PORTSYS®

TotalAccessControl™

THE BIDEN EXECUTIVE ORDER: IT'S ABOUT TIME

Zero Trust is no longer tech marketing hype. That much is crystal clear.

It's been clear to those of us fighting hackers in the cybersecurity world for quite a while.

And it's obviously clear to the Federal Government now, with the release of President Biden's Executive Order on Improving the Nation's Cyber Security…

And before that, with the release of the National Security Agency Zero Trust Guidelines…

And before that, with the release of NIST Special Publication 800-207 on deployment models and use cases for Zero Trust.

If you didn't know it before, you know now that the most targeted attack surface in the world – the U.S. Federal Government – is planting a Zero Trust flag securely in the ground. Zero Trust is now an absolute requirement. Not a nice to have. Not a when we get to it. Not a 2025 goal. Not even a 2024 or 2023 goal.

Zero Trust's time is here. Now. This is the inflection point.

And it's about time…in more ways than one.

TIME TO WIN THE CYBERWAR

The fact that the Federal Government has now put forth a significant Zero Trust initiative speaks volumes. Government agencies are not typically known as being IT trailblazers – they tend, with some exceptions, to follow the business world. They too often have been reactionary, not proactive.

But this is a government action that everyone should applaud. For once, the Federal Government is far ahead of much of the business sector.

The Biden Administration's Executive Order (See Digital Battlefield sidebar at right), as well as the NSA guidelines and NIST special publication last year, may have been overdue; but they are well-written, developed in the right spirit, provide an excellent roadmap, and ultimately build a stable foundation to transform the way Federal government agencies – and indeed any organization – can transform their IT security.

As the Executive Order outlines, the Zero Trust architecture security model and system design principles combine to form a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. Zero Trust brings together comprehensive security monitoring, granular risk-based access controls, and system security automation across all aspects of an organization's infrastructure to protect critical data against the relentless onslaught of threats we face in today's perimeterless world.

BIDEN'S EXECUTIVE ORDER: DESIGNED FOR TODAY'S DIGITAL BATTLEFIELD

Despite the rapid response of the Biden Administration to the DarkSide ransomware attack on the Colonial Pipeline, the cyberthreat to our government and business world isn't new. The extreme damage hackers could cause to our critical infrastructure, the financial losses they generate in our economy, the danger to life and limb they pose to patients in healthcare facilities around the world, the sheer depth and breadth of the attacks – these digital threats have been growing exponentially and pretty much unchecked for some time now.

The targeted Colonial Pipeline attack is the most recent example of a long history of attacks dating back decades that finally shook a usually ponderous and pedantic Federal bureaucracy into such urgent immediate action this month – prior to that was the global software supply chain SolarWinds Orion attack; which was preceded by the Hafnium hack into Exchange servers around the world; which was preceded by the Equifax breach in 2017; which was preceded by the 2015 breach of the U.S. Office of Personnel and Management in 2015; which was preceded by several state-sponsored attacks against the U.S. and UK governments since at least 2003, and undoubtedly earlier. There are thousands to choose from.

You get the picture. The full scope and number of these relentless attacks are too long to list here. Yet the global attack surface became even more vulnerable with the Work From Home (WFH) migration of employees away from government and company offices during the Covid-19 pandemic.

This approach "eliminates implicit trust in any one element, node, or service," as the Executive Order states. Instead, a Zero Trust approach – when implemented correctly – will continuously verify in real time every end user's full context of access, and not just their credentials. Situations change and people need to get access through different devices and under different circumstances. Any organization's security profile needs to adapt to all these variables and know the difference between acceptable and unacceptable requests for access.

Validating users' context of access (devices, security status of the devices, locations, and much more), combined with security policies for every resource that defines what is acceptable and what is not, are key to properly securing access to any enterprise organization's resources. This focus on access for each resource flips the traditional concept of IT security on its head, isolating each resource and segmenting the organization's internal infrastructure. This approach not only strengthens the infrastructure but makes it easier for users to access their resources through one consistent user interface.

Organizations we work with to implement a Zero Trust Access approach allow users access only to the minimum amount of resources they need to perform their jobs. If users do not meet the specific requirements for access for each resource, or if it is an attack by a hacker, they are not able to gain access. However, even if a hacker was able to use stolen credentials and get past the multifactor authentication and pass other device-specific checks, an access-focused Zero Trust approach leverages segmentation principles to ensure the damage is contained. First by limiting access to only the specific resources they should have access to under their current circumstance; and second, by having the users captive within the applications they have access to, rather than providing them with access to the entire network.

Zero Trust Access constantly limits access to only what is needed for a specific, fully authenticated official purpose. That enables any organization to significantly mitigate the amount of anomalous or malicious acts it is exposed to across its hybrid infrastructure.

A sample of the pandemic's impact on our IT infrastructure: ransomware attacks against critical infrastructure were up 93 percent in 2020 alone, accounting for 396 documented attacks, according to a report from Temple University. And those are just the attacks that have been reported. Many, many more go unreported.

Enterprise IT teams, both public and private, have been fighting this losing battle for so long now because they still rely far too much on reactive measures mostly focused on security's three R's": remediation, resolution and recovery. Colonial Pipeline is not alone when its infrastructure is described as something that "an eighth-grader could hack into."

Honestly, the aging legacy architecture most enterprises have in place today make them easy targets for hackers of any age. These legacy architectures simply were not designed for the 21st Century Digital Business Battlefield, in which all organizations must constantly guard against ransomware, malware, phishing, man-in-the-middle, dictionary and business email compromise (BEC) attacks… just to name a few.

It's way past time for a much stronger proactive approach to deal with the root cause: it is simply too easy for evil-doers to gain access to our proprietary network resources and applications, whether they are local, web-based, or in the cloud. That's why the Zero Trust approach being embraced by the Biden Administration is so critical to help organizations around the world – not just U.S. government agencies – to win this era's war on the cyber battlefield.

Time Matters

Time is money. This is true now more than ever when it comes to strengthening the Federal Government's IT security profile. The uber-distributed, massively-matrixed infrastructure powering the U.S. government around the globe – and even into Deep Space – demonstrates this as well as any organization in business today.

Federal agencies, with their aging, archaic architectures, basically have one of everything. If you want old legacy applications, they have them. If you want client server applications, they have them. If you want modern web-based applications, yes, they have those too.

Those mission-critical resources have become even more vulnerable during the pandemic. Many Federal agencies, partners and contractors rely on legacy remote access technologies such as VPNs – technologies that weren't designed for the types of threats we see today. The security solutions used for those decades-old remote access technologies lack the high levels of sophisticated segmentation needed to mitigate the lateral movement of these attacks across the infrastructure.

INCLUSIVITY: THE OVERLOOKED KEY TO ZERO TRUST

Inclusivity – the percentage of your existing infrastructure that can be protected through a Zero Trust approach – is the biggest key to any successful deployment of a Zero Trust solution.

Why is inclusivity so important? If you deploy a solution that can only protect some of your resources, you are still left with a patchwork of protection with multiple different products controlling access. This is a situation many organizations find themselves in today, despite repeatedly investing huge amounts for the past two or three decades across their IT security portfolio.

Even with all that investment of time and money, many organizations still find these solutions that claim to be Zero Trust are only partially effective. A good example of this is the experience many have when they turn to the cloud as the Holy Grail for their Zero Trust strategy.

Yes, cloud-based solutions work well for cloud applications, but they often fall short with on-premise resources and do not help you close attack vectors, such as open ports on your firewalls. Also, most of the Zero Trust cloud solutions only protect web-based applications. That's not practical for the vast majority of larger organizations and federal agencies who have a wide-ranging assortment of resources to protect – legacy applications, client-server applications, virtual desktop infrastructures, and more. That's why many organizations still struggle, just to find at the end of their rollout that they can only implement a partial approach to Zero Trust. The biggest contributing factor to those struggles is that they didn't first identify the correct critical factors needed to determine the best Zero Trust approach. Most organizations today require a Zero Trust

They simply drop users directly onto the internal network, opening even more opportunities to spread additional carnage across your resources – both local and cloud.

Federal agencies would also be wise to not overlook the needs of the end users in any Zero Trust deployment. The challenge isn't to make their lives more complicated with even more IT security hoops to jump through; the challenge is to make their lives much easier by seamlessly improving and simplifying the ways they gain access to information, while at the same time making the agency's infrastructure much more secure.

Both data-focused and access-focused approaches to Zero Trust (see ***Inclusivity sidebar at right***) can help any government agency, or any business for that matter, to effectively manage the oft-conflicting demands of these diverse digital ecosystems – the yin and yang of security vs. productivity.

strategy that fully addresses the complex and complicated access needs of their local and cloud-based resources – one that doesn't take years to launch and along the way makes lives for their end users and admins much easier.

Why is it that so many organizations still struggle with these Zero Trust decisions? A big reason is that Zero Trust, to a great degree, has become a nebulous term since it was first introduced as a security strategy more than a decade ago. For instance, at the 2020 RSA Conference, there were more than 90 vendors who claimed to provide some form of Zero Trust solution.

These Zero Trust products can generally be broken down into three specific categories: identify-focused, data-focused, and access-focused. While they have some common threads, there are significant deviations when it comes to their effectiveness, inclusivity, and ability to deploy – all of which have serious implications for safeguarding your critical resources across the enterprise.

- Identity-focused solutions have a narrow focus on shoring up identity and are typically too limited for the challenges outlined in the recent Biden Administration Executive Order. While shoring up identity is good, these solutions simply provide much too light of a touch to comprehensively address the complex security needs of any large matrixed organization today.
- Data-focused solutions, on the other hand, provide a significantly more robust approach. But that more in-depth approach comes with a big caveat: they usually require a huge, years-long effort to implement. And even then, these solutions do little to nothing to

But if it takes years to implement a Zero Trust solution, as often happens with the data-focused approach, that is valuable time these agencies will never recover. Meanwhile, they will continue to be exposed until their Zero Trust implementations go live and are fully implemented.

What is the cost of that risk exposure over such a lengthy period worth to the government, or any enterprise organization? Especially as the frequency and sophistication of the attacks continue to rise?

An access-focused approach fully addresses these challenges in the least amount of time when you compare the three types of Zero Trust solutions in use today. The longer it takes to deploy Zero Trust, the harder and more expensive it is to deploy Zero Trust, the more at risk these Federal agencies' archaic IT infrastructures will remain.

That's why the Biden Administration set such hyperaggressive timelines for implementing Zero Trust. They know that time is money – both when it comes to implementing Zero Trust, and when it comes to preventing cyberattacks.

Simply put, time matters. Time to deployment matters.

Time to security matters.

And time to Zero Trust matters. Now, more than ever.

improve the end user's experience. Worse, they don't truly focus on the root cause of your security gaps: controlling access. Data-focused solutions just control access to your data, so hackers can still roam free inside your infrastructure if they are able to get in somehow. And even then, if all your data is locked up tight – not an easy get for such a huge undertaking – there are still malicious activities that hackers can engage in while moving laterally across your infrastructure, both on-premise and in the cloud.

- Access-focused solutions offer the best of both worlds – shoring up authentication, protecting access both on-premise and in the cloud, and enabling quick implementation of Zero Trust across any enterprise. A Zero Trust Access approach can be up and running within mere days or weeks, instead of months or years – without having to rip and replace your existing IT security infrastructure, and all while strengthening your security. Their Single Sign On (SSO) technologies seamlessly authenticate access requests in real time, making life much easier for end users and administrators alike so they can focus on being productive instead of spending so much time trying to remember passwords or calling the Help Desk to reset their credentials over and over.

To learn more, visit www.portsys.com

View a Demo of TAC at
www.portsys.com/watch_demo

US: + 1 781-996-4900

UK: + 44 208 196 2420

www.portsys.com

AS THE FEDERAL GOVERNMENT MOVES FORWARD UNDER THE BIDEN ADMINISTRATION'S EXECUTIVE ORDER, ITS AGENCIES WOULD BE WELL ADVISED TO KEEP IN MIND THE IMPORTANCE INCLUSIVITY PLAYS WHEN IT COMES TO DECIDING WHICHEVER ZERO TRUST APPROACH IT WILL USE.