Smart Cities - Smarter, Safer, and More Resilient

Smart Cities may be the future of urban living – leveraging data, digital technology, and design to improve the effectiveness and efficiencies of city services, improving the quality of life for residents. However, the convergence of digital and physical infrastructures in this modernized ecosystem creates significant security risks that should be prioritized.

Technology is transforming every aspect of our lives – including smart cities. This interconnected network of digital and physical infrastructure is contributing to the amplification of cyber-threats in smart city ecosystems.

Protecting Beyond the Perimeter

The IT security solutions and tools we counted on to protect our networks were designed for yesterday's communications. No longer are networks confined to an isolated ecosystem. Quite literally, our networks, software, devices, and people have all left the building. **A more effective solution is required.**

"Smart cities are increasingly under attack by a variety of threats. In this increasingly connected technological landscape, every smart city service is as secure as its weakest link."
– Dimitrios Pavlakis, Industry Analyst at ABI Research.

How Can Smart Cities Get Smarter About Cybersecurity?

City and state leaders must adopt a 'network of everything' security mindset. In addition to having contingency and proactive disaster plans in place, cyber-resilience and safety should become a core component of the overall solution including a trusted, secure network solution based on NIST Zero Trust recommended guidelines.

Today, organizations depend on IT security for their entire network ecosystem. However, legacy OT (physical security, building automation, and critical infrastructure) is too complex and diverse to protect with standard IT approaches and tools. For example, 90,000+ operating systems in the market are up to 30+ years old with little to no standards. These "non-IT" assets are difficult to monitor, manage and scan for threats – creating an attack surface and hiding ground for bad actors. This vulnerability spans markets and can impact lives – not just data.

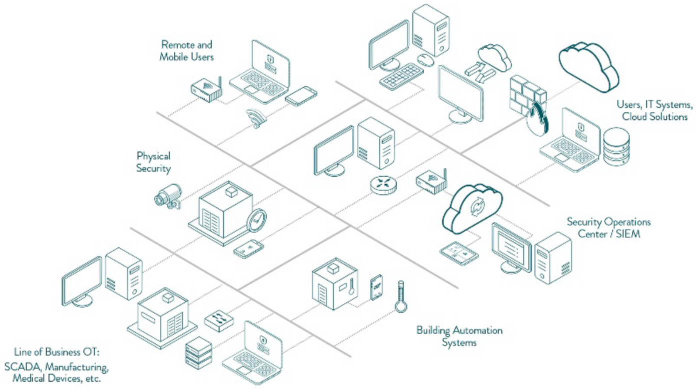
It takes, on average, **280+ days** to detect and contain a network breach.*

Smarter cities need to turn to network security based on Zero Trust Architecture

This requires integrating comprehensive and continuous monitoring capabilities, granular risk-based access controls, and system security automation in a coordinated manner throughout all aspects of the infrastructure to focus on protecting data in real-time within a dynamic threat environment. A private network is recommended for a city government and its different service providers – providing cryptographically secured networks and "zones" where OT and IT can run safely and securely must be created.

*Source: IBM Security: Cost of a Data Breach Report, 2020

A Smarter, Secure Network Based on Zero Trust

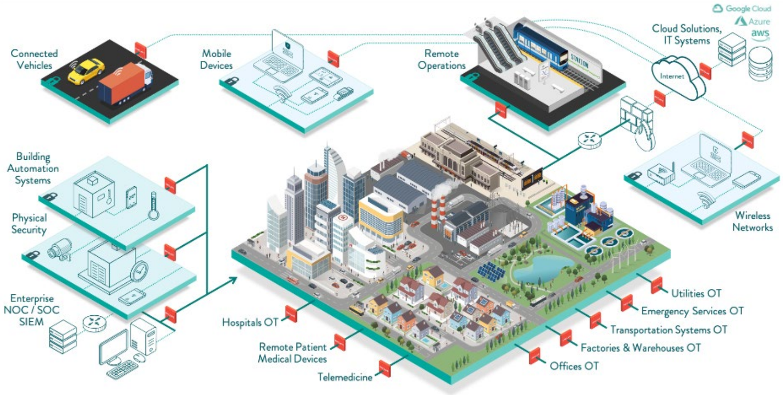


The Onclave TrustedPlatform™ identifies vulnerabilities found in co-mingled IT/OT networks across all industries including Smart Cities. We took proven techniques and technologies used by the U.S. Department of Defense (DoD) and our national security agencies and built a commercially viable solution that is easier to manage, scalable and more cost-effective. Onclave's platform aligns with the techniques, framework and guidelines recommended by NIST (National Institute of Standards in Technology), NSA, DoD and Defense Information Systems Agency (DISA).

> "We have repeatedly seen how important it is to secure not just our devices and networks, but the data as well. As the Internet of Things continues to rapidly expand, cybersecurity solutions like Onclave's Zero Trust platform are essential foundational elements of our new digital infrastructure."
>
> – David Ihrie, Chief Technology Officer, Center for Innovative Technology (CIT)

Cryptographically separated enclaves secure your network by continuously monitoring trusted devices and systems from future risks and potential breaches.

With increasing numbers of remote and mobile users, satellite infrastructures, data and services located outside the protection of traditional network security, Onclave can help you provide the fastest path to a more secure, simplified, and scalable network solution.



See the Onclave Difference for Yourself

Onclave provides a scalable solution purpose-built to protect vulnerable OT and IoT.

Contact us for a live demonstration or hands-on evaluation of our proven solution.

Visit our website. Scan this QR code to download our Zero Trust whitepaper here →

SCAN ME

Onclave Networks, Inc. is a global cybersecurity leader transforming the future of securing all IT/OT devices and systems. Leveraging the same methods and technology used by the Department of Defense (DoD) and U.S. Intelligence Community (IC), Onclave's mission is to provide the *fastest path to a more secure, simplified, and scalable solution* – making it easier and cost-effective for enterprises to manage and continuously monitor.

OnclaveNetworks.com | sales@onclavenetworks.com | 7950 Jones Branch Drive, #805 N, McLean, VA 22102