Enterprise Buyers Guide

Transform Your Security, Transform Your Business with Zero Trust Access

TotalAccessControl™

PORTSYS®

Table of Contents

TotalAccessControl™

PORTSYS®

How TAC Hits All the Marks on Your Shifting Security Priorities

As part of its Strategic Security Survey, Informa's *Dark Reading* asked IT and security professionals how future budget priorities are shifting during the pandemic.

Respondents cited 13 areas that they predict will get the highest priority going forward, all as a result of the Covid-19 pandemic – the greatest impact a single event has had on IT budget priorities in the survey's history.

"AND THE IMPACT OF THOSE CHANGES — INITIALLY THOUGHT TO BE TEMPORARY — IS NOW VIEWED AS A SEA CHANGE IN BUSINESS COMMUNICATIONS."

The question to ask is: *How prepared is your organization to address this sea change to transform your security and your business for success over the long term?*

TotalAccessControl™

Total Access Control (TAC) from PortSys addresses 11 of the top 13 top priority areas cited by survey respondents – *all in one consolidated Zero Trust Access Control solution. (Box at right)*

Today, organizations are overrun by one-off security solutions – for two-factor authentication, single sign-on (SSO), administrator access, partner access, customer access, file access, VPN, mobile device management, cloud access, RDP. The list goes on and on, with seemingly no end in sight.

It doesn't have to be that way. Read this buyers guide to learn how TAC can help your enterprise organization to more cost-effectively and securely address each of these priorities – all in one unified Zero Trust Access Control solution.

PRIORITIZATION OF SECURITY PROJECTS

(Listed in Ranked Order)

- Remote Access Systems
- VPNs
- Authentication
- Phishing/Social Engineering Protection
- Cloud Security
- Endpoint Security
- Network Security
  (Particularly Remote Connections)
- End User Security Awareness*
- Mobile Security
- Insider Threat Protection
- Application Security
- Encryption
- E-Commerce Security*

**NOTE: TAC Does Not Directly Address End-User Security Awareness Programs or e-Commerce Security.*

Source: Informa Dark Reading, 2020 Strategic Security Survey

Remote Access Systems

Prior to the pandemic, **44% of companies around the globe didn't allow remote work**. Worldwide, **just 2.8% of the workforce worked from home at least half the time**.

Those numbers were flipped when the pandemic hit, and as the survey indicates, they don't show any signs of reverting. However, the remote access systems most organizations rely on today – VPNs and Virtual Desktop Infrastructure (VDI) such as RDP – are not viable long-term solutions when it comes to performance and security.

One of the most common attack vectors is using an organization's own valid credentials to gain access. These are obtained by phishing, dictionary attacks, brute force attacks or even bought on the dark web. These attacks are invisible to most enterprise organizations, since the hacker looks like a normal user. Enterprise VPN vulnerabilities from four of the most well-known vendors – Pulse Secure, Fortinet, Palo Alto and Citrix – have all been exploited in the wild by hackers and nation-states using these methods. RDP, meanwhile, continues to be the most significant attack vector from which hackers can launch ransomware attacks.

Why do these attacks continue to succeed? The archaic perimeter defense schemes of yesteryear are still being used by many organizations today. When hackers use valid credentials to attack remotely, they flow right past those legacy perimeter defenses to the soft and gooey middle of your infrastructure. From there they have minimal hurdles to clear, because the assets they are after are directly available – or they simply need to crack the passwords on them, too.

Total Access Control, on the other hand, securely delivers a simpler yet richer experience to your remote users. TAC does this much more securely than VPN and VDI solutions, through a browser on any device. TAC's reverse proxy gateway sits between your remote users and the resources they wish to access.

From there, TAC compares the access request to the organization's own security policies for each resource, and then provides access only to those resources (not the network) for which the end user has the proper permissions.

TAC also makes it much easier for end users by providing single sign-on (SSO) to resources regardless of whether they are locally based or hosted in the cloud. Opening public ports directly to resources through firewalls is no longer required since TAC's sophisticated security allows organizations to remove ports that previously were opened through their firewalls. This increases the scrutiny each request for access gets before allowing users access to those resources, which means automated scans won't find any open ports in the usual places. Simply put, hackers can't attack what they can't see.

CONTEXT OF ACCESS

TAC examines a remote user's entire context of access to:

- Validate User Credentials
- Use Multifactor Authentication
- Verify User's Type of Device & Security Status of Device
- Confirm Patch Levels Are Up to Date
- Confirm Certificates
- And Much More

VPNs

VPNs were never designed as a secure way to access networks. Way before ransomware, malware, and phishing, VPNs were just a way to connect the outside world to your inside network. But because VPNs drop users right on the network, hackers can quickly take advantage of those connections with credentials they steal through phishing attacks or product vulnerabilities, and then pivot to attack other resources and applications within your infrastructure.

VPNs don't conduct in-depth inspection of your traffic to keep your security posture strong. While some security measures have been added that go beyond just username and password credentials, the tradeoff is that those measures also create a tremendous drag on a VPN's throughput. And it's still not ideal from a security perspective.

The heavy connection a VPN uses requires significant bandwidth – a limited resource when entire workforces around the globe log in remotely. That's because VPNs connect at the network level, relying on standard communications as if users are still on the network in their offices back at HQ.

Total Access Control takes a different approach. Instead of working at the network level – which requires sending all your traffic back and forth across the Internet – TAC manages all the session and network interactions for your end users, without exposing your network on a wide basis to hackers.

All that transverses the internet with TAC is an optimized flow of screen traffic and minimal overhead. Even these exponentially smaller traffic flows are compressed and optimized through advanced algorithms and caching. The result is a much faster user experience with dramatically lower overhead than traditional VPNs, as well as reduced loads on application servers.

Organizations using TAC can also quickly and efficiently create and modify security policies. For instance, you may need to add permissions for a new group of users to gain access to certain applications. With TAC, you just add that group to the security policy for that application and they have access, provided they meet the security requirements you've instituted for that application. They no longer need access to the network; they now get access to the resources they qualify for and nothing more – creating the segmentation that prevents hackers from pivoting to attack other applications and resources.

Another issue for VPNs is the complexity of your network. VPNs often require clients to be installed on remote machines. TAC provides a secure and fast alternative that does not require a complex client like VPN solutions do. It can be run with either a light client or without any client at all, dramatically simplifying implementation and ongoing operations to be the primary access solution for all resources, local and cloud.

TAC's full reverse proxy engine also works fabulously for popular enterprise applications like SharePoint, while dramatically increasing security, significantly improving performance, and improving productivity over legacy VPNs.

Authentication

The old ways of relying solely on username and password are simply not enough today. It is far too easy to compromise a user's credentials, whether that is through a brute force or dictionary attack, or through a phishing attack.

Using just username/password for authentication purposes creates a significant security risk. But when Total Access Control combines those credentials with other factors of authentication, your infrastructure benefits from the strength of a Zero Trust Access Control approach – one that locks down your environment more securely – all while making access easier for fully authenticated end users.

TAC doesn't restrict you to one authentication repository. You have multiple ways to validate an end user, and these methods can be combined to provide more certainty in distinguishing your users from imposters. For example, you can combine Active Directory usernames and passwords with hardware device credentials, certificates, smartcards or even biometric authentication. And it's not limited to just these. You can combine many different factors of authentication, all without making it more difficult for your end users.

TAC also adds authentication or multifactor authentication to applications that don't support those added protections themselves. This can be especially important for legacy applications. Instead of having to rewrite those applications, TAC presents the authentication/validation before the user is allowed access to the applications, therefore implementing full vetting before the user can access any application. This also works well for cloud-based resources that do not natively support your choice for multi-factor authentication.

TAC provides more stringent controls over end users through device validation, if implemented. A user's credentials can be bound to the end-user's actual hardware device ID. The only way end users can access resources is to use approved devices bound to their accounts. This is very effective in protecting against phishing, brute force attacks or other credentials-based hacks. End users don't have to do anything extra to make this strong multi-factor authentication happen. TAC makes it all frictionless for end users, but the increase in security for your organization is substantial.

It is important to note that TAC also offers a robust suite of supported authentication solutions with which it easily integrates – including Active Directory, Radius, OKTA, Ping, ADFS, LDAP, SAML and much more. TAC also includes several multifactor authentication solutions and supports most multifactor products. *(See box below.)*

Of course, being able to vary the way you authenticate end users based on the risk they present to your organization is important. For example, if a user is trying to access protected resources from an unknown/untrusted device, you may choose to present additional verification for that end user. You can even vary the resources available to that user based on their risk, and this all happens dynamically through TAC without the need for intervention by administrators.

MFA SOLUTIONS

Supported

- RSA SecurID
- Safenet
- Swivel Secure
- Biometrics
- Vasco
- Smartcards
- DUO
- FIDO2

Included

- SMS Tokens
- Device Validation
- Push Notifications
- One-Time Passwords (OTP)
- SAML Tokens
- API Integrations

Protection against Phishing And Social Engineering Attacks

Most organizations still focus on fighting phishing and other social engineering attacks by educating users about what not to click on – an important first step in mitigating the all-too-human errors that can lead to significant breaches.

However, end users are still too ill-equipped to fight this battle on their own, regardless of how much security awareness training they receive. That's why hackers continue to refine their social engineering strategies for phishing, spearphishing or whaling, as well as for business e-mail compromise attacks.

Once hackers gain your users' credentials, the game is over before you even know it began. They can attack your valuable resources and applications with your users' own credentials. Then, when they are inside your infrastructure, hackers can use that breached account to pivot and attack even more assets, as well as target more high-profile end users for additional attacks.

Simply put, identity is not security. Yet that lesson hasn't sunk in everywhere. Major enterprise organizations continue to fall victim to these costly social engineering attempts, some of them multiple times.

As these attacks become increasingly more sophisticated, organizations using Total Access Control significantly reduce their end users' security burden. They accomplish this by seamlessly incorporating many transparent factors for authentication that more thoroughly protect enterprise resources than traditional user credentials. Hackers find it impossible to access your resources on all the factors that TAC considers, which is based on the end user's full context of access.

Hackers are getting much more sophisticated with their social engineering attacks, making it increasingly challenging for even the best-trained end user to discern when they are being targeted. It's always good to provide security awareness training, but when that fails – and it will – it's important to have a solid strategy in place to manage those failures. TAC takes the burden for preventing these attacks off your end users, while greatly improving security.

INTO THE BREACH

HOW MUCH DOES A BREACH REALLY COST?

2021 Average – $4.24 Million

That's the average cost of a data breach, according to the IBM Ponemon ***2021 Cost of a Data Breach Report***. The true cost can skyrocket far past this amount (*see Equifax example below*), since this doesn't take into account the damage to a brand's reputation or other market factors that could add to the loss.

Equifax – $2.4 Billion

Equifax agreed in 2021 to settle a class action lawsuit coming out of its 2017 data breach for $1.4 billion. But that wasn't all:

- Moody's downgraded the company's credit outlook to negative because of the breach.
- Equifax agreed to spend $1 billion on data security over five years.

Cloud Security

Total Access Control brings together all access control for your organization in one place, strengthens the security you have, and allows you to protect your business the way you want to. You are no longer subject to the restrictions of cloud providers for managing access – TAC puts YOU back in control of your infrastructure, so you can take advantage of the most economical hosting solutions without disrupting your end users.

With TAC, your local and cloud security policies can be made consistent. Moving between a local datacenter and a cloud-hosted environment is easy with TAC, and your end users never have to know the difference.

TAC offers significantly stronger protection for cloud resources, such as Azure, Amazon Web Services, Microsoft 365, Exchange/Outlook, and SharePoint, to name just a few. It also works hand-in-hand with security mechanisms used by cloud service providers such as Microsoft, Citrix, Oracle/PeopleSoft, Salesforce, and many others.

TAC also protects access to your hosting infrastructure in the cloud. Typically, organizations could use RDP or something similar to gain access to the cloud infrastructure. This is problematic since RDP is generally only protected by username and password. Hackers routinely scan for RDP ports to gain access, because they know those ports provide easy entry into the root network, from where they can attack further.

TAC protects you from these types of attacks by making your RDP ports invisible to the outside world, while shoring up your access controls to make your cloud security profile much more robust at the same time.

To maintain both identity and access control for cloud and local resources in one central location, TAC provides integration support for cloud identity management vendors such as Okta Federated Identity and PingFederate. Using TAC's consolidated approach to authentication and access management, organizations can now more quickly deploy applications within their existing local infrastructure and into the cloud.

This integration support with cloud identity management vendors is especially important for the vast majority of enterprise organizations who today rely on Microsoft 365's productivity solutions. An organization can set its own customized security policies within TAC to determine, limit or prohibit access to valuable enterprise resources in cloud applications, such as those found in the Microsoft 365 suite.

TAC also protects your cloud applications from lockout situations – because it handles and defends against threats like brute force attacks, without those attacks ever reaching your cloud services provider. Only properly authenticated users can get access to your cloud resources through TAC.

Endpoint Security

Zero Trust Access isn't just about username and password. It's also about understanding the end user's full context of access, including the status of the endpoint.

For instance, you may not want a user working at your office to have the same access to your financial data when they are using the public WiFi in a coffee shop. Based on information about the user's context of access and endpoint, Total Access Control will dynamically vary the user experience.

With TAC, your organization can now validate the device the user is employing, the security status of that device (including antivirus and certificates), the exact location from where access is being requested, who is making the request, and more – all in one place. TAC then grants, denies, or limits access to critical resources wherever those resources reside. *(See box at right.)*

TAC creates microsegmentation by only providing access to the resources and applications themselves rather than the entire network. This also prevents lateral movement within your infrastructure if an attacker somehow gains entry with stolen end user credentials. TAC only allows users access to the resources for which they have been authorized.

TAC can also bind specific devices to that end user's account. The devices must be approved for use by an administrator before the user can gain access to any resource within your infrastructure. Once approved, the user must have both valid credentials and an approved hardware device before access is allowed.

A hacker may still be able to successfully learn a username and password. But with TAC's device-binding capability, the connection request would be denied, since the hacker wouldn't have the physical hardware device bound to that user.

TAC also makes it easy for administrators to quickly revoke the access privileges of a specific device – for example, if a mobile phone is lost but the end user still has an approved tablet or laptop. The administrator can block or fully or partially wipe a device; and if the device is later recovered, the administrator can then easily unwipe the device so the end user can quickly use it once again.

TAC's comprehensive endpoint inspection works seamlessly with the other multiple factors of authentication described in this guide to provide, simpler, stronger and more unified security across your enterprise, for both local and cloud resources.

ENDPOINT INSPECTION

Prior to granting access to any of your organization's resources and applications, TAC conducts a robust endpoint inspection that is transparent to the end user.

This comprehensive endpoint inspection determines whether the end user's context of access meets your organization's security policies regarding:

- Operating System
- Patch Level
- Hardware Device
- Current Anti-Virus
- Anti-Spyware
- Specific Installed Software
- Registry Key Entries
- Certificates
- Domain-joined Status
- Hidden Files
- Network Location
- Device Specifications
- PIN Code

... and more

Network Security

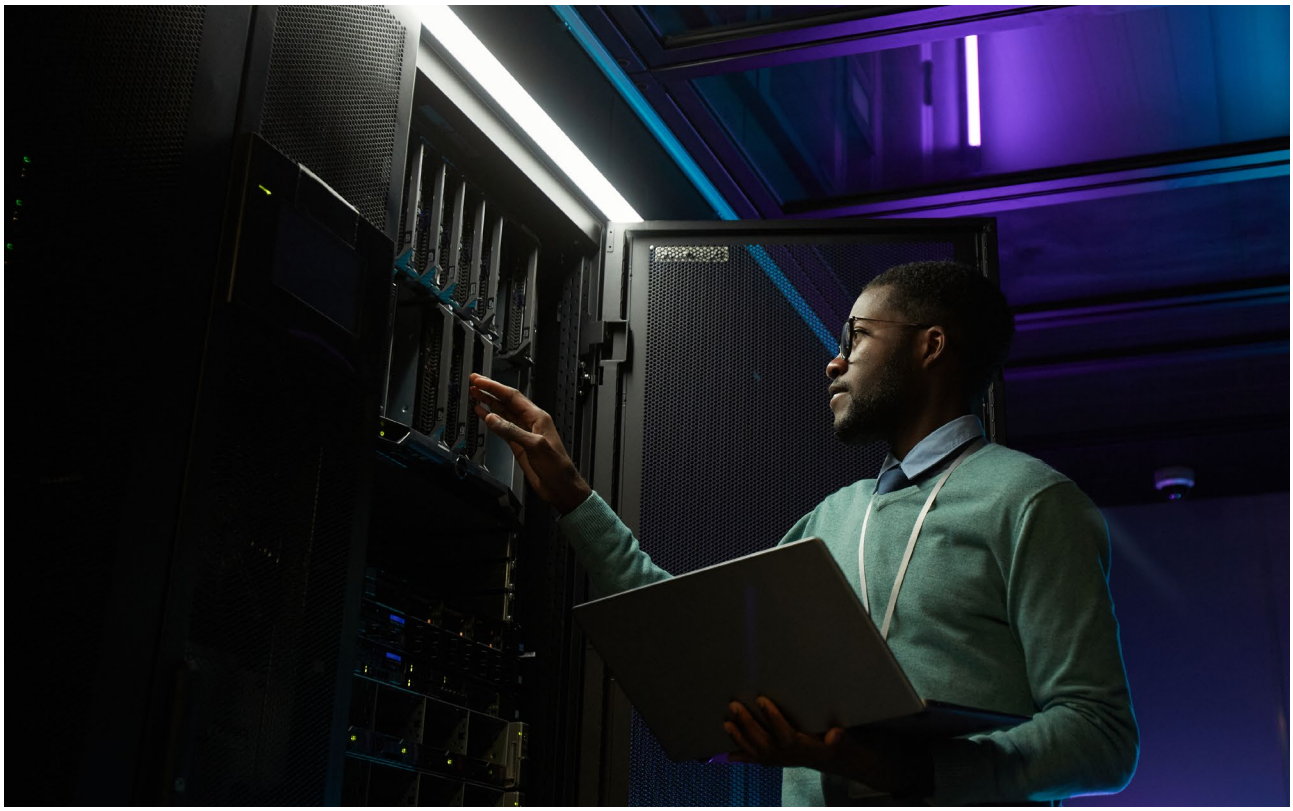
The ways most enterprise organizations secure their networks today are obsolete. They still focus too much on a perimeter-based approach. That may have worked for your legacy applications that were first rolled out two or three decades ago, but it doesn't work in today's perimeterless world, with cloud and web applications operating outside your corporate firewall.

Instead, Total Access Control's focus is on protecting your assets rather than your network, regardless of where they are. Think of it this way: the network is the plumbing that keeps your castle running; TAC protects your real crown jewels, the applications and resources.

Many enterprise organizations today still rely on a highly complex and segmented security infrastructure that is increasingly difficult to manage and more and more prone to leaving gaps for hackers to exploit. Different products are responsible for securing different parts of the network. The lack of a cohesive central product capable of controlling and communicating with all the different elements makes organizations vulnerable to attacks.

The result is a spider web of autonomous products that is expensive to maintain, difficult to manage, prone to breaches in security, challenging to keep updated properly, and relies on solutions that often don't even speak the same language. That's a hacker's Holy Grail.

With the explosion of distributed workforces around the world when the pandemic hit, organizations came to the full realization that their network security was more at risk than it had ever been. They now have a business imperative to provide their staff and business partners with a secure, stable, and user-friendly way to access all company applications, from anywhere, with any device.



Total Access Control meets that business imperative. At the heart of the TAC Gateway is a reverse proxy that sits between your end users and valuable company resources. A user can login from any device – whether corporate or BYOD – from any location, but can only see what has been authorized by the organization under the user's current situation. TAC dynamically examines the end user's access request against the access policies for each resource to provide very granular control over access to all resources, local and cloud. The result is a user-friendly secure login with a lot more security muscle behind it.

For instance, a user coming in on an untrusted device but with proper user credentials and multifactor authentication may only be able to view – and not edit – files remotely. Context of access is the key to being able to effect more granular security policies while keeping the end user experience simple and consistent.

When it comes to the "Next Normal" – where workers are increasingly logging in from outside the traditional office environment – TAC bolsters security while significantly reducing the exposure from network vulnerabilities that result from such a widely distributed workforce.

Even more important, TAC simplifies security for end-users and administrators alike by offering a single access security solution – instead of requiring you to deploy multiple solutions to address the long list of serious security challenges you face in today's rapidly evolving working world.

CONSOLIDATE YOUR NETWORK INFRASTRUCTURE

TAC achieves much stronger network security, especially for remote connections, by consolidating all these technologies into a single solution:

- VPNs
- Mobile Device Management
- Single Sign-On
- Cloud & Local Application Access
- Application Acceleration
- Portal-based Access
- GEO IP Intelligence
- Multifactor Authentication
- Role-based Access Control
- Centralized Auditing and Reporting
- Clientless RDP
- Always-On VPN
- Device Binding
- Device Validation
- Integrated Load Balancing
- SSH Network Services Protection
- Virtual Desktop Integration
- Global Configuration Synchronization

Mobile Security

Mobile security has taken on a much greater significance for enterprise organizations in today's socially distanced working world. Your organization has to secure access from an ever-growing mobile workforce using both personal and corporate devices in a way that enables the business while still effectively controlling risk.

So how does Total Access Control accomplish that? TAC's device approval process requires that each user device – whether it is a personal or corporate device – is approved by an administrator before that device is allowed to access any corporate information. This device validation is a strong but seamless additional factor of authentication that provides users frictionless access – applied consistently across both local and cloud applications.

By adding the device approval process to other robust multiple factors of authentication already within TAC, your organization can now leverage three full factors of authentication for the various devices your end users rely on to do their jobs without making it more difficult for them. This ensures a much greater level of security than is possible in most organizations today. A user's credentials – username and password – are combined with multifactor authentication and a specifically approved device, before allowing access to any resources or applications. All of this is done while making the sign-on process easier for the end user through TAC's web portal.

In addition to the device approval process, organizations can enforce device behavior by requiring a device PIN, facial recognition, other passwords, restricting access based on the device's operating system or patch level, or requiring the presence of an anti-virus running on the device.

TAC can also bind end users' various devices, both personal and corporate, to a specific account or group using services such as Active Directory. Once a device has been approved by an administrator and the end user has met the other multiple factors of authentication that TAC's proprietary security engine requires, the user can then access resources and applications – but only those resources or applications they are approved for, and not your entire network.

This all happens seamlessly for the end user. Of course, a hacker may still be able to successfully learn a username and password. But with TAC's device-binding capability and multifactor authentication, the connection request would be denied since the hacker wouldn't have the device bound to that user.

When it comes to mobile security, TAC provides a unified, user-friendly access experience that secures access to corporate resources regardless of where they reside, local or cloud.

Insider Threat Protection

According to ObserveIT, the average annual cost of insider threats has increased by a staggering 31% since 2019. Here's how the costs break down ***on average*** for each type of insider threat, according to ObserveIT's research:

Negligent Employees – $307,000

Malicious Employees – $756,000

Credential Theft – $871,000

In order to protect your organization from these costly insider threats, it is imperative that you get rid of your legacy security infrastructure. Here's why:

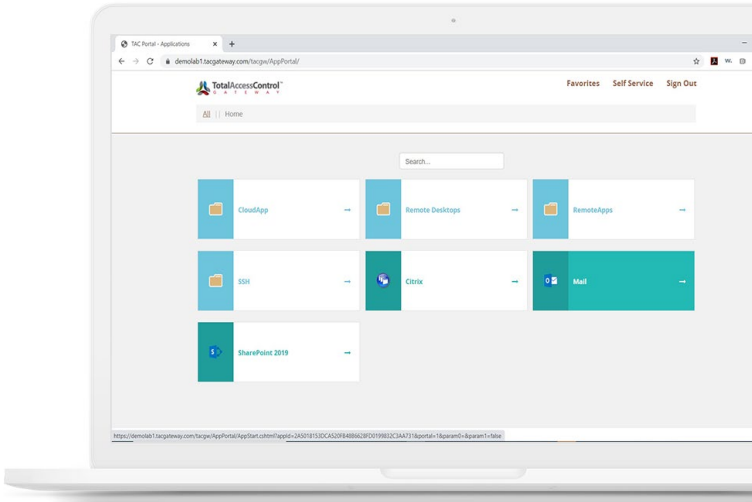
Most legacy infrastructure places an internal user right on the network. From there, an end user is free to go to whatever resources they wish. Of course, there are some levels of security in organizations, but they are often very inadequate. Plus, an insider or (or even a hacker who has gained access to your internal network) can pivot from what they are allowed to access and attack other resources that they are not supposed to gain access to. This can be as simple as guessing a username and password (or getting one via several methods from another valid user).

The issue with this legacy access design is that the user has too much access potential, otherwise called "latent risk." With Total Access Control, users do not get access to the network infrastructure. Rather, they get access just to the application resources that they qualify for.

Rather than connecting directly with the network where everything is potentially accessible, TAC creates microsegmentation – the key to TAC's Zero Trust approach to controlling access – which only provides the end user with access to application resources for which they have been approved. From there, an insider – or hacker with compromised credentials – cannot pivot to attack other resources or infect the organization with malware or ransomware.

TAC also provides administrators with comprehensive reports about all access requests for all resources and applications, both local and cloud, in one central location. These reports help highlight unusual access requests and suspicious activities, such as people logging in from unusual locations.

TAC's insider threat protection with microsegmentation and its comprehensive reporting changes the game for security across your infrastructure.



Application Security

TAC provides secure access to any application – local or cloud – from any device, acting as a reverse proxy for the applications it is protecting.

If your application security relies on username and password alone – whether we are talking about local, email or cloud-based applications – you are a prime target for hackers. Password crackers, brute force attacks and the current top preferred method, phishing, make it easy for bad actors to compromise the integrity of applications across your hybrid infrastructure.

Total Access Control goes far beyond an identity-based approach by examining multiple additional factors related to the end user's full context of access. The combination of all these factors creates a 3-dimensional profile of the user at that specific point in time to apply against the security policy engine your organization uses for access management.

The TAC gateway sits between your organization's application servers and your end users. Your users log in to the TAC gateway and it applies your security policies to determine if the user should be allowed access to the requested application server, whether it is hosted in a local datacenter or the cloud.

TAC examines the user's full context of access before granting access only to those applications for which the end user is authenticated. Or, if the user doesn't meet the security policies, TAC can deny any or some access, depending on the situation.

For instance, a user who is logging in remotely from an unsecure airport WiFi should not be granted the same level of access to your most valuable resources – such as downloading the CFO's draft report for the next quarterly earnings call, employee records in the HR department, or prospects and leads from the sales automation database. But with TAC, the user could still check email and gain read-only access to files they may need to continue working on the road.

In addition, not all end users are created equal. Some, such as a senior executive, may require full access to all corporate applications. Others, such as a web designer, may be privy to just a select number of applications focused on marketing.

Equally important, these Zero Trust authentication methods are done seamlessly for end users, who use TAC's web portal for secure one-click access to any of the local and cloud applications they need to do their jobs.

TAC's comprehensive approach to authentication, based on the user's full context of access, offers your organization a much stronger way to control all access to applications, local and cloud, and greatly improves protection of your entire infrastructure.

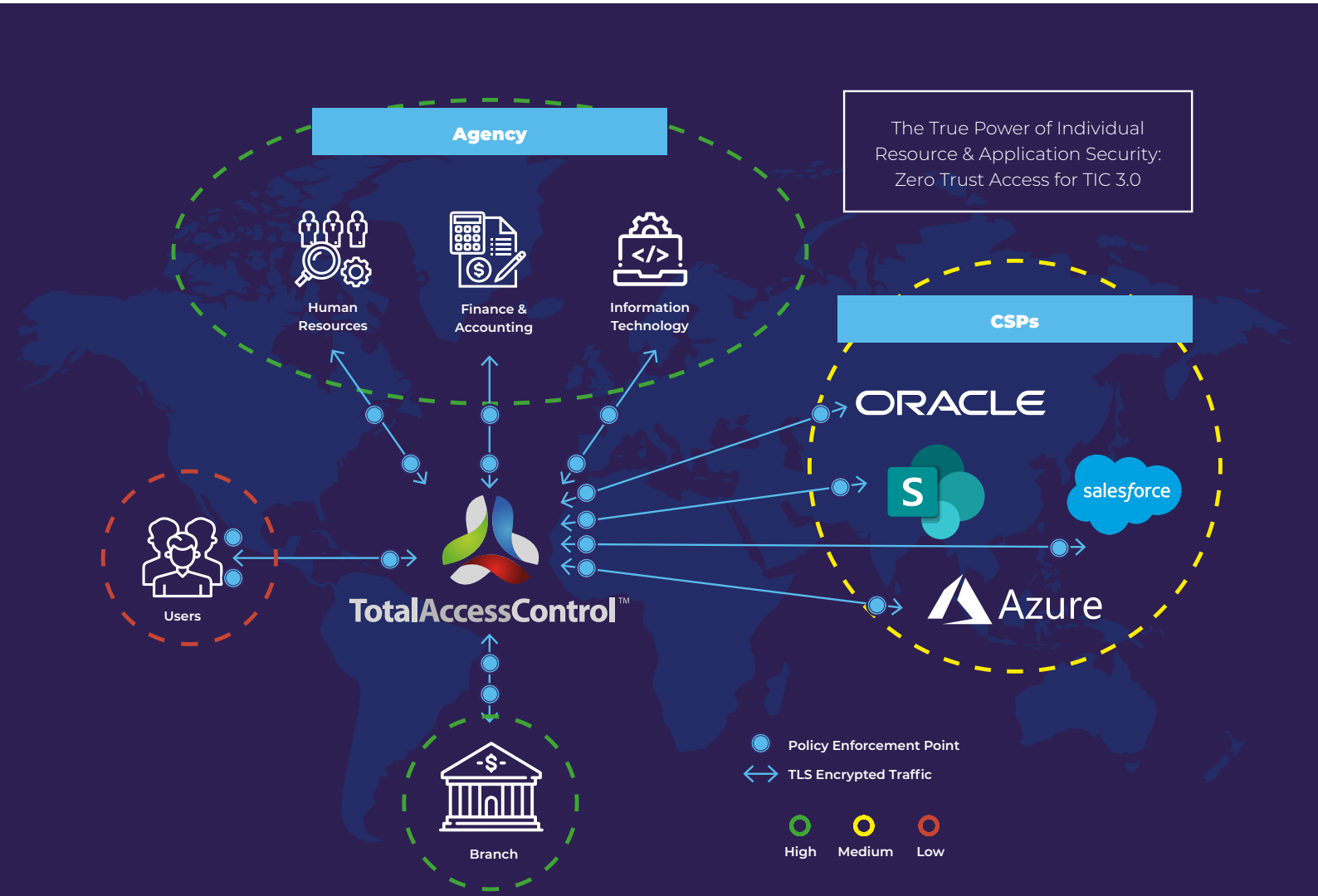
Encryption

Encryption is important to maintain the integrity of all communications across any public (or even private) network. Being able to support the latest and best levels of encryption is crucial to security and preventing many types of attack.

Total Access Control encrypts traffic automatically, between the end users and the resources they are connecting to in order to ensure privacy and security of the information in transit. This is true even if the native application or resource does not inherently have encryption itself – all communication to and from that application and the end user will be encrypted.

All this is done seamlessly before the user even touches the network – without any lulls in performance. The same encryption takes place when traffic is sent back from the application or resource to the end user.

TAC keeps prying eyes away from your valuable information regardless of whether that bad actor is scanning the internet or is already inside your corporate network. Privacy and security are maintained for all traffic. TAC also optimizes your budget outlay for encryption, since it is designed from the ground up to guarantee optimum performance with its complete portfolio of security features running.



Final Notes: End-User Security Awareness & E-Commerce Security Programs

While Total Access Control does not directly address end-user security awareness programs or e-Commerce security, it is important to note what TAC does provide to your enterprise organization ***when*** those programs fail.

And history shows that ***they will fail*** at some point, despite your best efforts.

As outlined in the **Authentication** section of this guide, TAC helps mitigate the impact of those vulnerabilities caused by lost or stolen credentials through phishing, brute force, and business email compromise (BEC) attacks that even the most rigorous security awareness programs won't prevent.

Also, TAC is not designed to directly secure the transactional nature of eCommerce solutions. However, it does have a direct impact on securing and managing access to those solutions, as outlined in the **Application Security** section of this guide.

TAC's comprehensive approach substantially improves the protection of your entire infrastructure, which may include the eCommerce platforms themselves.

Transform Your Security, Transform Your Business with Total Access Control

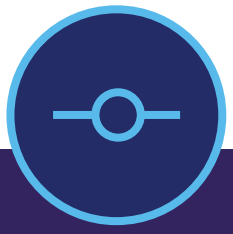
When it comes to delivering on Zero Trust, PortSys is a leader and visionary with Total Access Control.

TAC is a proven, widely used Zero Trust Access solution that allows you to define robust security policies for each resource and provides a centralized view over all access, whether local, cloud or web-based, across your hybrid infrastructure.

With TAC you can control all methods of access in one place, with stronger security policies and evaluation of user credentials, as well as their context of access.

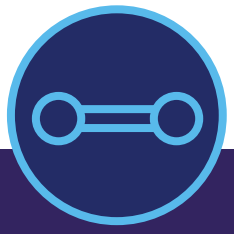
TAC is simple to use, manage and scale, with a wide range of physical, virtual and cloud deployment models.

Visit https://portsys.com/ to learn more about how you can transform your security and transform your business with Total Access Control from PortSys.



SIMPLIFY

- Easier Access for End Users
- Eliminate Need for Multiple Security Products
- Lower Operational & Technology Costs
- Scale User Access Quickly
- Physical, Virtual & Cloud Models Make Deployment Quick & Easy



STRENGTHEN

- Vigorous Authentication
- Context of Access Used to Grant or Deny Access
- Define Security Policies for Each User Group – Internal & External
- Close Exposed Routes for Hackers
- Provide Access Only to Resources, not Networks

UNIFY

- Centralized Access to All Resources, Local & Cloud
- Single Sign-On Across Extended Enterprise
- Consistent Policy Enforcement Ensures Compliance
- Integrated Audit & Reporting of All Access in One Central Location

Watch this short video to see how you can transform your security and transform your business by taking a new TAC with Zero Trust Access:

https://portsys.com/time-to-take-a-new-tac/

www.portsys.com | info@portsys.com
+1 781 996 4900 | +44 208 196 2420

PORTSYS®