work was rare a decade ago, even a few years ago remote work was considered a "benefit". Working from home was only available as a special arrangement to accommodate families in specific cases or was offered as a bonus for employees that could operate in an unmanaged, self-initiating model of operation. Thankfully, teleconferencing and telework technology evolved to the point where most businesses can enable completely remote teams, but even though that had taken place up until February 2020 remote work was still a luxury. But 2020 and the Covid19 crisis changed the conversation around remote work from one of "nice to have" to a must-have for both safety and survivability.

According to a recent Gartner survey, 80% of business leaders plan to allow employees to work remotely at least 30 percent of the time after the pandemic, and 47% will allow employees to work from home full-time (Baker). In a similar PwC survey of 669 CEOs, 78% agree that remote collaboration is here to stay for the long term. Other data points looking at remote work for the future found that 65% of respondents report wanting to be full-time remote employees post-pandemic, and 31% want a hybrid remote work environment. Overall, that's 96% who desire some form of remote work. Additionally, in those same surveys, roughly 27% of workers said that the ability to work from home is so important to them that they are willing to take a 10% to 20% pay cut to work remotely.

But in reality, when one looks at the benefits of remote work it is plain to see that remote work Is actually good for businesses. Several studies indicate that businesses lose an estimated $600 billion a year to workplace distractions and that remote workers are 35% to 40% more productive than their in-office counter-parts. Among performance-based remote work statistics in 2020, 94% of surveyed employers reported that company productivity has been the same (67%) or higher (27%) since employees started working from home during the pandemic.

A recent study from OpenVPN found that more than one in three organizations, 36% has dealt with a security incident due to an unsecured remote worker. 68% of businesses reported having a compromise that was directly related to a remote worker access or connectivity issue within the past year. A similar study from MalwareBytes companies noted that their preparedness on a scale of 1-10, with 1 being the least prepared and 10 being the most, was on average 7.23. Among those surveyed, 44% said their company didn't provide cybersecurity training focused on the potential threats of working from home, 45% didn't analyze the security or privacy features in the software tools considered necessary for remote working, and 68% did not deploy a new antivirus solution for work-issued devices (MalwareBytes). In that same study, respondents noted that about 20% had faced a security breach as a result of a remote worker. 18% of the business leaders surveyed acknowledged that cybersecurity was not a priority for employees (MalwareBytes).

The point is that remote work is here to stay and is a competitive business advantage for the foreseeable future. But enabling remote work is not "easy", especially when the need for security is tossed into the mix. With more workers going remote and more assets, applications, data, and users moving into this business model at such speed enabling focused and effective security capabilities exponentially increases in importance.

If remote work is now the "normal" and security is a necessity, not an option then what solutions and technologies are needed to enable such a transformative strategy as Zero Trust? In the next section, we will delve into that very question.

BYOD is here to stay

COVID19 not only accelerated the adoption to remote working, but also the use of 'Bring Your Own Device' for home computer, tablets, etc. was given a push. The shortage in client hardware at the start of the pandemic in 2020 was one of the main drivers as there simply were not enough alternatives at hand.

The problem is that a of businesses equipped these BYOD devices with VPN for remote access. While at first, that seemed like a great concept and approach to the problem, in reality, thanks to the massive breaches that contained usernames and passwords and the nation-state hacks that compromised VPN providers the VPN became not much more than a hindrance for users at best and a direct pipe for hackers into a network at worst. NGFW and segmentation can't fix the issue of a VPN when that connection for a BYOD user was authenticated with a hacked password and administrator privileges.

An April 2021 Awingu® survey by revealed that…

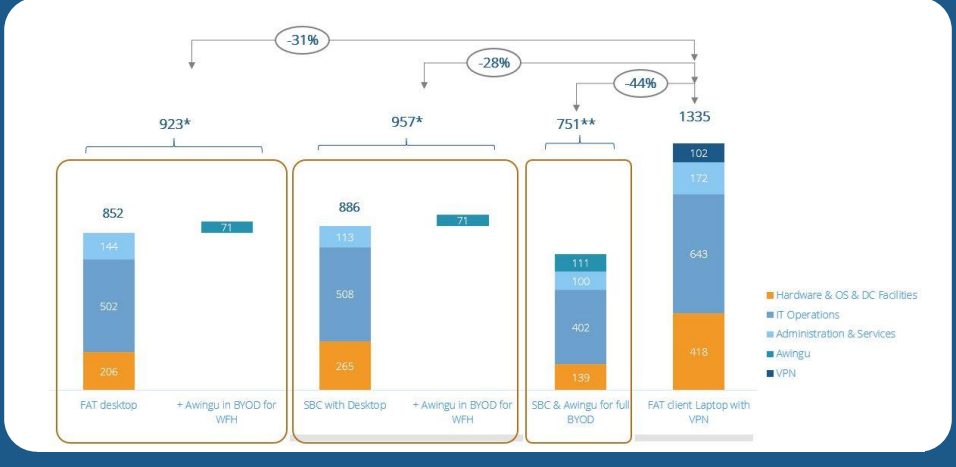
55% of businesses were doing BYOD…

…but only **16%** of them had an actual BYOD policy in place

BYOD and Awingu® reduce end-user computing TCO with 44%

Adopting BYOD can be interesting for many reasons, one of which being a significant impact on your EUC TCO. In a 2020 study, we compared the price points of many different "BYOD scenarios" and compared them to the costs of running a "managed fat client with VPN". The results were staggering: depending on the scenario, combining BYOD and Awingu can save you up to 44%.

Read the full analysis



"The problem is that a of businesses equipped these BYOD devices with VPN for remote access. While at first, that seemed like a great concept and approach to the problem, in reality, thanks to the massive breaches that contained usernames and passwords and the nation-state hacks that compromised VPN providers the VPN became not much more than a hindrance for users at best and a direct pipe for hackers into a network at worst"

Dr. Chase Cunningham
In Awingurutalks

Powering the user

Zero Trust is not a technology, it's not even a suite of technologies. It is in fact a strategic focus on leveraging available security solutions in order to deal with the fundamental issues that enable the proliferation of compromise activities. That's the academic version of Zero Trust. What this really means is that an organization must intelligently and strategically choose what security solutions they must have and apply those technologies in a manner that deals with the core issues that enable compromises. To do this requires the use of a variety of solutions. Some that can and probably should operate independently and others that work well in a packaged or platform-based approach.

One of the fundamental issues that help enable Zero Trust is the use of technologies that enable micro-segmentation. Micro-segmentation is really just a granular enforcement capability that helps segment systems based on users, their locations, and other data to determine whether to trust a user, machine, or application seeking access to a particular part of the enterprise.

A key piece of Zero Trust, and any good security strategy is enabling least-privilege access. Solutions that help dynamically provide access to data and information on a need-to-know basis, which helps to reduce the exposure of certain data sets within your environment are key here. Using these solutions as part of your Zero Trust approach helps to classify information suitable for use by certain users, which then limits the damage if a data breach might occur. Typically, solutions that help here are able to classify data and apply one-time-use credentials which are revoked after a period of time.

Micro-segmentation technologies allow for the breaking up of security perimeters into small controlled zones of infrastructure. This allows for more granular control and helps to enhance visibility and operational cognizance of the assets which must be managed. Additionally, these technologies are key to limiting the spread of a compromise should a successful exploit occur. In short, more segmentation is a good thing if done correctly with technologies that function dynamically to enhance control and isolation.

Multi-factor authentication (MFA) is needed because passwords are no longer sufficient protection for any asset or any enterprise. Most people create very weak and/or reuse passwords, in fact, analysis indicates that even in 2021 the most common passwords globally are 123456, qwerty, and password1 (Meyer). Bad passwords and single-factor authentication virtually guarantee a compromise will succeed. Multi-factor authentication requires more than one authentication piece to validate the user, usually, this comes in the form of a prompt via SMS or through the use of an authenticator application. These technologies help to enforce tighter restrictions in a network and ensure that account takeovers are rare. Additionally, for administrators of systems having MFA enabled helps validate "who" is active on a system, and this single security solution was the reason for the identification of the Solarwinds hack. Without MFA likely that attack would have continued for years had a single administrator noticed a login on a phone they did not physically own.

There are other tools and technologies that can help enable and enhance Zero Trust but these are some of the "simplest" and yet most effective.

Experience matters

Security has typically been seen, and noted, as an area of conflict. The conflict between the average everyday user and the security administrators and leaders that are working to secure those users. Additionally, there is often friction noted as the users of "secure" systems are constantly negatively impacted by the security solutions that they have been forced to use.

Legacy technologies such as the archaic VPN and DLP have fallen onto users' shoulders with the heft of inefficacy that leaves users frustrated and unhappy with their security solutions, and the teams that put deployed them. Users have become aware of the reality that while these old, outdated, obtrusive solutions are not only hard for them to use they also now see that VPNs do not protect them from malware, or ransomware. According to researchers at Akamai, "VPNs are a weak security solution", and users know this (Meisnner). Users also note that the VPN is notoriously slow. Users complain that it slows their execution on critical workflows which lowers productivity.

Security solutions today should not be obtrusive. They should be much like the modern automobile. One does not need to be an ASE certified mechanic or a GPS administrator to operate their vehicle and get where they want to go. The vehicle is easy to use, safe, and intuitive for the user. Security solutions can and should be as easy to use as a modern car. Zero Trust security solutions are notably better at enabling the user to be more engaged with security tooling and have been noted as improving employee productivity and happiness.

*If you go back historically and look at where security was ten years ago, it was around firewalls and the network. And now **it's really about the user, the identity and the access** and that's where we're continuing to progress towards. So that evolution means that security is going to be more focused on what the end-user does, behavioral analytics, those type of things. It doesn't have to be as difficult as you would think for people to adopt this and luckily, we're moving into a space where banking and healthcare are also moving to multi-factor authen-tication, so most people are getting more familiar with. if I want to get into my bank account, "I've got to set up MFA or 2FA", or at least have seen it somewhere.*

Dr. Chase Cunningham
In AwinguruTalks

Using the cloud the right way

The cloud is where an organization "wants" to be. For a variety of reasons that vary from a reduction in costs to improved efficiency and speed, the cloud is the place to be. Added to this a move to the cloud, or a "greenfield environment" as it's often called, is the right time to re-architect for improved security infrastructure. Most businesses of any significant size will likely have some semblance of an old on-premise infrastructure that is coupled with or "to" cloud assets, and that is completely acceptable. But for those businesses that are seeking to move into truly 21st-century operating models they should be as cloud heavy as they can be. The benefits of leveraging the power, cost savings, and adaptability that the cloud offers is a competitive differentiator.

Most businesses choose to move their data, applications, and information from an on-premise server or local, data center to public cloud architecture. Each cloud migration process is unique, just like each business. The complexity of cloud migration is dependent on the number of resources supported in each project. Anything can migrate to cloud platforms for business services, web/mobile applications, IoT, edge servers, CRM support systems, productivity software, enterprise databases, remote desktops, SD-WAN, network administration tools, and more to the cloud.

When done right, the cloud can be more secure than traditional network systems. It's important to remember that the cloud consists of systems, networks, and applications that must be configured and maintained securely and is part of a "shared responsibility" model. In the "shared responsibility" model, the business is responsible for its part in securing its infrastructure in the cloud.

The sharing part comes in as companies like Amazon and Google have built their cloud offering with security as a primary criterion. This also means that a business can gain increased security capability via that cloud system as cloud providers offer a variety of built-in tooling for security that is part of the cloud deployment model.

By centralizing and storing business information and data in a cloud repository, the cloud can offer stronger and more dynamic security than traditional data centers. Most cloud providers take care of some of the more overt security issues like keeping unwanted traffic outside a specific scope from accessing the machines on which business data and apps reside and deploying automatic security updates on various systems. Many cloud providers also have compliance certifications including ISO27001, PCI-DSS, AICPA/SOC, and HIPAA via their cloud offerings. This means that an organization that has specific compliance requirements or concerns, by using that cloud infrastructure that business could be immediately compliant.

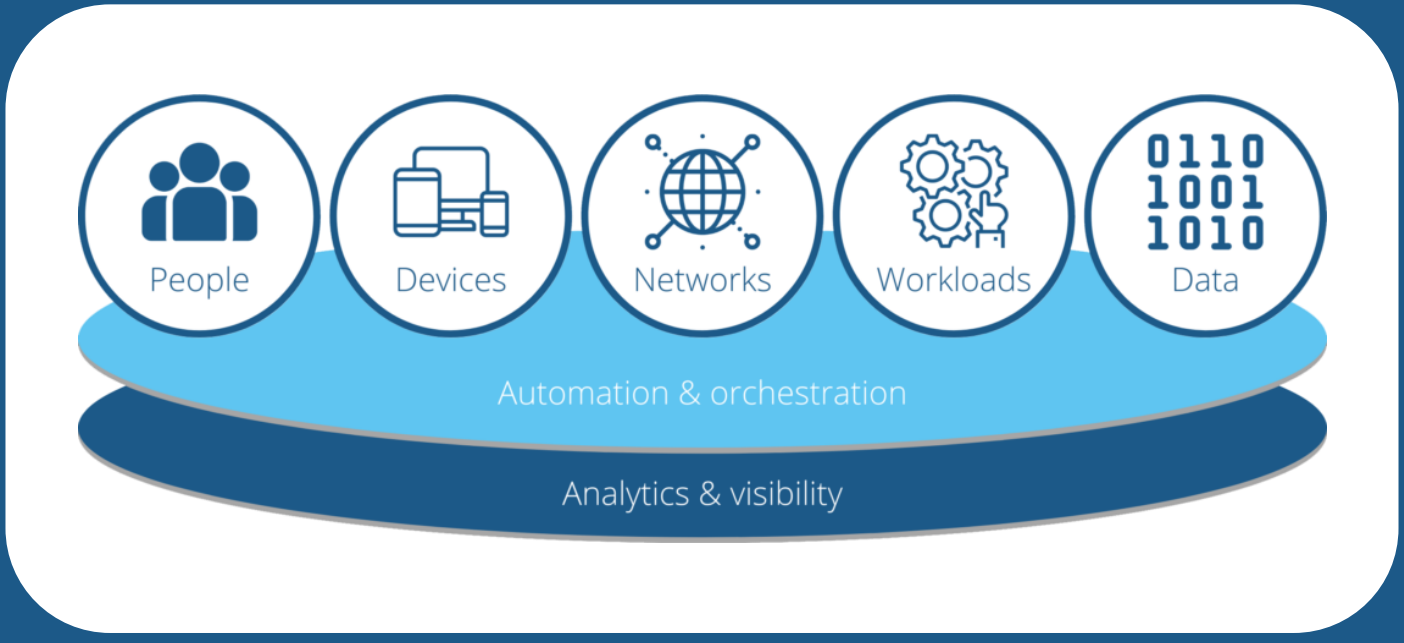
Using the cloud also offers a better ability to scale up or down based on various IT requirements and business needs. With cloud migration, organizations have the ability to dramatically reshape their infrastructure and workloads to accommodate the needs of today without being chained to the equipment and assets that were useful in the past. The cloud gives a business the power to control IT resources based on the business and its customers' needs. This would not be possible with other solutions that lock businesses into contracts, minimum terms, and one-size-fits-all plans. To be blunt, the cloud is where a business wants to be and honestly should be to be future-proof.

The Value of a Zero Trust Strategy

Zero Trust is taking hold in a very meaningful way in the last few years, with 275% year-over-year growth in North American the amount of exponential growth of the strategy has certainly taken hold. A study from IAM provider Okta found that in 2020 study 60% of organizations in North America, and 40% globally are currently working on zero trust projects (Okta).

Organizations increasingly see the value of looking at risk signals beyond simply checking only which network or networks a user is connecting from. Zero Trust-focused organizations are using their ZT technologies to help determine device health to help improve their security and reduce the risk from an unpatched device. By using device health as a key indicator of a valid and safe access request, Zero Trust technologies now are focused on telemetry data derived from device posture, physical location, and the users desired resource connection.

Zero Trust is not an isolated initiative.
It's an all-encompassing strategy.



What is Awingu®?

Awingu® is a unified workspace that offers a highly secure and audited access to your company files and legacy, web and SaaS applications in a browser-based workspace, accessible via any browser, on any device.

ANY DEVICE
Access the same workspace anywhere, on any device, via any web browser

SECURE
Provide a highly secure and audited access to all your applications and files

SIMPLE
Easy to install, manage and use, both for the user and the administrator

COST-EFFICIENT
Drives cost reduction compared to alternative solutions, and optimizes TCO up to 81%

Awingu® leverages your company's current architecture and is deployed as a virtual appliance on most hypervisors. This can be a private or public cloud. From there, Awingu® will connect into a classic back-end environment. It will link with Active Directory, LDAP, or an external IdP for user management. It will connect to application servers running Microsoft RDP for legacy applications or desktops. Web applications (e.g. intranet) can be connected via the Awingu® Reverse Proxy.

Finally, it will connect to classic file systems via WebDAV and CIFS and with cloud storage environments such as Microsoft's OneDrive.

For end-users, everything is available in a browser via Awingu®'s online workspace. No need to install agents, plug-ins, etc.

Learn more via awingu.com

Awingu®'s architecture: simple and non-intrusive

Awingu® helps businesses by strategically enabling Zero Trust

Awingu® was built to enable remote workers to access their apps, desktops, and files remotely from their browser and to do so securely. In line with Zero Trust principles of segmentation and isolation with Awingu®, there is no local data on the device, everything runs via an encrypted tunnel that pipes the content to the browser. Additionally, this capability allows the operation of a secure ZT system without the need for a VPN. With Awingu® in a matter of minutes and with nothing more than an internet connection, a business can deploy and offer a ZT- focused solution set to end-users and remote offices at a fraction of the cost of other heavier security solutions.

Awingu® also embraces Zero Trust principles as it works to enable the "least-privilege" approach for its users. By using RBAC, role-based access control as part of it's offering Awingu® further ties capabilities into the offering that integrate context awareness and granular usage controls based on the telemetry that a user's access request is sending across the encrypted system. Awingu® has MFA as a built-in offering that helps with identity and access management and further progresses the implementation of ZT strategically for any organization. Lastly, and possibly most importantly Awingu® makes life for the user simple and secure by default.

Awingu® gives the same flexibility and security for customers running their own cloud as well as public cloud. On-premise businesses can deploy Awingu® from scratch into their existing legacy environment in hours. Scaling up or down is super easy from there. The bar to adoption is very low - and there is virtually no change needed in the existing back-end setup to get started. Furthermore, there is no lock-in. You can evolve easily to public cloud or hybrid cloud strategies; both the technology as the license mobility allows for this.

To really understand some of the capabilities that are offered via the Awingu® platform that is in line with Zero Trust, are a few of the many solutions that are integrated into this browser-based system listed in the next pages.

Finally, a solution needs to be solely more secure. It also needs to take the end-user UX into account. Awingu® has made this balancing act. Simple setup for the admin without too much room for critical errors in the setup, with Awingu®, the life of the end-user is simple: take any device and authenticate security via the browser. Apps and desktops behave the same.

The most common issue that is cited as a hindrance to enabling Zero Trust is that ZT is "hard to do" and "technically difficult to implement". With Awingu® that is not the case. If a user can work via a browser, which we all do daily, they can operate in a Zero Trust environment. By leveraging this system, a business can deploy, control, administer, and leverage the power of a Zero Trust solution set and do so with all the benefits that businesses should get from security solutions.

Awingu® features enabling Zero Trust

EXTENSIVE USAGE AUDIT

Awingu® comes built-in with an extensive usage log. The usage audit tracks what application session users open (or close) and when and where (from what IP address) they do that. It also tracks what files are opened, deleted, shared, etc. The audit log is available via the Awingu® dashboard (admin), can be hooked into a SIEM, and custom reports can be extracted.

ANOMALY DETECTION

Get informed about irregularities in your environment, such as someone who logs in too often with a wrong password or someone trying to log in from abroad. This information is available via the Awingu® dashboard (admin only) and can be pushed into a SIEM.

HTML ISO RDP

RDP is known to have numerous exploits, especially when running older and unpatched versions. HTML minimizes the 'threat vector' specific to RDP (e.g. Bluekeep, NotPetya).

GRANULAR USAGE CONTROLS

Specific rights can be allocated for every user (group); e.g. preventing the use of the virtual printer (i.e. no printing at home), preventing downloading (or uploading) of files to and from the local desktop, preventing Awingu® application session sharing, preventing Awingu® file sharing, etc.

SESSION RECORDING

Awingu® can enable auto-recording of set applications or users (note: excluded for Awingu® Reverse Proxy sessions). The end-user will get a warning of the recording prior to starting his Awingu® application/desktop and will need to 'accept'.

CONTEXT-AWARENESS
Awingu® has a granular built-in context engine. Admins can define context restrictions (i.e. countries and/or IP addresses) per resource (i.e. streamed apps/desktop and file share). Outside of the context restrictions (e.g. in a foreign country), users will either be pushed to authenticate with MFA or just not be able to get access. This applies to all applications and file shares where the context restrictions are set up. You can imagine the setup of context awareness for share drives with sensitive data and applications like email clients and ERPs - blocking access or limiting share capabilities when outside the context restrictions '.e.g no Copy-/paste, no file sharing, no printing, … when access outside the context restriction.

NO LOCAL DATA
All applications, files, hosted desktops, etc. run in HTML5 inside the browser. There is no footprint on the device (cf. granular usage controls) and only screen 'images' are shared.

MULTI-FACTOR AUTHENTICATION
Awingu® comes with a built-in MFA solution and can (if necessary) easily integrate your current method of authentication. By adding MFA, you minimize the risk for 'brute force attacks'. The Awingu® built-in MFA supports the use of One-Time tokens (HOTP) and Time-Based tokens (TOTP). Awingu® also integrates DUO Security, Azure MFA, SMS Passcode, or Radius-based services.

ENCRYPTION OVER HTTPS
Between the end-user (browser) and the Awingu® virtual appliance, Awingu® favors and enables encryption over HTTPS. Awingu® allows the use of your own SSL certificates (or SSL Proxy). Furthermore, Awingu® has a built-in integration with Let's Encrypt, which automatically generates a unique SSL Certificate and takes care of its renewal.

PORT 443 ONLY
When set up correctly, Awingu® only requires port 443 to be available for end-user clients.

BIBLIOGRAPHY

- Baker, Mary. "Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time." Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, Gartner Research, 14 july 2020, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time. Accessed 22 april 2021.

- Courtney, Emily. "Remote Work Statistics: Navigating the New Normal." Remote Work Statistics: Navigating the New Normal, flexjobs.com, 21 december 2021, https://www.flexjobs.com/blog/post/remote-work-statistics/. Accessed 21 april 2021.

- MalwareBytes. "Enduring From Home." Enduring From Home, MalwareBytes, 2020, https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf. Accessed 22 april 2021.

- Meisnner, Gerd. "VPN: A Big Misunderstanding?" VPN: A Big Misunderstanding?, SecurityBoulevard.com, 15 March 2019, https://securityboulevard.com/2019/03/vpn-a-big-misunderstanding/. Accessed 25 april 2021.

- Meyer, Bernard. "Most common passwords: latest 2021 statistics." Most common passwords: latest 2021 statistics, cybernews.com, 9 april 2021, https://cybernews.com/best-password-managers/most-common-passwords/. Accessed 23 april 2021.

- Miltz, Kimberly. "Annual spending on cloud IT infrastructure worldwide from 2013 to 2024." Annual spending on cloud IT infrastructure worldwide from 2013 to 2024, statista.com, 1 april 2021, https://www.statista.com/statistics/503686/worldwide-cloud-it-infrastructure-market-spending/#:~:text=Global%20cloud%20IT%20infrastructure%20spending%202013%2D2024&text=This%20statistic%20displays%20spending%20on,reach%20110.5%20billion%20U.S.%20dollars. Accessed 21 april 2021.

- Okta. "The State of Zero Trust Security in Global Organizations." The State of Zero Trust Security in Global Organizations, Okta, 2020, https://www.okta.com/sites/default/files/pdf/zero-trust-security-in-global-org.pdf. Accessed 25 april 2021.

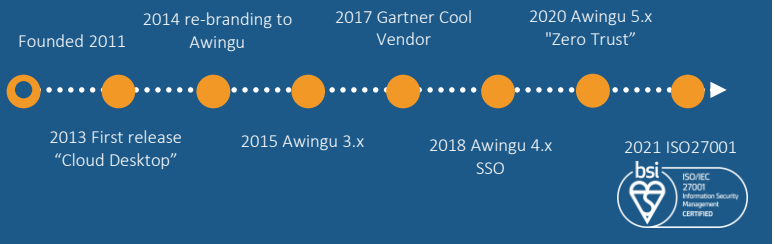
- Peek, Sean. "Communication Technology and Inclusion Will Shape the Future of Remote Work." Communication Technology and Inclusion Will Shape the Future of Remote Work, businessnewsdaily.com, 18 March 2020, https://www.businessnewsdaily.com/8156-future-of-remote-work.html. Accessed 21 april 2021.

- Turner, jack. "Study Reveals Average Person Has 100 Passwords." Study Reveals Average Person Has 100 Passwords, tech.co, tech.co october 2020, https://tech.co/news/average-person-100-passwords. Accessed 22 april 2021.

ABOUT AWINGU®

OFFICES

TIMELINE



STRATEGIC PARTNERSHIPS

Barracuda · BlackBerry · américa móvil · Google · IBM · Microsoft

RECOGNITIONS

Gartner Cool Vendor 2017 · Ovum · TAKE ME TO THE CLOUDS WINNER Start-up Company Award for Excellence

CHANNEL AWARDS 2016 AWINGU · CHANNEL AWARDS 2016 AWINGU · CHANNEL AWARDS 2017 AWINGU

Beloftevolle Onderneming van het Jaar® 2017 *Finalist*

ABOUT THE AUTHOR

Dr. Chase Cunningham

Dr. Chase Cunningham, aka *Dr. Zero Trust*, is a retired Navy Chief Cryptologist with more than 20 years of experience in Cyber Forensic and Analytic Operations and offering deep technical expertise, advanced education, various certifications and operational experience. He is the author of the book "Cyber Warfare – Truth, Tactics and Strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare" and is a former Forrester Research analyst in Security & Risk (specialized in the topic of Zero Trust).

HEADQUARTERS

Awingu® N.V.
Ottergemsesteenweg-Zuid 808 B44
9000 Gent, Belgium
+32 9 296 40 11

US OFFICES

Awingu® Inc.
530, 7th Avenue (suite 1407/08)
NY 10018, New York
United States