BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

OTaccess™

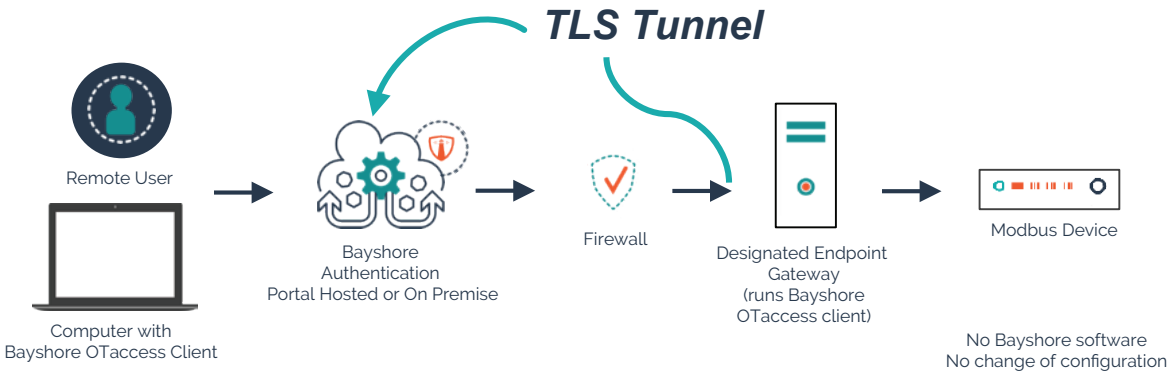
INDUSTRIAL SECURE REMOTE ACCESS

Datasheet

Overview

OTaccess™ is the only real-time secure remote access solution designed specifically for OT networks and assets. It offers granular access control, with far more precision than conventional VPNs, enabling customized control per protocol, per user activity, and per seat, with continuous monitoring and enforcement for the duration of every session. It enforces a logical "line of sight" protection model, where operators have assurance that people can only touch what they can see across their connection, and absolutely nothing else. It's available as an on-premise solution, or via a hosted cloud model, and is often used as a central control around third party vendor risk management.

	OTaccess	Software Defined Networking Tools	VPNs
Native OT Protocol Support	Yes, including deep packet inspection	Port-level only	N/A
Session origination	Outbound only via TLS from customer to policy engine	In-bound our outbound, depending on product/vendor	Inbound through to perimeter firewalls
Session Types	Highly granular single-user to single-service permissions	User – network permission defaults	Network to network permission defaults
Local-use or AD users/groups	Yes	Yes	Yes



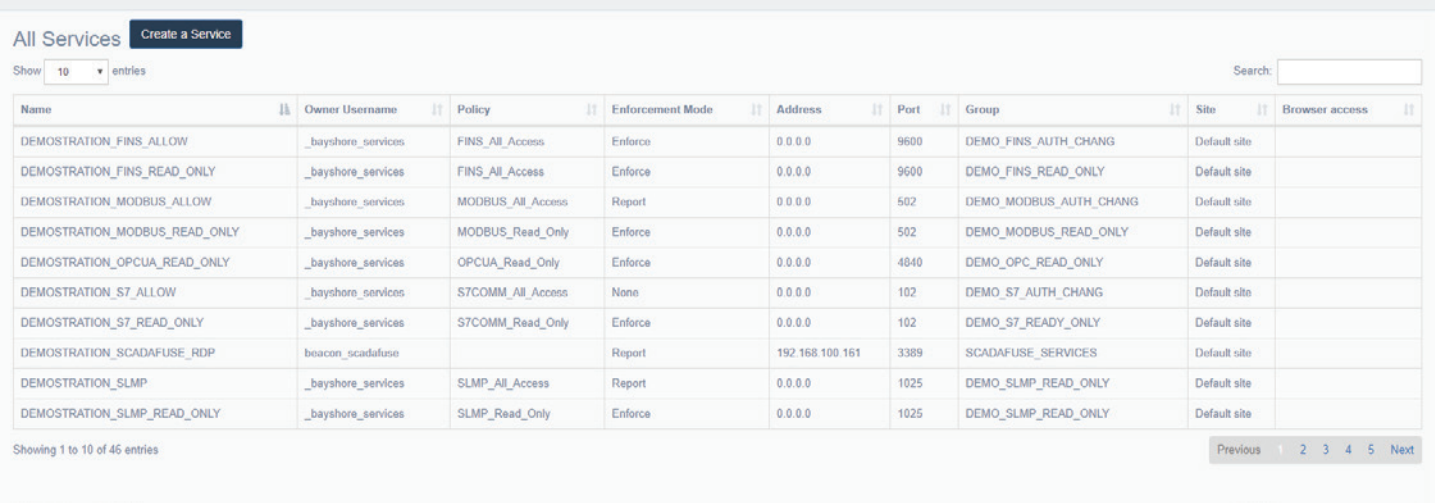
- *Most industrial VPNs do not provide enough granularity*
  - Other VPNs create a secure tunnel to the OT network, but do not have the ability to limit remote use actions after login
  - Other VPNs cannot apply further security restrictions once access is granted
- *OTaccess secure remote access was designed by automation engineers to provide:*
  - Guided creation of highly granular access policies — i.e. Endpoint + user + time + duration
  - Easy deployment and configuration compared to standard VPN
  - Easy integration into tightly controlled OT environments
  - Enforceable 3rd party vendor risk management
- *Hosted version uses customer-dedicated AWS cloud instance for authentication and policy enforcement*
- *Onsite version uses standard 1U industrial server with separate management and administration interfaces*

Native Policy Controls

	FINS	Modbus	OPCUA	S7	SLMP	RDP	Ethernet/ IP	VNC	HTTP/S	sftp	ssh	telnet
Read-only	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Read-write	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
No SQL Injection	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
No XSS	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Single endpoint	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗

OTaccess permits highly granular and configurable protocol and policy support by individual published service through our patented Pallaton™ policy engine.

Available services and policies


All Services Create a Service

Show 10 entries Search:

Name	Owner Username	Policy	Enforcement Mode	Address	Port	Group	Site	Browser access
DEMOSTRATION_FINS_ALLOW	_bayshore_services	FINS_All_Access	Enforce	0.0.0.0	9600	DEMO_FINS_AUTH_CHANG	Default site	
DEMOSTRATION_FINS_READ_ONLY	_bayshore_services	FINS_All_Access	Enforce	0.0.0.0	9600	DEMO_FINS_READ_ONLY	Default site	
DEMOSTRATION_MODBUS_ALLOW	_bayshore_services	MODBUS_All_Access	Report	0.0.0.0	502	DEMO_MODBUS_AUTH_CHANG	Default site	
DEMOSTRATION_MODBUS_READ_ONLY	_bayshore_services	MODBUS_Read_Only	Enforce	0.0.0.0	502	DEMO_MODBUS_READ_ONLY	Default site	
DEMOSTRATION_OPCUA_READ_ONLY	_bayshore_services	OPCUA_Read_Only	Enforce	0.0.0.0	4840	DEMO_OPC_READ_ONLY	Default site	
DEMOSTRATION_S7_ALLOW	_bayshore_services	S7COMM_All_Access	None	0.0.0.0	102	DEMO_S7_AUTH_CHANG	Default site	
DEMOSTRATION_S7_READ_ONLY	_bayshore_services	S7COMM_Read_Only	Enforce	0.0.0.0	102	DEMO_S7_READY_ONLY	Default site	
DEMOSTRATION_SCADAFUSE_RDP	beacon_scadafuse		Report	192.168.100.161	3389	SCADAFUSE_SERVICES	Default site	
DEMOSTRATION_SLMP	_bayshore_services	SLMP_All_Access	Report	0.0.0.0	1025	DEMO_SLMP_READ_ONLY	Default site	
DEMOSTRATION_SLMP_READ_ONLY	_bayshore_services	SLMP_Read_Only	Enforce	0.0.0.0	1025	DEMO_SLMP_READ_ONLY	Default site	

Showing 1 to 10 of 46 entries Previous 1 2 3 4 5 Next

OTaccess™
INDUSTRIAL SECURE REMOTE ACCESS

BAYSHORE NETWORKS