Zero Trust Mobility with ISEC7 SEVENCEES

Next Generation Security, Today

Mary Quinn

ISEC7
GOVERNMENT SERVICES

Zero Trust Mobility with ISEC7 SEVENCEES

Next Generation Security, Today

Executive Summary

In today's dynamic cybersecurity landscape, Chief Information Security Officers are tasked with the formidable challenge of safeguarding their organizations against increasingly sophisticated threats while balancing a finite budget and operational demands. The dual pressures of maintaining robust security measures and optimizing limited resources require a strategic approach that balances immediate needs with long-term resilience. While striking this delicate balance of budget and operational needs proves to be a major challenge for CISOs, ISEC7's new platform **ISEC7 SEVENCEES** can ease this burden. Built on Zero Trust Architecture and designed around end-to-end security and traffic obfuscation to the mobile endpoints, **ISEC7 SEVENCEES** leverages existing infrastructure to create a bespoke solution that addresses the business needs of organizations whilst securing traffic across trusted and potentially compromised networks. **ISEC7 SEVENCEES** not only simplifies the complex task of balancing security and operational demands but also ensures cost-effectiveness by leveraging existing infrastructure, allowing CISOs to meet budget constraints while enhancing overall security posture.

Introduction

A Chief Information Security Officer's role requires a careful balance of security posture against the ever-evolving threat landscape, budget constraints, resource limitations, technological advancement, data privacy, third party risks, employee awareness, and regulatory compliance. CISOs must contend with the high costs associated with advanced security technologies, the need for continuous monitoring and adaptive defenses, and the imperative to comply with evolving regulatory requirements and Zero Trust Architecture mandates. Additionally, there has been a shift towards remote work in recent years, with 92% of organizations touting employees who work from home at least some of the time[1]. This shift towards remote work has created new attack vectors, necessitating more comprehensive and flexible security solutions at a cost.

Stretching Your Budget

In a 2023 study, CISOs reported their top three areas of responsibility as leadership (35 percent), risk assessment and management (44 percent), and data privacy and governance (33 percent)[2]. CISOs also face the challenging task of managing a limited budget and resources while needing to adapt to the constantly evolving threat landscape, which often requires significant investment. To maximize their resources, many CISOs ensure that existing technologies are utilized throughout their full depreciation or amortization lifecycle. This approach allows them to stretch their budget further and allocate funds towards implementing new security frameworks, such as Zero Trust Architecture (ZTA), which are essential for modern cybersecurity but may not yet be in place. Oftentimes CISOs are in a position where they must strategically leverage current investments to balance immediate security needs with long-term resilience and compliance requirements.

---

[1] Verizon, *2024 Mobile Security Index* (2024), 5.

[2] CISO Global, *CISO Workforce and Headcount 2023 Report* (2023), 7.

Operational Hurdles

The other challenges CISOs face in their roles are also driven by the ever-evolving landscape of cybersecurity threats and technological advancements. One of the primary challenges is the sophistication and diversity of cyber threats, including AI-driven attacks[3], ransomware, and zero-day exploits, which require continuous monitoring and adaptive defense mechanisms. Additionally, the widespread adoption of remote work has expanded the attack surface, necessitating stringent security protocols to protect sensitive data accessed outside secure office environments. CISOs also grapple with regulatory compliance and mandates, such as the adoption of Zero Trust Architecture, and they must navigate these complex frameworks to avoid severe penalties.

The Solution

The **ISEC7 SEVENCEES** platform, built on Zero Trust Architecture, offers a technology agnostic path to incorporate your existing infrastructure to achieve quantum safe security and built in redundancy to ensure minimal exposures in your mobility ecosystem. **ISEC7 SEVENCEES** incorporates an all-encompassing management and monitoring platform offering health and status of all the underlying solutions along with cryptological and IP connection inventory. **ISEC7 SEVENCEES** incorporates preexisting network elements, eliminating capital write-offs when deploying the framework, and extends a full suite of services to the retransmission access point, allowing for secure local area access for approved connected devices. This eases the administrative burden, enables device flexibility, and enables the use of classified devices with an enhanced level of security beyond what's required from the National Security Agency (NSA).

The SEVENCEES Framework is based on several key capabilities adaptable to meet customer needs including UEM flexibility, device agnosticism, redundancy for Dual DAR/DIT, Secure Voice, and crisis communication notification building off NSA's CSfC Mobile Access Capability Package. As with CSfC deployments, end user devices connect through the internet through an Outer Tunnel to an intermediate network before connecting through an inner tunnel to an internal or air-gapped network. The solution automatically applies user/endpoint-specific network policy and leverages quantum resistant session keys to deliver secure, encrypted data transport and network micro-segmentation. It authorizes only those users allowed by network policy to access other endpoints and resources on the network. The defense in depth architecture leverages a quantum resistant outer VPN and inner business and operation specific tunnel (TLS, IPSEC or another quantum resistant option). This configuration enables cryptographic flexibility and security as the control is completely separated from the data in time and space. Cryptographic keys are delivered independently of the data ensuring that an attacker cannot access both if one is compromised.

Finally, **ISEC7 SEVENCEES** facilitates clear communication of cybersecurity risks and investments to non-technical stakeholders by demonstrating how the platform's capabilities directly support business objectives and regulatory compliance. This holistic approach ensures that CISOs can effectively safeguard organizational assets and maintain resilience against evolving cyber threats. **ISEC7 SEVENCEES** provides a flexible framework that delivers a great end-user experience and comprehensive, monitored, and managed end-to-end security to the endpoints, regardless of business needs. It also has the ability to integrate other elements as the business and security demands of the ecosystem evolve.

ISEC7 SEVENCEES Objectives:

[3] Verizon, *2024 Mobile Security Index* (2024), 25.

- Flexible framework to secure all endpoints
- Provides end to end security to all endpoints
- Leverages existing infrastructure to minimize cost of upgrade
- Quantum safe out of band key exchange
- Visibility Across entire ecosystem
- Alignment with NSA CSfC, CISA and DISA recommendations for the most robust security protocols

ISEC7 SEVENCEES Benefits:

- **Enhanced Security**: **ISEC7 SEVENCEES** is designed to significantly reduce the risk of data breaches and unauthorized access.
- **Operational Efficiency**: **ISEC7 SEVENCEES** streamlines command and control operations, ensuring that all communications are reliable and secure.
- **Compliance**: **ISEC7 SEVENCEES** helps users comply with stringent security regulations and standards, ensuring that all data handling practices meet or exceed required guidelines.
- **Resilience**: **ISEC7 SEVENCEES**' robust security measures enhance resilience against cyber threats, ensuring continuous and secure operations even in the face of sophisticated attacks.

In an era where cybersecurity threats are constantly evolving, CISOs need a solution that not only addresses these challenges but also integrates seamlessly with existing infrastructure to optimize costs and operational efficiency. Underlining this is the fact that 83% of global organizations are planning to implement a converged security solution extending comprehensive security measures across services, networks and platforms[4]. The **ISEC7 SEVENCEES** platform provides a comprehensive, technology-agnostic solution built on Zero Trust Architecture, ensuring quantum-safe security and robust protection for all endpoints. By leveraging existing network elements and offering a flexible, scalable solution, **ISEC7 SEVENCEES** empowers organizations to enhance their security posture without incurring significant capital expenditures.

Our platform's holistic approach simplifies the complex task of managing cybersecurity risks, enabling CISOs to focus on strategic initiatives while maintaining compliance with stringent regulatory standards. With **ISEC7 SEVENCEES**, you can achieve a resilient and secure infrastructure that supports your business objectives and adapts to future security demands.

Take the next step towards securing your organization's future. Contact us today to learn more about how **ISEC7 SEVENCEES** can transform your cybersecurity strategy and provide peace of mind in an increasingly uncertain digital landscape and prepare yourself for next generation issues today.

[4] Verizon, *2024 Mobile Security Index* (2024), 41.

What Makes ISEC7 Government Services Different?

Whether you request one of our experts to be on site with you or simply contact our 24/7 support desk staff, ISEC7 Government Services will work with you at the level you need. With our full suite of services, we are more than just a link between an endpoint and the data center. ISEC7 Government Services Architects and Senior Engineers have deployment and operational experience spanning decades for the most secured federal organizations and regulated industry domestically and globally. With our full suite of services, we are more than just a link between an endpoint and the data center.

No matter how mature your digital workplace environment is, we can assess strengths and risks and provide recommendations for optimizations. We enable digital workplace managers, operations teams, and administrators to achieve both short and long-term goals. At each point of engagement, we are committed to excellence.

As an early entrant into the enterprise mobility market ISEC7 Government Services provides a unique mix of products and consulting/professional services focused on enabling and endpoint use in the enterprise. In addition to ISEC7 Government Services solutions, we also partner with leading endpoint security tools on the market to offer a true one-stop-shop for all enterprise mobility needs. Our service offerings include managed services, professional consulting services for vendor selection, implementations, and ongoing 24/7 support for system administrators.

The ISEC7 Government Services team offers an objective view of the ecosystem against the business needs and limitations of the preexisting infrastructure.

About ISEC7 Government Services

ISEC7 Government Services is the professional & managed services branch of ISEC7 INC in Baltimore, Maryland, and part of ISEC7 Group, supporting the United States Federal Government and federal agency partners and a serving as a leading provider of mission critical digital workplace solutions for both unclassified and classified use.

Our professionals specialize in designing and supporting environments focused on enabling secure and productive end user computing. We emphasize usability while also maintaining a strong security posture around key Zero Trust principles and implementing continuous monitoring capabilities to meet NSA requirements for CSfC environments. 100% of the ISEC7 Government Services workforce holds government security clearance.

Whether your organization needs communications for field/remote workers, classified air-gapped mobile communications, or simply wants to enable an anywhere workplace for employees, we provide the services and tools to enable those capabilities.

CONTACT
PHONE: +1 (833) 473-2747
WEB: www.isec7-gs.com
EMAIL: sales@isec7-us.com