# Miovision Detection Security

Overview of Miovision
Video Detection System Security
Version 1.4 | June 2023


MIOVISION

# Miovision Security

Security in the software industry is an ever-changing entity, and its importance is only growing as time goes on. As technology improves, so does the need to protect data and prevent inappropriate use and theft of information. Security is a critical part of Miovision One; this paper outlines the elements of Miovision One and how Miovision keeps them secure. For information on our data privacy practices, please refer to our Privacy Policy.

## Security Culture

At Miovision we understand that security starts with us as the bottom line. Everything we do factors it in and we are always looking for ways to improve and grow our security practices. Our work culture means that everyone has a role to play in maintaining security, and we show this through our training and business goals.

## Employee Security Training

At Miovision, all employees undergo security training during orientation and receive ongoing security training throughout their career here. Employees agree to our Code of Conduct and sign a non-disclosure agreement, both of which outline our commitment to safeguarding corporate and customer information. Certain roles may require additional security training depending on their job responsibilities and access to information.

## Dedicated Security Team

Miovision has a team of security professionals dedicated to managing and continually improving our security programs, protections and processes. The team actively:

- Establishes and maintains our security policies, processes, and controls.
- Scans for security risks and monitors for suspicious activity in our corporate and service environments.
- Consults and provides guidance to our product and engineering teams on security best practices.
- Engages external security experts to perform or augment security reviews and assessments.
- Monitors threat intelligence for new security risks.

# Operational Security

Security is a central feature of our company operations and is always in consideration. We limit information access to relevant parties to minimize risk. Miovision is always working to identify and eliminate the possibility of security breaches through innocuous or otherwise unintentional actions.

## Vulnerability Management

Miovision implements a vulnerability management program that actively scans for security threats using commercially available tools, internal and external security reviews, penetration testing, and active monitoring of threat feeds, and security advisories. Vulnerabilities are investigated for applicability, and vulnerabilities that require remediation are prioritized according to severity, assigned an owner, and tracked through the remediation process. To report a suspected security issue, please contact security@miovision.com.

## Malware Prevention

Miovision implements several methods to prevent the introduction, detection, and propagation of malware. We implement strong email filtering rules to reduce the risk of malicious attachments and download links. We also use a commercially available anti-malware solution that detects and prevents the execution of unknown or suspicious applications. Our network architecture limits the ability for deployed systems to communicate with each other, further reducing the risk of spreading malware.

## Security Monitoring

Miovision implements a security monitoring program that collects information from internal network traffic and system behaviors and analyzes it for suspicious or abnormal activity. The program uses commercially available tools for monitoring system behavior, communication, and an industry leading managed detection and response vendor that provides operational security experts on a 24/7 basis.

## Incident Management

We implement an incident management process for security events that may impact systems or data. The process is based on NIST guidance provided in NIST SP 800-61, Computer Security Incident Handling Guide, and includes procedures to provide notifications directly to customers and external parties that may be affected. To report a suspected security incident, please contact security@miovision.com.

# Product Development Security

Security is integrated into our product design and development practices through the use of security tools and techniques at multiple steps in our product development lifecycle.

### Employee Identity and Access Management

A core aspect of our secure product design and development practices is managing employee access to designs and implementations. An employee is only authorized for the level of access required to perform their job function. This includes restricting access to source code, operational software, and supporting infrastructure to authorized employees only. Access is managed through strict employee authentication that confirms an employee's identity and subsequent authorization that confirms an employee's job function. Both steps require multi-factor authentication (MFA).

### Secure Software Development Lifecycle

Our Secure Software Development Lifecycle (SSDL) is designed to identify and mitigate security risks during the development of Miovision software products. It incorporates industry best practices and guidelines from organizations such as SANS Institute and Open Web Application Security Project (OWASP) and is regularly reviewed for continual improvement.

Our SSDL integrates security testing, reviews and monitoring throughout the key stages in software development:

Design | The Design phase is where product managers, technical architects, and developers begin the high-level architecture and planning of new software capabilities and the supporting operational infrastructure that satisfies product requirements.

Develop | The Develop phase is where developers create or modify operational software and its operational infrastructure to meet the design requirements.

Deploy | The Deploy phase is where operational software and its infrastructure are deployed to test and staging environments, tested for quality assurance, and then deployed to our production environment for availability to customers.

Maintain | The Maintain phase is where operational software and infrastructure in our production environment is subject to ongoing maintenance and monitoring for performance and security.

# Miovision Detection Solution

The Miovision Detection solution includes the Miovision One platform and Miovision hardware.

## Miovision One

Miovision One™ allows you to remotely manage and track your traffic network, while also providing industry-leading performance measures and actionable insights. Miovision gives you complete control of your data through an open platform that integrates with existing investments and other traffic technologies. The Miovision One platform includes hardware and software.

Miovision One provides the entire range of solutions needed for a traffic team to collect, monitor, and understand their traffic signals. This includes a managed cellular connection, tools for signal monitoring, video streaming, Automated Traffic Signal Performance Measures (ATSPMs), and maintenance alerts.

Miovision One is a web-based platform that allows agencies to access their traffic data, reports, and analytics. It enables agencies to remotely manage traffic signals, including monitoring and alerting functionality. Users can remotely access signal telemetry, fault alerts, video streaming, traffic data, and network information via cloud architecture.

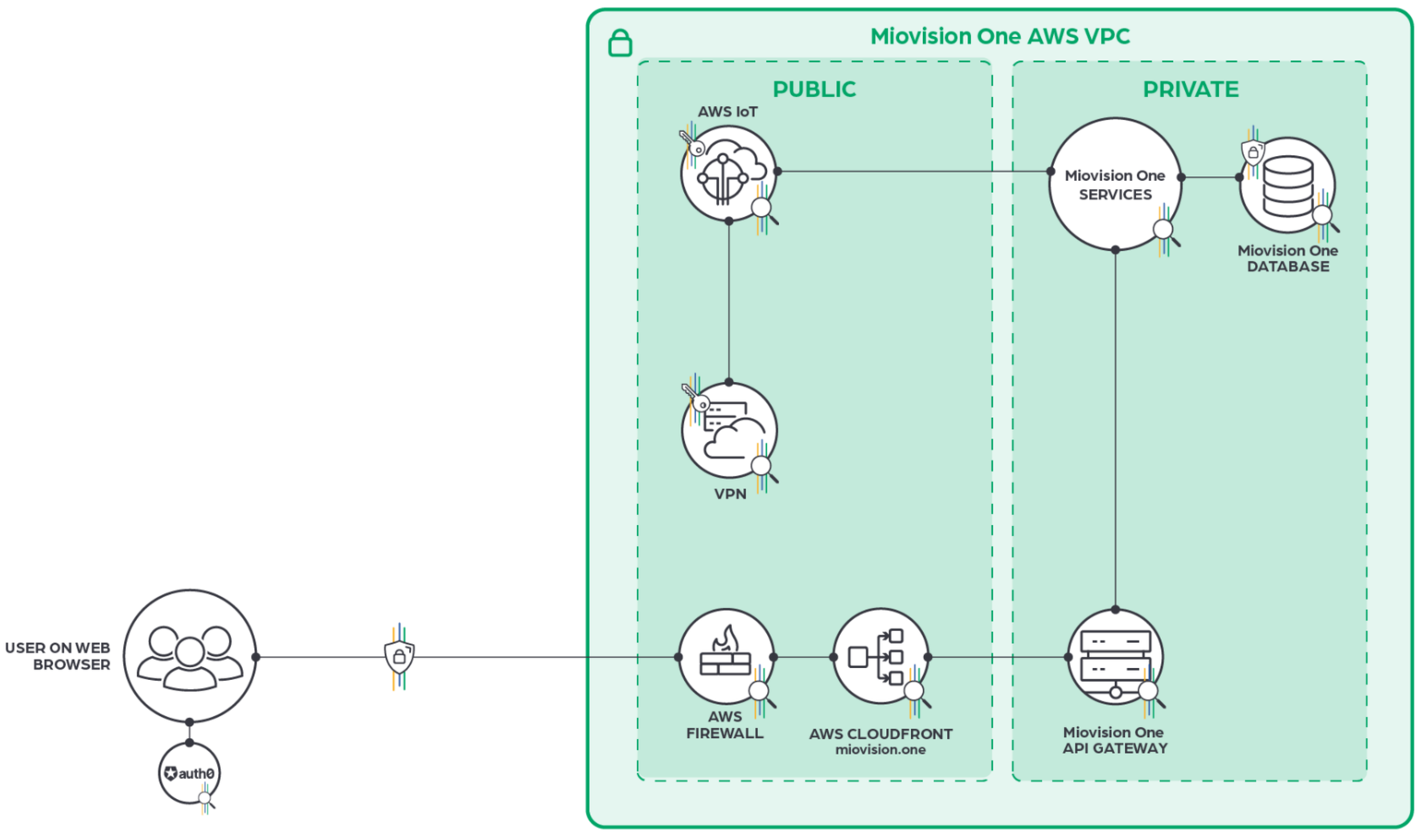
## Miovision Hardware


**Miovision Core:** Miovision's in-cabinet communications device. Performs monitoring, traffic operations, and management solutions- gathering data from the existing controllers and devices. It also provides convenient, secure remote connectivity to the cabinet. It can read the data from existing controllers and cabinet devices and transform it into meaningful insights. Also includes a 4G LTE cellular connection to provide wireless connectivity to traffic signals.

**Miovision Core DCM:** Miovision Core with the Detection and Counts Module (DCM). The DCM slots into the Miovision Core mainframe, providing the edge processing power necessary for Miovision's specialized computer vision algorithms.

# Miovision One Security

Our security model incorporates a defense in depth approach that considers the security of its cloud environment, devices, users, and data. Its high-level cloud security architecture is shown in the following figure.




## Cloud and Network Security

Miovision One is hosted in an Amazon Web Services (AWS) Virtual Private Cloud (VPC), a virtual network in the AWS cloud. AWS logically isolates each VPC within the AWS cloud and provides each VPC owner with security controls to further protect the resources within their virtual environment. Miovision One operates in a virtual network dedicated to Miovision and implements multiple security controls to protect its resources.

The Miovision One virtual network is separated into a private and public subnet to host the resources that comprise the Miovision One platform. Resources in the private subnet are not directly accessible via the Internet; these resources are only accessible by authorized resources in the public subnet that are members of the corresponding AWS security group. Resources in the public subnet are accessible via the Internet and are subject to multiple network access controls, such as IP address deny lists to prevent known malicious actors from attempting to access resources, rate limiting connection attempts to prevent denial of service attacks, and application firewalls. Resources leverage mutual Transport Layer Security (TLS) authentication to interact with each other, regardless of their subnet location. The Miovision One platform and its virtual network leverage the security logging capabilities provided by AWS and are monitored for suspicious or

malicious activity. If any such activity is detected then Miovision staff are alerted and we perform an investigation and communicate any instances where a customer may be affected.

## User Security

Users of Miovision One access the platform via a web-based application using a standard web browser. They must have a valid Miovision One account and must authenticate prior to accessing the service. User accounts are assigned role-based permissions and may be assigned read only, read and write, or administrator permission sets.

Miovision One supports service provider initiated (SP-initiated) single sign on (SSO) using the security assertion markup language (SAML) version 2. Customers that leverage an identity provider (IdP) solution that supports SAML version 2 can work with Miovision to enable SSO for Miovision One.

User authentication, account management, and SSO integration for Miovision One leverages Auth0, an Okta company that provides an industry-leading authentication provider solution. For more information on Auth0, please visit https://auth0.com/security.

TLS is used to protect the web browser session via mutual authentication (browser to Miovision One platform and platform to browser) and to encrypt communication. TLS versions 1.2 and higher are supported.

## Data Security

Protecting data is a core component of the Miovision One security model. All data in transit and communication with Miovision devices and resources is encrypted using the TLS protocol. Data stored in the Miovision One databases (such as intersection data) is encrypted using their native encryption capabilities. All data processing and storage is performed within the Miovision One VPC, an isolated environment.

## Security Monitoring

In addition to security monitoring of Miovision devices, the Miovision One platform leverages an industry-leading cloud security posture management solution to implement security monitoring and threat detection for suspicious or malicious activity. This monitoring includes user behavior (such as multiple failed login attempts) and system behavior such as unexpected communication attempts. When such activity is detected, Miovision staff are alerted to investigate to determine if they represent a security risk or require internal action.

# Miovision Device Security

Miovision supports two key models for deploying a device at an intersection. The first model is a cellular deployment that leverages a cellular network at the intersection, and the second is a fibre deployment that leverages a customer network at the intersection.

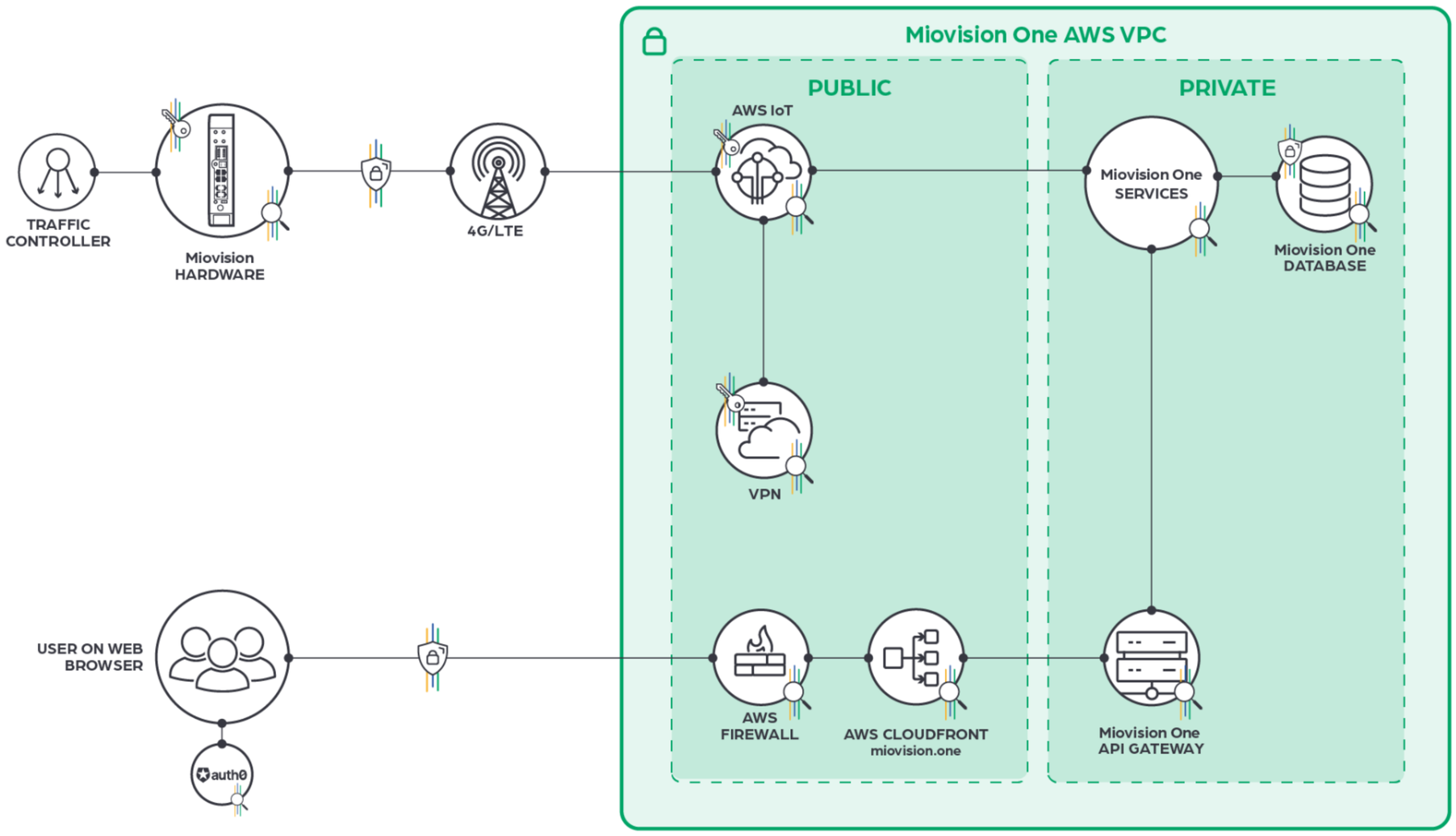
The main design principle behind Miovision device security is that we do not trust the network, because at some point the communication between a device and the Miovision One platform will leverage the public Internet.

Miovision devices communicate with the Miovision One platform via the AWS IoT service. Depending on the deployment model, as shown below, devices communicate with the AWS IoT service directly or via the Miovision VPN service. Both deployment models use certificate-based mutual authentication and encryption to protect the direct communication with the device.

Miovision devices are monitored for suspicious or malicious activity and when any such activity is detected, Miovision staff are alerted to investigate to determine if they represent a security risk or require remediation.

## Miovision Cellular Deployment

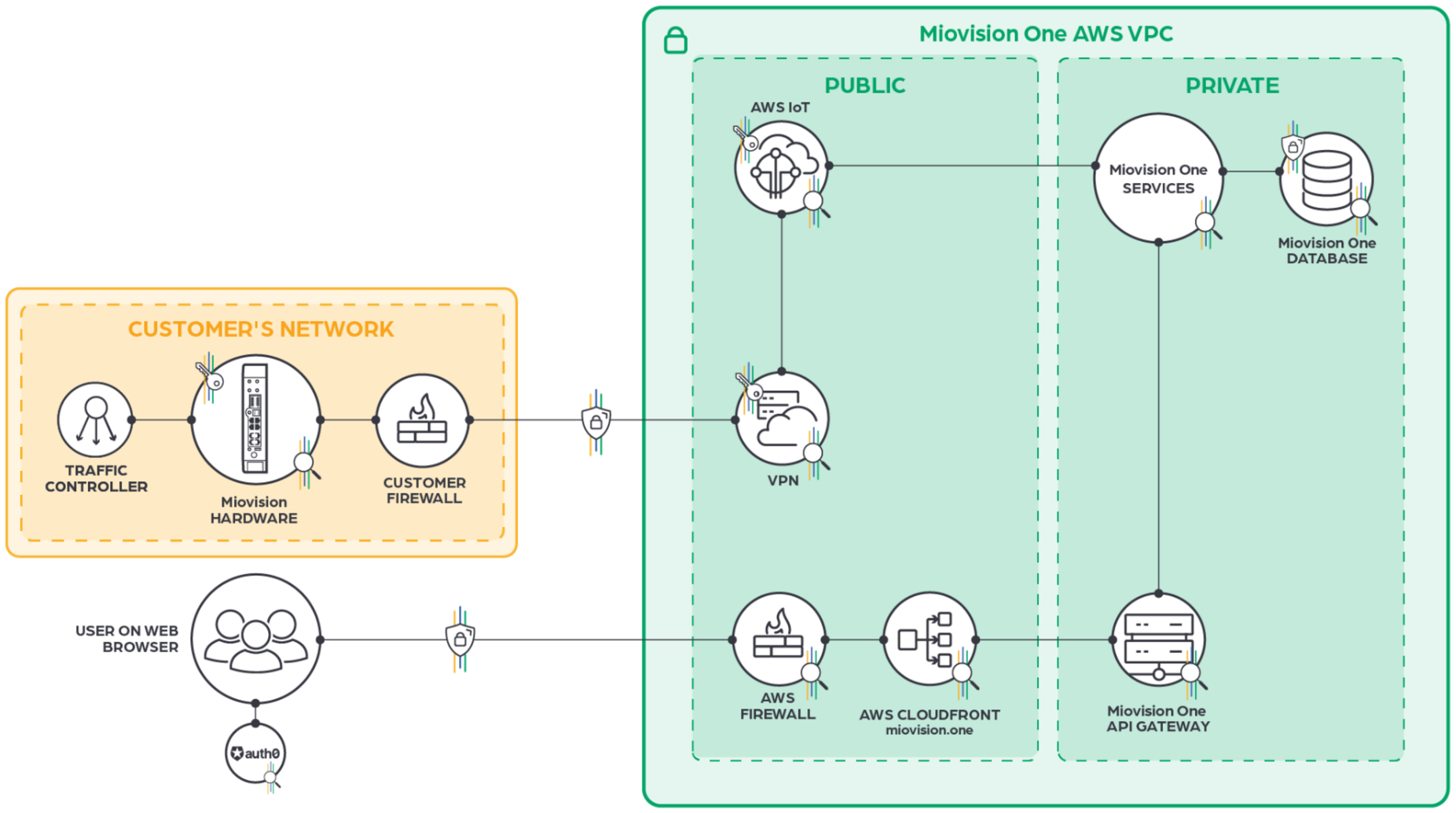
In the cellular deployment model, a Miovision device is wirelessly connected to a cellular network that exists at the intersection.  By default the device connects to a private Access Point Name (APN), a private cellular network.  The cellular deployment model is shown in the following figure.




The device communicates with the Miovision One VPC via the AWS IoT service, over the cellular network. Therefore, network configuration changes are not required for the customer network. This deployment model is ideal for intersections without a fibre network available or for customers who wish to leverage the convenience of a direct connection to the Miovision One VPC. In a cellular deployment, TLS is used for mutual authentication (Miovision device to Miovision One platform and platform to device) and to encrypt communication using AES-256. TLS versions 1.2 and higher are supported.

## Miovision Fibre Deployment

In the fibre deployment model, a Miovision device is physically connected to a customer network that exists at the intersection, as shown in the following figure.




The device communicates with the Miovision One VPC via the Miovision One VPN service, over the customer network. The communication is initiated by the device and is outbound only as part of the Miovision One defense in depth approach to security.

To support a fibre deployment, customer networks must provide or permit the following for each deployed Miovision  device:

- An IP address
- A default gateway
- Primary and secondary DNS servers
- TCP outbound to its-mgmt-production.signals.miovision.com, port 443
- TCP outbound to gateway.signals.miovision.com, port 443
- UDP outbound to gateway.signals.miovision.com, port 1194

In a fibre deployment, TLS is used for mutual authentication (Miovision device to Miovision One platform and platform to device) and to encrypt communication using AES-256. TLS versions 1.2 and higher are supported.

### Miovision One Administrative Access

Authorized Miovision employees may access the Miovision One platform and its supporting infrastructure to manage service operations and performance and to provide customer support. This administrative access is limited to employees who need access for their role, such as Customer Support or Service Operations, and is regularly reviewed. Access is managed through employee authentication that confirms an employee's identity and subsequent authorization that

confirms an employee's job function. Access to Miovision One platform infrastructure is strictly limited and controlled and requires multi-factor authentication (MFA).

Authorized Miovision employees may access Miovision devices to provide customer support. Customers that wish to disable this access can do so by disabling the "Support Access" toggle in the Miovision One web portal.

# About Us

Miovision provides cities with modern tools to fix today's traffic problems. We offer solutions that collect multimodal traffic data and uncover actionable insights, helping municipalities get more out of their road network. This results in streets capable of moving more people – safely and efficiently – whether they are in a car, on a bus, on a bike or e-scooter, or walking. Since 2005, our systems have counted more than thirty billion vehicles around the world. We have offices in Kitchener, Canada as well as operations in Germany, Serbia and the US. For more information, visit miovision.com.