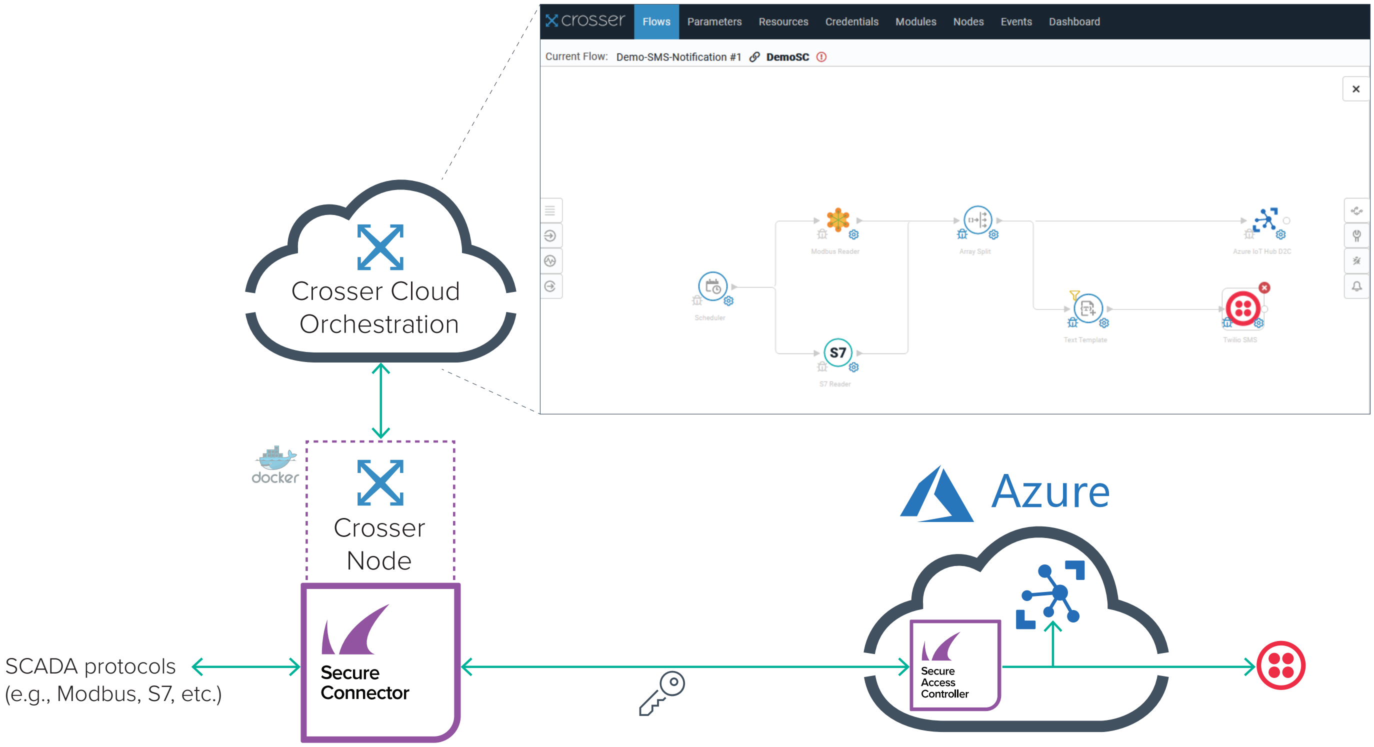
Security and intelligence for the industrial edge

Secure and scalable connectivity meets edge analytics and intelligence

The technology integrates Barracuda's secure and scalable connectivity solution for IoT environments with Crosser's edge analytics solution – all on a single hardware platform.

The challenge

Collecting, processing, and analyzing production-critical data in IoT and OT environments requires edge computing. Traditional server architectures cannot meet modern requirements in scalability and computing power. Near real-time processing also demands that the intelligence be closer to the edge. Edge analytics and consolidation can also help to reduce overall data loads, prefilter at the edge, save storage and bandwidth, and, finally, reduce the cost for cloud services.



Current Flow: Demo-SMS-Notification #1 DemoSC

The Crosser platform

The Crosser Edge analytics software allows data produced by sensor-rich assets like machines, equipment, and devices to be pre-processed in real-time closer to where it is created.

Removing dirty and irrelevant data significantly reduces the cost or storing and processing collected data. Sometimes less really is more. Crosser let's you collect meaningful data only, discard unnecessary information, and use edge analytics to combine data points and convert to a commonly used format such as MQTT or OPC-UA.

Local triggers between machines or PLCs with ultra-low latency can run autonomously without cloud connectivity and report anomalies or trigger alerts based on events.

The Crosser Cloud is the heart of the platform – where all design and orchestration takes place. The Crosser Node is the real-time engine processing and analyzing all data right at the edge in a Docker container.

Barracuda Secure Connector

With digitalization growing rapidly, and the industrial internet of things becoming reality, security challenges are becoming dramatically more complex. Managing and protecting network traffic among the vast numbers of devices now going online is a potential logistical nightmare. Barracuda Secure Connector is designed with unique capabilities to help you secure IoT traffic easily and economically.

The Secure Connector is a small hardware appliance optimized to efficiently connect remote devices and micro-networks to a Secure Access Controller in the public cloud or a data center. The configuration is centrally managed, with the Secure Access Controller acting as a policy and security enforcement instance where all traffic is processed. With its powerful next-generation security features and advanced remote access capabilities, it introduces a new level of security into IoT networks.

The Secure Connector itself acts as a hardware VPN client and forwards all traffic to a central location. On top of the security and connectivity features, the Secure Connector is an edge computing hardware platform that can run the Crosser Node application in a Docker container. The deployment and updates of the container application are centrally managed.

The joint solution

The Barracuda Secure Connector is a scalable and secure connectivity solution designed to connect hundreds or thousands of industrial IoT endpoints to a central location. The configuration is centrally managed and does not require any firewall-specific knowledge at the edge. In addition, the Barracuda Secure Connector also supports custom applications in a Docker container. With the Crosser Node application running on the Barracuda hardware platform, only one hardware device can provide edge analytics and intelligence with secure connectivity.

Key benefits

- Small form-factor firewall units designed for industrial environments
- Extreme scalability to accommodate very large and dispersed networks of industrial and IoT devices
- Ease of deployment and use, intuitive centralized management, and granular, multi-tiered role-based administrative access
- Zero-touch deployment
- Up to 14 layers of security inspection on different network layers with application and industrial protocol detection
- On-demand remote machine access operable by floor staff with no IT expertise
- Local intelligence and automation
- Transformation of raw data and merging of more data points without increasing data cost
- Significant data reduction by removing dirty and irrelevant data
- Granular control of data sent for remote analytics or received for remote control

Use cases

Cleaning and normalization

A common IoT scenario is collecting data from various sensors and devices that are often communicating with different protocols and setups. To be able to use that data, users must normalize and prepare the data for further processing.

Predictive maintenance

A global manufacturer wants to become a leader in real-time remote condition monitoring and predictive maintenance within the process industry by using anomaly detection algorithms and machine models for predicting and optimizing machine runtime windows. And so it considered Crosser's detection intelligence combined with Barracuda's secure remote access capabilities to be *the* solution for maintenance.

Remote condition monitoring and connected machines

The Barracuda small-factor hardware device with its Wi-Fi and 4G capabilities was designed to bring connectivity to distributed environments. All kinds of stationary or mobile machines and vehicles can be connected in order to analyze data for condition monitoring and enhanced service programs for the end customer.

Remote access

Whereas traditional edge solutions have a limited capabilities when it comes to control and access, edge devices using the Barracuda connectivity solution enable full access over encrypted VPN connections. This results in granular control over which data is processed while also allowing for full access when desired. In addition, access can be controlled via numerous authentication methods.

Azure integration

Barracuda and Crosser partner closely with Microsoft and offer native product integration with Azure. Barracuda Firewall Control Center, Secure Access Controller, and Crosser Node are available in the Azure Marketplace and provide seamless connectivity to Azure Services. Both the Barracuda Secure Connector and the Crosser Node application can be integrated with Azure IoT Edge enabling deployments directly via the Azure Marketplace. And finally, with Crosser the data can be streamed directly to other Azure Services, simplifying the architecture and reducing cloud consumption costs.

About Barracuda

Barracuda is committed to making the world a safer place and believes that every organization should have access to cloud-ready, enterprise-wide security solutions that are easy to acquire, deploy and use. Barracuda protects email, networks, data and applications with innovative solutions that grow and adapt as the customer journey continues. More than 200,000 companies worldwide trust Barracuda to help them focus on growing their business.

Learn more at barracuda.com.

crosser

Crosser designs and develops streaming analytics and integration software for any edge, on-premise or cloud. The Crosser Platform enables real-time processing of streaming or batch data for industrial IoT, data transformation, analytics, automation, and integration. The solution is built to fight complexity with simplicity through the Crosser Flow Studio, the visual design tool that enables teams to innovate faster than ever without developers. The software is ideally suited for enterprise customers of various industries and applications, including industry 4.0, condition monitoring, predictive maintenance, and next-generation hybrid integration.

Learn more at crosser.io.

Barracuda®
Your journey, secured.

SOLUTION BRIEF • US 1.0 • Copyright 2021 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com