Zero Trust Access Control in a Perimeterless World

Transform Your Security, Transform Your Business

In today's perimeterless world, IT security is a critical imperative for your organization's success. That's why it is consistently ranked as one of the top three priorities in C-suite and boardroom surveys.
Total Access Control™ (TAC™) is a Zero Trust approach designed for the needs of today’s hybrid enterprise, providing your organization with a competitive edge in today’s challenging business world.

We built TAC to address the significant challenges of securing your infrastructure against increasingly sophisticated attacks, enabling your teams to focus its time and efforts on driving the digital transformation that provides a competitive edge, instead of dedicating valuable time and resources to fighting attacks.

PROTECT & CONTROL ACCESS TO ALL YOUR RESOURCES, NOT JUST THE EASY ONES

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

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

Easy to Deploy, Scale Quickly
- Achieve Zero Trust in days or weeks, not months or years, in your existing infrastructure – with no changes required
- Functions in local datacenter, cloud or both
- Implementation scales based on your needs

Isolate Resources, Remove Threats
- Seamlessly evaluates many factors of authentication for every access request
- Creates segmentation by granting users access to specific resources, not entire network
- Prevents or limits access from untrusted states, based on your own policies

Reduce Complexity, Lower Costs
- Consolidates many security products into one solution at much lower cost
- Provides centralized management of all access, local and cloud
- Creates more comprehensive, integrated and fortified architecture

Unify Security, Strengthen Control
- Closes vulnerable ports and reduces exposure while improving security and performance
- Evaluates users’ full context of access – device, OS, location, patching, certificates
- Provides virtually unlimited combination of granular controls for any application
Transform Your Business

TAC’s Impact on Your Business

- Achieves Zero Trust goals without costly rip and replace of your existing IT infrastructure
- Makes your end users’ lives easier, improving productivity across your hybrid enterprise
- Accelerates modernization efforts to grow your business through digital transformation

Simplify Access, Improve Productivity

- Single-Sign On (SSO) from any device, anywhere makes users more productive
- Delivers a more personalized user experience for all resources, local and cloud
- Reduces time admins need to devote to reset credentials, resolve lockouts

Eliminate Risk, Accelerate Innovation

- Thwarts phishing, ransomware, brute force, BEC, and data exfiltration attacks
- Ensures business continuity and redundancy with high-performance connectivity
- Fast-tracks ability to securely adapt to forces driving innovations in your market

Drive Digital Transformation, Grow Your Business

- Enables mobility for remote access anywhere, including work from home and partners
- Provides dependable, predictable performance at scale to meet growing business needs
- Empowers end users to focus on transforming your business to increase market share

www.portsys.com
TECHNICAL SPECIFICATIONS

DEPLOYMENT

- Designed to Work in Any Environment: Stand-Alone, Distributed or Hybrid
  - Single Server
  - Azure
  - Amazon Web Services
  - Hyper-V
  - VMware
  - Physical Appliance (HP)
  - Citrix XenServer
  - Dell Nutanix Conversions
- Integrated Load Balancing
- Global Configuration Synchronization
  - Hyper-resilient Session Persistence
  - Scalability Optimization
  - Business Continuity
  - Disaster Recovery
  - Failover Scenarios
- SDK Programming Support
  - Android
  - iOS
- Mobile Apps Supported
  - Android
  - iOS
- Cloud Provisioning Supported
  Out of Box (OOB)
  - Developer Portal
  - ITSM Integration
  - Threat Intelligence Integration
  - Endpoint Detection & Response Integration
  - AI/ML Integration
  - HTTPS Offloading
  - Extensive Knowledge Base
  - 24/7/365 Support

SECURITY

- TLS 1.2
  - Backward Compatibility Support – TLS 1.0 & TLS 1.1
- SSL 3.0
- FIPS 140-2 Compliant
- TIC 3.0 Compliant
- NIST SP 800-171 Compliant
- Integrated Firewall
- Customer Data Encrypted in Transit
- Resources & Applications – Including Legacy Infrastructure
  - Context-Aware Microsegmentation
  - Latent Risk Protection
- Authorization for All Access, Local or Cloud
- Endpoint Inspection
- Operating System
  - Registry Key Entries
  - Patch Level
  - Certificates
  - Hardware Binding
  - Domain-Joined Status
  - Current Anti-Virus
  - Hidden Files
  - Anti-Spyware
  - Network Location
  - Specific Installed Software
  - Device Specifications
- Insider Threat Protection
- Unauthorized Account Takeover Detection – Manual & Bot
- Risk-Based Authentication & Authorization
- Social Engineering Protection
  - Brute Force Attacks
  - Phishing
  - Pretexting
  - Baiting
  - Quid Pro Quo
  - Tailgating
- Fraud Detection and Prevention
  - Multi-Factor Authentication
  - GeoIP
  - Device Detection
  - Device-to-Account Binding
  - SYSLOG for External Solutions
  - SQL Connection for External Solutions
  - Account Creation
- Unauthorized Access/Tampering Protection
  - RBAC for Administrators
  - ABAC for Administrators
  - PAAC for Administrators
- SSH Network Services Protection for IoT
- GUI Policy Editor
- Audit & Access Logs
- SYSLOG Integration
- GeoIP Intelligent Access Policies
- Delegated Policy Management Support
- Static/Dynamic Authorization Support
- All-Inclusive Administrator Policy Management
- Flexible Entitlement Model Support
  - Roles
  - Group
  - Business Activities
  - Organizations
  - Projects
  - Time-Restricted
  - Tasks
  - Profile
- API Protocol Support
  - SOAP
  - LDAP
  - RADIUS
  - TCP Socket
- Custom Access Methods
  - API
  - External IdP
- Best Practice HTTP Security
  - Headers
  - Framing
  - Scripting
  - Cross-Site Scripting XSS
  - Denial of Service Protection
  - Response Caching
  - Content Filtering
  - Routing
- Supported Access Control Principles
  - Attribute-Based (ABAC)
  - Role-Based (RBAC)
  - Context-Based (CBAC)
  - Policy-Based (PBAC)
  - User Groups
- SSH Network Services Protection for IoT
- GUI Policy Editor
- Audit & Access Logs
IDENTITY

- Integrated TAC User Database
- SSO Engine (Forms-Based, HTTP 401, Client SSL Certifications)
  - Across Multiple Web Applications
  - For Non-Web Applications/IT Systems
  - Single Sign-Off Support
- Supports Contextual-Adaptive Authentication
  - Device Profiling
  - Device Tagging
  - Device Health State
  - Phone Printing
  - Network Profiling
  - Network Connection Type
  - User Profiling
  - User Activity
  - Location Awareness
  - Other Geo-Informative Attributes
- Authentication Methods Supported
  - Username/Password
  - Email OTP or Link
  - Phone OTP
  - SMS OTP
  - Client-Side Certificates
  - RADIUS
  - Mobile Push Notifications
  - Vendor-Provided Mobile App
  - DuoSecurity Mobile App
  - Google Authenticator
  - Microsoft Authenticator
  - Okta Mobile App
  - SafeNet MobilePASS
  - iOS Face ID
  - iOS Touch ID
  - FIDO 2.0/WebAuthn API
- MultiFactor Authentication Supported
- Windows NTLM
- RSA SecurID
- Safenet
- Swivel Secure
- Vasco
- Smartcards
- Cisco Duo
- FIDO2
- Biometrics
- QR Codes
- Google Token
- Symantec VIP
- Yubikey

Included
- SMS Tokens
- Device Validation
- Push Notifications
- One-Time Passwords (OTP)
- SAML Tokens
- API Integrations
- Conditional MFA
- SafeLogin
- Supports All Authentication Solutions Including:
  - Active Directory Federation Services (ADFS) Connector
  - OAuth1
  - OAuth2
  - SAML 2.0
  - SAML 1.1
  - RADIUS
  - Okta Federated Identity
  - PingFederate
- Supports Global Time-Out
- Directory Services Fully Integrates & Also Supports:
  - Microsoft Active Directory
  - Microsoft Azure AD
  - LDAP Directory Services
  - RADIUS
  - NTLM
  - Kerberos Constrained Delegation (KCD)
  - Customer-Built Directory Services
  - TAC's Proprietary Secure Database
- Privileged Access Management
- Client Certificates

USER EXPERIENCE

- Platform Agnostic – For Any Application, On Any Device
- Simplified & Centralized End User Experience
  - Windows Client
  - Browser
  - Mobile
- Single Sign-On for All Resources, Local & Cloud
- Browser-Agnostic
- Responsive-Design User Portal
- 17 Portal Themes Included
- Fully Customizable Portal Experience Using CSS (Colors, Logos, etc.)
- Branding Customization
- Self-Service Password Management/Reset/Account Recovery/Unlock
  - Security Questions/Knowledge-based Authentication
  - Email OTP/Link
  - Phone OTP
  - SMS OTP
  - Mobile Push Notices
  - Account Linking
- User-Defined Favorites & Search
- Section 508-compliant
• Full Microsoft 365 Integration including:
  - Teams
  - Exchange
  - SharePoint
  - Office
• SaaS Integration including:
  - Salesforce
  - Oracle
  - SAP
  - Adobe
  - Zoom
  - Skype
  - Slack

**TAC ENGINE**

- Reverse Proxy – Web Application Delivery for any HTTP/HTTPS Application
- Full Exchange Publishing
  - ActiveSync
  - OWA
  - Outlook
- Remote Access
  - VPN
  - Web-Based File Access
  - Citrix Storefront
  - RDP
    - Secure Native Client
    - Secure Clientless HTML5
    - Context-Aware RDP Profiles
- Virtual Desktop Integration (VDI)
  - Citrix XenApp
  - Citrix Xen Desktop
  - VMware Horizon View
  - Microsoft Azure
  - AWS Desktop as a Service (DaaS)
- Cloud Application Access Control
- SSH & IoT Access Controls with Clientless HTML5
- TCP/IP Port Listeners – Enables Non-Native Client Application Connections
- Full HTTP Control, Inspection & Modification
- Client/Server Tunnel TLS – Socket Forwarding for Publishing Thick Client Applications

**MANAGEMENT**

- Centralized Reporting Engine
- Out of the Box (OOB) Reports
  - IGA
    - Accounts
    - Delegate Access
    - Group
    - Privileged Access
    - Roles
    - User Access
  - Operations
    - Performance
    - Volume
    - Security
    - Policy/Compliance Violations
- Report Formats Supported
  - HTML
  - XML
  - CSV
  - PDF
  - Dashboard
- Single Pane of Glass View to Manage All Array Members
- Analytics & Intelligence (AI/ML) Reports
  - User Behavior
  - User Device Usage
- Delegated Administration
- Centralized Management of Each Instance
  - Availability
  - Usage
  - Automatic Logging of All Events/Incidents
- Export/Import of Configuration
- GUI Management
- Wizard-Driven Application Publishing
- Session Management Support
  - HTTP Headers
  - Browser Cookies
  - Maximum Session Time-Out
  - Idle Session Time-Out
  - Max/Idle Session Timeout Value Configuration
  - Brute Force Detection
  - Session ID Anomaly Detection
  - Session ID Guessing
  - Session ID Binding to User Properties
  - Session ID Lifecycle Monitoring
- Tracing Capabilities Across Logs to Identify Errors
- Automated Administrator Alerts
- Updates & Configuration
  - Changes Applied in Real-Time
  - Does Not Impact Any Services/Sessions
- Direct Migration from Other Application Gateway Products
Experience for yourself how Total Access Control’s Zero Trust approach secures access to all your resources, both local and cloud, in a single, comprehensive access control solution that will transform your security, and transform your business. You can zip from 0 to Zero Trust in 30 days or less with Total Access Control. To sign up for a no-risk trial of TAC, contact us at:

info@portsys.com  +1 781-996-4900  +44 0208 196 2420

ADDITIONAL RESOURCES

- Video: Time to Take a New TAC
- Case Studies
- Analyst Reports
- Industry Solution Briefs
- eBook – Cybersecurity Risk: A Board’s-Eye View
- White Paper – What to Look for in a Zero Trust Solution
- Zero Trust Access Implementation Guide
- Executive Order on Improving the Nation’s Cybersecurity
- National Security Agency (NSA) Guidelines on Zero Trust
- National Institute of Standards and Technology (NIST) SP 800-207
- Cybersecurity & Infrastructure Security Agency’s (CISA) Guidelines on Trusted Internet Connections (TIC) 3.0
- Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework