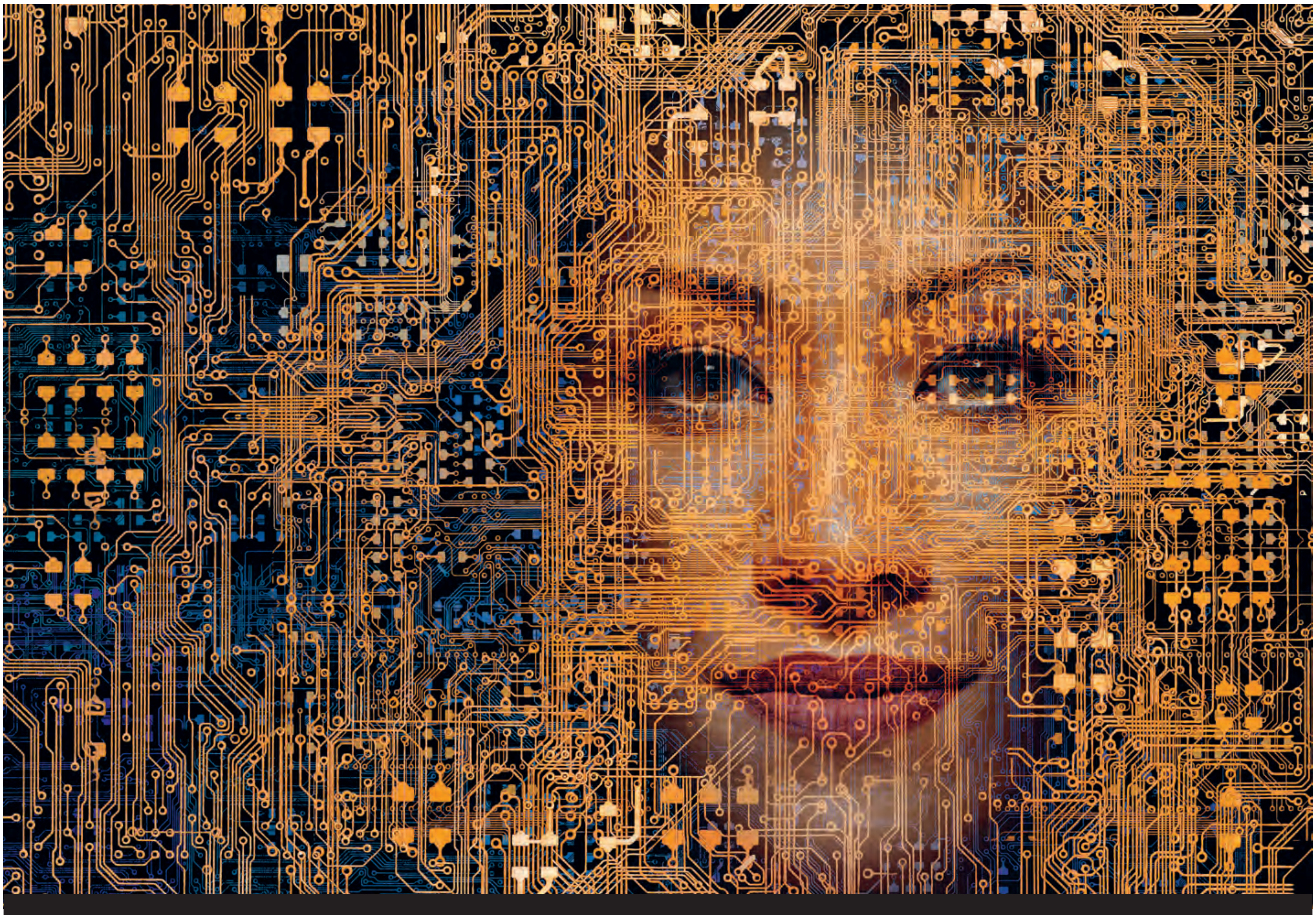

As we settle into ongoing hybrid work environments, zero trust is becoming the only option for keeping the remote office safe, writes **Roisin Kiberd**

IN ZERO TRUST WE TRUST

Confucius, apparently, once said that "it is more shameful to distrust our friends than it is to be betrayed by them". But then, do we really know that he said that? Perhaps we should distrust our friends, and distrust the source of this Confucius quote too.

It pays to be sceptical – at least, that's the approach businesses are taking with cybersecurity in the wake of the pandemic. With new legislation being drafted to protect those working from home, and the Omicron variant continuing to wreak havoc on the nation's sinuses, organisations are pursuing the zero trust approach, a security framework which relies on verifying the user's identity at every step, and only granting them access to exactly what they need – no more, and no less – at any given time.

The traditional office is gone, and with it the perimeter, the clear line of defence cybersecurity experts were once able to construct around a business. Now data floats freely between devices, some personal and some corporate-owned, and employees can work from anywhere, connecting to wifi in coffee shops and on trains more often than they make use of an office network. Unlike traditional, perimeter-based security, zero trust can accommodate a mobile workforce.

"Security risks are obviously greater as we have moved massively to a work-from-home environment," Rob Norton, chief technology officer at Paradyn, a provider of IT security services and consultancy, said.

Paul Donegan, country manager for Ireland at Palo Alto Networks
Picture: Chris Bellew

While organisations have adjusted their security policies to reflect the fractured nature of Covid-era work, they're struggling to keep pace with criminal attacks.

"Social engineering is on the rise and training should be provided around identifying fraudulent emails. A recent report (published by Barracuda Networks) indicated a spike of over 600 per cent increase in email phishing attacks," Norton said.

There's also the risk of lost or compromised devices; if they can't be wiped remotely, organisations risk losing sight, and control, of crucial data.

"The biggest thing we've seen is more and more reliance on emails," said Karl Curran, director and head of mergers and acquisitions and transaction solutions at Aon Ireland, a global professional-services firm specialising in risk mitigation.

"In a traditional work environment you might call over to a colleague to talk about something, but now everything happens over email, and the amount of phishing and targeted attacks we've seen has increased exponentially since the beginning of the pandemic."

This rising number of cyber attacks, in particular ransomware, preyed on businesses still coming to terms with other cultural shifts, including the widespread adoption of cloud computing.

"The big risk is that employees are accessing sensitive data systems from often insecure and unpatched assets," Ronan Murphy, chief executive officer and founder of SmartTech247, a leading international cybersecurity firm, said.

"The huge increase in successful cyber attacks during the pandemic has shown us that there are gaps in the ability of organisations to implement adequate security controls with remote work."

A state of mind

Zero trust can fill in these gaps. The first step is understanding what it means, and what version of it will work for you. As with cybersecurity in general, technology can only go so far here. Experts advise that zero trust is as much a state of mind as it is an approach to security architecture.

> *Experts advise that zero trust is as much a state of mind as it is an approach to security architecture*

Karl Curran of Aon Ireland: 'We've seen more and more reliance on emails'

"We're seeing technologies built to be robust and to minimise the impact of attacks, but that can only go so far," said Michael Conway, director of Renaissance, specialists in business continuity and ICT security as well as training and accreditation.

"That's the whole point with the zero trust model; no one is trusted to do anything. You need to work out the minimum that each person within the organisation needs access to. That means knowing what data you have, and managing it dynamically."

Paul Donegan, country manager for Ireland at Palo Alto Networks, characterised zero trust as "a strategic approach to secure an organisation by eliminating implicit trust and continuously validating every stage of a digital interaction".

"Instead of trusting particular devices or connections from certain places, zero trust demands proof that people, devices, or connections should be granted that access."

With John Kindervag, regarded as the godfather of zero trust, working for several years at Palo Alto Networks as field chief technology ➡

▶▶ PROFILE: Exertis

COMMERCIAL CONTENT

Four times the storage from Dell's fully automated array

Dell PowerStore all-flash data storage appliances offer intelligent and scalable storage for today's high-performance applications

Whether for critical databases, highly transactional applications or ERP, businesses always need more storage capacity and performance, but enterprise-grade solutions have often been out of reach. Today, this has changed.

PowerStore from Dell Technologies brings intelligence to the storage array: the cost-and-space-efficient storage solution is fully programmable, and runs autonomously, meaning labour-intensive processes such as initial volume, placement, migrations, load balancing and issue resolution are automated by PowerStore's onboard machine learning (ML) engine. In addition, CloudIQ proactive health and cybersecurity analytics are built in.

It also does this at a price point that makes this kind of enterprise-grade technology widely available.

"PowerStore is designed to work for everyone from entry-level small and medium businesses (SMBs) right up to the enterprise," said Colin Boyd, datacentre sales manager, Dell Technologies Ireland.

Crucially, PowerStore provides data reduction at a guaranteed ratio of 4:1, doing so through always-on, in-line de-duplication and compression.

"It's fully automated and it's built right in, and we go to great lengths to guarantee that to our customers," he said.

The cost savings and performance achievements achieved by this alone are significant, but PowerStore is also an ideal technology to scale with business.

Scale up and scale out

Unlike traditional arrays, PowerStore is designed to grow with businesses, and so expanding the capabilities of your initial PowerStore configuration is simple and efficient with capacity and performance able to be scaled independently.

"There is a very high ceiling on capacity – each appliance can grow to over 2.8PB in size, and you can also add more nodes to further improve performance," Boyd said.

This is crucial as data becomes more and more central to business, and the world as a whole is hurtling towards an ever more digital future. The amount of data we generate is growing rapidly, and it needs to be stored, kept safe, retrieved, deleted when required by law and, most of all, processed.

Running traditional and modern application workloads, relational databases or virtualised ERP and electronic medical record applications directly on the array is possible thanks to the innovative AppsON functionality, making them portable, agile and fast. VMware investments are also extended as the PowerStore array is designed with an integrated VMware ESXi hypervisor.

Overall, Dell PowerStore storage arrays are seven times faster than previous arrays, with up to three times faster response time.

PowerStore is also easy to use, and its management interface, PowerStore Manager, has been built with the administrator in mind. Using browser-native HTML5, PowerStore Manager can be used across various operating systems and web browsers without requiring an external management server or appliance.

This kind of flexibility is only available with PowerStore, and Dell Technologies has been noticed in the business world.

"The most interesting statistic is that 23 per cent of all PowerStore customers globally have not previously bought Dell Technologies Storage," Boyd said.

Colin Boyd, datacentre sales manager, Dell Technologies Ireland

What businesses like is that not only can they easily complement and extend their existing investments with PowerStore's uniquely adaptable storage solution, it also offers cost certainty.

"The PowerStore proposition is unique to the market. We underpin the contract with a future-proof loyalty programme, guaranteeing the 4:1 data reduction ratio with a three-year satisfaction guarantee, anytime upgrades and a clear price for the future cost of maintenance," Boyd said.

For more details on the Dell Storage Portfolio including PowerStore visit: https://www.exertis.ie/dellstorage

exertis

officer, the firm has long promoted the approach, and is able to customise it for each organisation.

"Adoption is different for everyone. Organisations need to define the attack surface and the different policies around it, and then define exactly what zero trust means to them. It depends where their most valuable data sits, and where they are on their journey," Donegan said.

While zero trust has a reputation as one of the most demanding approaches to cybersecurity, in terms of both effort and the resources it requires, experts said that there's a version for everyone.

"There are standards for a zero-trust architecture such as the NIST 800-207 (Zero Trust Architecture)," Norton said, "but organisations often select the most appropriate elements that are both affordable and practical to implement."

While stressing that zero trust is rarely a one-size-fits-all solution, Norton listed common traits in deployments. "The entire enterprise private network is not considered an implicit trust zone, and no resource is inherently trusted," he said. "Not all enterprise resources are on enterprise-owned infrastructure, and remote enterprise subjects and assets cannot fully trust their local network connection."

Devices, too, are rarely owned or configured by the enterprise; zero trust is an ideal policy for bring-your-own-device workplaces.

Rob Norton, chief technology officer at Paradyn: 'Social engineering is on the rise'

A race against the cyber criminals

Experts have long held the view that cyber attacks are not a matter of if, but when; they cannot be averted, and can only be prepared for. By implementing zero trust, you can radically reduce the damage done by criminals infiltrating your system, also cutting down on the time it takes to recover.

In this ongoing, possibly never-ending arms race against cyber criminals, firewalls will only get you so far. Zero trust is a safeguard; the criminal can break in, but they won't get very far.

"The evidence suggests that cybercriminals have reached such a level of sophistication that they can get access to networks irrespective of security controls," Murphy said.

"But when it's done correctly, zero trust plays its part by dramatically reducing the access to critical data and critical assets."

All this talk of 'not if, but when' might sound pessimistic, but consider the landscape: 2021 saw a surge in ransomware attacks; the average ransom paid to cyber criminals rose to $570,000 early in the year, with industrial goods and services companies, universities and health services, including Ireland's HSE, among the most popular targets.

One US-based insurer, CNA Financial, even shelled out $40 million to recover its data, believed to be the largest ransomware payment made to date.

"Ransomware, over the last ten to 11 quarters, has increased by over 400 per cent. One of the phenomena we've seen is that a few years ago the attacks were less targeted, but now they're against specific companies, and there's ransomware-as-a-service to contend with," Curran said.

"It's becoming an industry in itself, with seven to eight-figure losses for many Irish companies."

Late last year, the US Department of Defence announced the creation of a new office at the Pentagon, dedicated to advancing the zero trust security model.

Coupled with the increase in cyber crime, and its very visible damage to brand reputations, this development has helped convince industry leaders to take zero trust seriously.

"Multinationals are talking about zero trust at a board level, rather than how it was in the past, with mid-level management attempting to convince them," said Donegan.

"With Irish organisations, a lot of them have very flat structures. With the legacy idea of senior managers having access to everything, that fear of them losing access is finally starting to fall away thanks to the visibility of cyber attacks."

Donegan even said that organisations that previously considered themselves too small to be attacked have returned

> *Late last year, the US Department of Defence announced the creation of a new office at the Pentagon, dedicated to advancing the zero trust security model*

ZERO TRUST: A GLOSSARY

Multi-factor authentication: familiar to users of Gmail and social media, this method demands more than one piece of evidence to authenticate users and grant them access to a service (ie in addition to a password, it requires a one-time code sent to the user's phone).
Conditional access: an 'if-then' system requiring that certain criteria are met (ie device type, location, time of login or device settings) before the user is allowed access.

Single-sign on facilities: a session and user authentication service that allows access to multiple applications with one set of login credentials. Examples include OpenID and SAML.

XDR: An acronym for 'extended detection and response', this solution correlates data across the security layers of your business, including email, endpoints and cloud workload, to rapidly detect any threats.
MTR: Another acronym, this time for 'managed threat detection and response', this option involves an expert team managing threat detection as a service, alerting businesses in real time and taking action to neutralise threats on their behalf.

UEBA: 'User and entity behaviour analytics' implies the gathering of information on network events day-to-day. The 'entities' in question include routers, servers and any potentially malicious applications.

seeking advice after falling prey to phishing and ransomware.

"John (Kindervag) always made the point that it wasn't about defining the attack surface; it's about defining the protect surface, and in order to do that you need buy-in across the organisation. The most important part of that is having the board and senior management on side."

Winning the faith of board members is one task; convincing them to assign a substantial budget to security is another. Curran made the point that each organisation will have competing interests within it.

"A lot of boards and C-suite level people will be concerned about what a really bad day at the office looks like; what we term a 'doomsday event'. What does that look like, in terms of balance sheets?"

While this might be difficult for an IT team to articulate, Aon, and others, can help bridge the communication gap between teams.

"With really large organisations they can actually be quite fragmented," Curran said, "and that can be an attacker's dream – especially if there are different security standards within different divisions of an organisation."

Part of the appeal is that zero trust can be supported with automation – in fact, AI might be the only way to keep up with the dynamic permissions management that zero trust requires, not least in the face of a global shortage of cybersecurity professionals.

"A lot of the investments organisations previously made were in legacy point solutions, and now there's a lack of personnel on the market who are able to understand these technologies," Donegan said.

"Technologies that make use of interoperability, and use machine learning and AI to stitch everything together will be very important in the near future, so that organisations will be able to use their machines to fight criminals' machines."

Conway made the point that while automation can certainly help with zero-trust, organisations should choose their solutions carefully.

"It can be automated to a significant degree, but you have to choose the right kind of technologies and the right solutions. You need to find technologies designed for this; it's not something people tend to be able to manage manually, and it's not something traditional authentication can do."

A recent Security Magazine survey of more than 250 chief information security officers found that the majority of those surveyed viewed zero trust as a critical security approach.

In a relatively short window of time, zero trust has grown from an approach favoured by the highest-risk industries, handling the most sensitive data, to one that many see as inevitable for any and all organisations operating online.

"I fundamentally believe that every business should evaluate implementation of zero trust security," Murphy said. "Irrespective of an organisation's size, the threats remain prevalent."

Murphy went on to predict that while the approach is suitable to most businesses, it's unlikely to work without buy-in from the top down: "Typically the type of business that will struggle to implement zero trust is one where cybersecurity is not high on the leadership agenda."

Curran mentioned work within Aon aiming to identify the patterns and behaviours of 'winners' and 'losers' after cyber attacks; businesses that recovered quickly, and successfully contained the damage to their systems, were characterised by their strong leadership.

"We looked at over 1,500 cyber incidents, and there are certain qualities the winners display; preparedness is the first one, a real commitment to loss prevention and mitigating risk. Leadership is another; it needs to be strong and visible. Communication, accurate and coordinated, is another."

Underlying vulnerabilities

A cyber incident will expose any underlying vulnerabilities in any organisation.

"No organisation can prevent this. We tell people to prepare for the expected, not the unexpected, and there's lots of data and evidence that well-prepared companies are able to weather this threat," Curran said.

A ready replacement for VPNs and traditional remote access models, zero trust was designed to replicate the security employees could once count on behind traditional perimeter controls.

"Networks from the 1990s and 2000s are no longer fit for purpose; they allow you all in or they keep you all out," Conway said. Adopting zero trust now will not only prepare your business for cyber attacks, but will afford you resilience and adaptability into the future.

"For modern workspaces, with flexible working, you need a different environment," Conway said. "The pandemic has sped up a lot of this, but also cloud computing changed everything. We're going to see zero trust everywhere, soon, in some guise."

The final part of this puzzle is training; as with all cybersecurity measures, technology can only take you so far. Implementing a zero-trust architecture will limit the damage if your network is infiltrated by criminals, but only awareness training can prevent them from getting in, in the first place.

"A lot of people rely on technology to solve these issues. We don't think you can do that; it needs to be about people and process, because people and processes are what allow these attacks to get in in the first place," Curran said.

"I think the focus needs to shift away from instant response and recovery to a more proactive approach based on three things: identity, detection and protection."

Curran called for a shift in thinking, away from believing that security is something that can be fixed once, or irregularly, and then left alone, to viewing it as an ongoing task.

"Within Aon we have a simple method; we call it 'cyber loop', meaning that the strategy is ongoing. It's not a linear process; there is no beginning or end."

For this reason, any zero trust measures need to be paired with a dedicated staff training programme, and a prioritisation of cybersecurity in the organisations as a whole.

"It's about adopting the right way of thinking around the user, the application and the infrastructure," said Donegan. "Zero trust is a mindset, as opposed to any given technology."