Executive Overview for Critical Infrastructure Leaders

Executive Overview for Critical Infrastructure Leaders

Challenge 1: Static Access. Reactive Investigation. Unnecessary Risk.

Problem Statement

Critical infrastructure environments rely on static access controls that grant permissions once and trust them indefinitely. In a world of remote vendors, legacy OT systems, and escalating insider and supply-chain threats, these static controls create implicit trust and unnecessary risk. Security teams are forced to react after suspicious behavior occurs, and regulators increasingly expect continuous oversight that existing access tools cannot deliver.

Hyperport Breakthrough

Hyperport v3.3 introduces **Autonomous Secure Access**, which combines two capabilities: an AI-driven Trust Engine that autonomously scores user and session risk throughout every connection, and a policy-based access control engine that enforces the organization's pre-defined security rules based on those scores. Unlike traditional tools that make a single access decision at login, Hyperport's Trust Engine assigns an **Adaptive Trust Score** (ATS) to every user and session, updated in real time based on more than two dozen trust signals spanning identity, in-session behavior, device posture, and network context. The Trust Engine evaluates risk autonomously. The policy engine enforces the access decisions your organization has already defined.

When trust conditions change, the Trust Engine updates the Adaptive Trust Score in real time. The policy engine then enforces the organization's pre-configured responses at machine speed: alerting administrators, triggering step-up authentication, forcing re-authentication, terminating sessions, or locking accounts. Humans define the policies and thresholds, and the system executes them. Four policy types provide layered enforcement across the access lifecycle:

- **Login Policies** enforce conditions at initial authentication
- **App Connection Policies** govern access to specific applications based on trust, device health, and context
- **User Monitoring Policies** continuously enforce security across active user sessions
- **App Monitoring Policies** continuously enforce security across active application sessions

App Security Levels (L1–L5) classify applications by criticality, ensuring high-value systems require higher trust thresholds. Trusted Endpoints validate device identity via client certificates, and EDR integrations incorporates real-time device health into access decisions. Crucially, this intelligence **runs entirely on-**

premises, enabling security-sensitive and regulated operators to deploy advanced behavioral analytics without cloud dependencies or external data transmission.

Autonomous Secure Access elevates Hyperport from secure access to intelligent access governance. The Trust Engine continuously evaluates risk. The policy engine continuously enforces the organization's rules. Together, they adjust security posture in real time, reduce operational risk, and eliminate the attack windows created by static permissions, all while keeping humans in control of every access decision through the policies they define.

Challenge 2: Operational Technology Specific Access Challenges

Problem Statement

Critical infrastructure companies are not standardized, uniform environments. They combine a diversity of mixed OEM equipment, legacy operating systems, proprietary HMIs, and network architectures across plants and regions. Traditional access tools were designed for homogeneous IT networks without this kind of diversity. They require agents which introduce compatibility issues, or force infrastructure changes that jeopardize reliability. As a result, organizations cannot establish a consistent, secure access model across their OT footprint without increasing operational or cybersecurity risk.

Hyperport Outcome

Hyperport delivers a standardized user access platform that works across any OT environment, regardless of OEM, device age, protocol, or operating system without requiring clients/agents or modifying production assets. It provides uniform, policy-driven access to HMIs, engineering workstations, PLCs/RTUs, and other OT systems through a non-disruptive, browser-based experience that ensures operational continuity. Protocol isolation renders RDP, SSH, and VNC sessions as encrypted streaming video over HTTPS, eliminating direct protocol exposure. By normalizing how users connect to diverse infrastructure, Hyperport brings modern security controls to OT environments without the downtime, integration risk, or architectural changes required by legacy tools.

Challenge 3: User Access Tool Sprawl & Fragmentation

Problem Statement

Enterprises have accumulated multiple access technologies over time including VPNs, jump hosts, VDI solutions, privileged access tools, and vendor-specific access platforms. This creates excessive costs through overlapping vendor contracts, operational complexity that expands attack surfaces, poor user experience requiring multiple tools for different systems, and no unified visibility or monitoring of who accesses what systems, when, and whether that access is actually needed or cost justified.

Hyperport Outcome

Hyperport consolidates fragmented access tools into a single platform that provides unified visibility and control across internal and third-party access without disrupting critical operations. Organizations gain centralized oversight and governance with analytics for usage patterns, cost optimization, and access right-sizing. The HyperView analytics workspace provides detailed behavioral analysis with activity timelines, while the Unusual Activity Report surfaces behaviors that deviate from established patterns. The platform unifies visual display protocols (RDP/SSH/VNC), isolated browser access, IPSec-based ZTNA, secure file transfer with approval and AV scanning, session monitoring, and a TPM-backed secrets vault, reducing vendor overlap and cost, lowering operational and security complexity, and improving the user experience through a single, comprehensive access platform.

Challenge 4: Enterprise Governance Across Distributed Operations

Problem Statement

Large enterprises often operate as federations of semi-autonomous business units with fragmented access tools across IT and OT environments. This creates local agility but makes it difficult to enforce consistent cybersecurity policies globally while limiting enterprise visibility and delaying incident response.

Hyperport Outcome

Hyperport's multi-tenant architecture allows each business unit to manage its own access environment while providing enterprise-wide oversight through centralized visibility and unified control. The expanded policy framework enables consistent enforcement of security standards across all environments while accommodating local operational requirements. Real-time Trust Engine analytics provide immediate situational awareness across the enterprise, and integrated policy-based enforcement ensures consistent security posture across every site and region. The platform's distributed, fault-tolerant architecture delivers enterprise-scale resiliency and uniform governance without sacrificing local autonomy.

Challenge 5: Compliance in Critical Infrastructure

Problem Statement

Expanding regulatory frameworks such as NIS2, NERC CIP-005-7/003-09, TSA Security Directives, and CMMC require consistent access controls, continuous monitoring, and evidence collection across energy, manufacturing, pharmaceuticals, rail, and other sectors.

Hyperport Outcome

Hyperport simplifies compliance with centralized auditability featuring granular session logs, keystroke and video capture, and exportable evidence. The Trust Engine's continuous monitoring capabilities directly address regulatory expectations for ongoing security assessment rather than point-in-time compliance. Blocked Session Reports provide audit trails of denied access with administrator review workflows. Automated video rendering and export to external storage enables long-term evidence retention. These capabilities reduce audit preparation time and minimize findings across diverse regulatory environments, providing the documentation and controls that critical infrastructure organizations need to meet current and future mandates.

Summary

Critical infrastructure companies operate in environments defined by non-standardized OT systems and networks, expanding third-party access needs, and escalating cybersecurity and regulatory pressures. Traditional access technologies cannot provide consistent, secure, non-disruptive access across this complexity. Hyperport delivers a unified platform purpose-built for these realities.

Hyperport:

- Introduces Autonomous Secure Access with an AI-powered Trust Engine that autonomously scores risk in real time, combined with policy-based access controls that enforce the organization's security rules at machine speed.
- Provides unified visibility and centralized governance while preserving local plant autonomy.
- Consolidates fragmented legacy access tools and reduces operational complexity and attack surface.
- Prevents advanced threats through protocol isolation, end-to-end session protection, and integrated file governance.
- Supports OT reliability by securing legacy HMIs, engineering workstations, and field-level devices without disruption.
- Streamlines compliance with continuous monitoring, centralized evidence, immutable audit logs, and regulatory-aligned access controls.

About Hyperport

Hyperport delivers autonomous secure access for critical infrastructure by unifying zero trust, secure remote access, and privileged access with AI-driven trust and policy enforcement across IT, OT, and hybrid environments. Learn more at http://hyperport.io.