TeskaLabs’ SeaCat Application Gateway

An Evaluator’s Guide

TeskaLabs

Table of Content

Introduction

Each year sees enormous growth in the number of devices connected to the Internet. However, one of the biggest obstacles to the expansion of Internet of Things (IoT) is the management of such a large number of devices. This is a significant challenge for IoT as the vast array of IoT applications tend to be managed manually, and therefore inefficiently. Enterprises that operate large-scale IoT applications invest up to 80% of their time and money into IoT application management. This represents a significant barrier, limiting their adoption of IoT apps.

This Evaluator's Guide focuses on how TeskaLabs SeaCat Application Gateway (SeaCat) provides and manages a reliable, risk-free and secure method of managing fleets of connected IoT devices, increasing operating effectiveness while at the same time helping enterprises address their security-related need.

What is SeaCat Application Gateway?

SeaCat Application Gateway is a high-performance networking and security technology designed to easily operate large fleets of connected devices and applications. For instance, it can be used for Smart Grid (energy), Connected Cars (transport and logistics), Smart Health (Health) and in B2C mobile applications or applications deployed as cash registers and kiosks.

SeaCat technology works independently of existing IT infrastructure and the Internet connectivity of individual devices or applications. The technology is highly autonomous and provides a large level of flexibility and interoperability in monitoring, management, and configuration areas.

Built on the concept of Software Defined Network (SDN), SeaCat has the advantage of allowing companies to maximise the use and utilisation of their existing equipment at remote locations. At the same time, there is no dependency on network connectivity or specific hardware vendors. This is because SeaCat Application Gateway can run on numerous hardware network elements including industrial computers, routers, servers, mobile devices, tablets, and more.

SeaCat delivery includes integrating the technology with a security operation centre (SOC) and the training of IT personnel (IT operators) to increase their competency and help them shorten the return on investment (ROI). IT operators are able to address security and operational incidents quickly, often pre-empting problems and preventing them from occurring - incidents which could have a highly negative impact on the company's operations and reputation.

Key benefits

Faster route to market

Time-consuming proprietary solutions developed in-house will inevitably fall down when it comes to scalability and security. This can lead to an expensive, drawn-out development cycle, where the end results cannot be accurately predicted. This is because organisations often lack the necessary expertise in cybersecurity, networking, and scalability of highly-distributed connected products. On the other hand, SeaCat technology offers an out-of-the box option that allows for fast integration with existing or new applications, and therefore significantly shortens the time to market.

Centralised management of the connected product

A lack of the effective management is the most common problem in the current generation of large-scale IoT applications. This problem poses a serious risk to growth, revenue, brand, and reputation.

SeaCat technology enables organisation to efficiently manage and grow their fleets of devices, so that they don’t have to worry about whether or not their devices are being properly managed and run.

Uncompromised security

Application security is a complicated topic, and many organisations fail to properly implement security measures into their products. A cyber security flaw can result in significant damage to the company or users, which could lead to fines and a loss of reputation. Operators of the connected product also need to conform to numerous regulations and policies to maintain safety and privacy of the users.

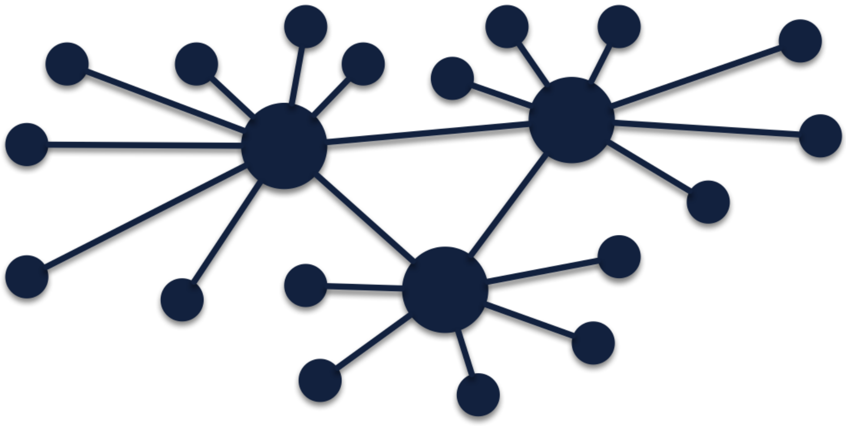
SeaCat technology has been designed with security as the top priority. It provides proven protection, strong cryptography and compliance with industry regulations to ensure that both businesses and users remain safe and secure at all times.

SeaCat Application Gateway Overview

SeaCat technology is made up of multiple components. The main parts are SeaCat Client, which is a library or stand-alone executable (also called SeaCat Agent), designed to integrate with the connected device or application. SeaCat Gateway acts as a central orchestration node in the data centre or the cloud. SeaCat Client is integrated with the applications on the end devices such as industrial computers, routers, remote telemetry / telecontrol units (RTU), and numerous types of hardware.

Together SeaCat Gateway and SeaCat Client provide:

- Comprehensive security protection against cyber-attacks on the application and the central data hub, including the protection of data transmission between the application and the Gateway
- Centralised remote management, including remote access and control
- Powerful monitoring of the device fleet and the applications fleet that these devices are running
- Permanent, unambiguous, and non-transferable identification of connected devices and applications
- Encryption of the data traffic transmitted amongst devices and gateways, thus ensuring the data's confidentiality and integrity
- Strong authentication of applications and devices regardless of their location
- Separation of individual communication channels
- Easy scalability from hundreds to millions of simultaneous active connections
- High availability of the entire system



High performance networking and scalability

Traditional software such as HTTP or VPN servers are built on software threads. However, threads have a high CPU overhead and don't scale well because these threads are competing for access to shared resources such as memory or network interface (Ethernet). For this reason, software servers cannot scale linearly with the growing number of connections, instead succumbing to a condition called "C10k problem." Thread-based servers cannot handle over 10,000 simultaneous connections. A common way of solving this problem is to increase the amount of hardware used. However, this approach is not economically viable for applications which have to process thousands and more concurrent connections.

SeaCat Application Gateway is designed to avoid the C10k problem. It is not based on threads, but rather utilises an event-driven architecture. This advanced architecture uses isolated groups of resources (such as memory, processes, and access to IO) for each the connection. This approach scales linearly and doesn't slow down due to competition for resources under higher loads. One SeaCat Application Gateway server can comfortably handle up to 50,000 concurrent connections on standard hardware.

Low network bandwidth usage requirements

Encrypted network communication such as HTTPS increases network data consumption because of the extra information like cryptographic certificates and keys need to be transmitted between communication parties to establish a secure communication channel. This increased data consumption can even lead to additional networking costs if a company pays based on the amount of data that they use.

The connection provided by SeaCat technology removes this overhead and provides optimal network data consumption. This is because Seacat Gateway performs the mutual authentication process (an important crypto-graphical procedure widely used to establish encrypted channels) only once, when the encrypted data channel with the application is first established. After this point, the encrypted channel is kept open and thus become persistent. This approach removes redundant data transmissions whilst maintaining a high security level of communication. If the connection is dropped because of the degrading network conditions, SeaCat can quickly and transparently recover the encrypted data channel.

Thanks to these features, SeaCat technology operates well on slow or low-quality networks, such as GPRS. SeaCat is agnostic to an underlying network technology and supports a variety of communication technologies including PSTN, LAN / WAN, GSM, LTE, 3G, NB-IoT, TCP / IP, M-Bus, radio, PLC, serial lines and more.

Support a wide range of communication protocols

SeaCat technology establishes an encrypted data channel agnostic to all communication protocols working from the fifth to seventh layer of the ISO / OSI model. The security of the communication is therefore not dependent on the used protocol. This function is available thanks to SeaCat client, which serialises digital data (aka communication protocols) into data frames and transmits them over the encrypted data channel to the gateway and vice versa.
SeaCat transports HTTP(S), Telnet, SSH, (S)FTP, TCP/IP, SCADA (IEC 60870-5-104), TCP / IP, and much more.

System concept

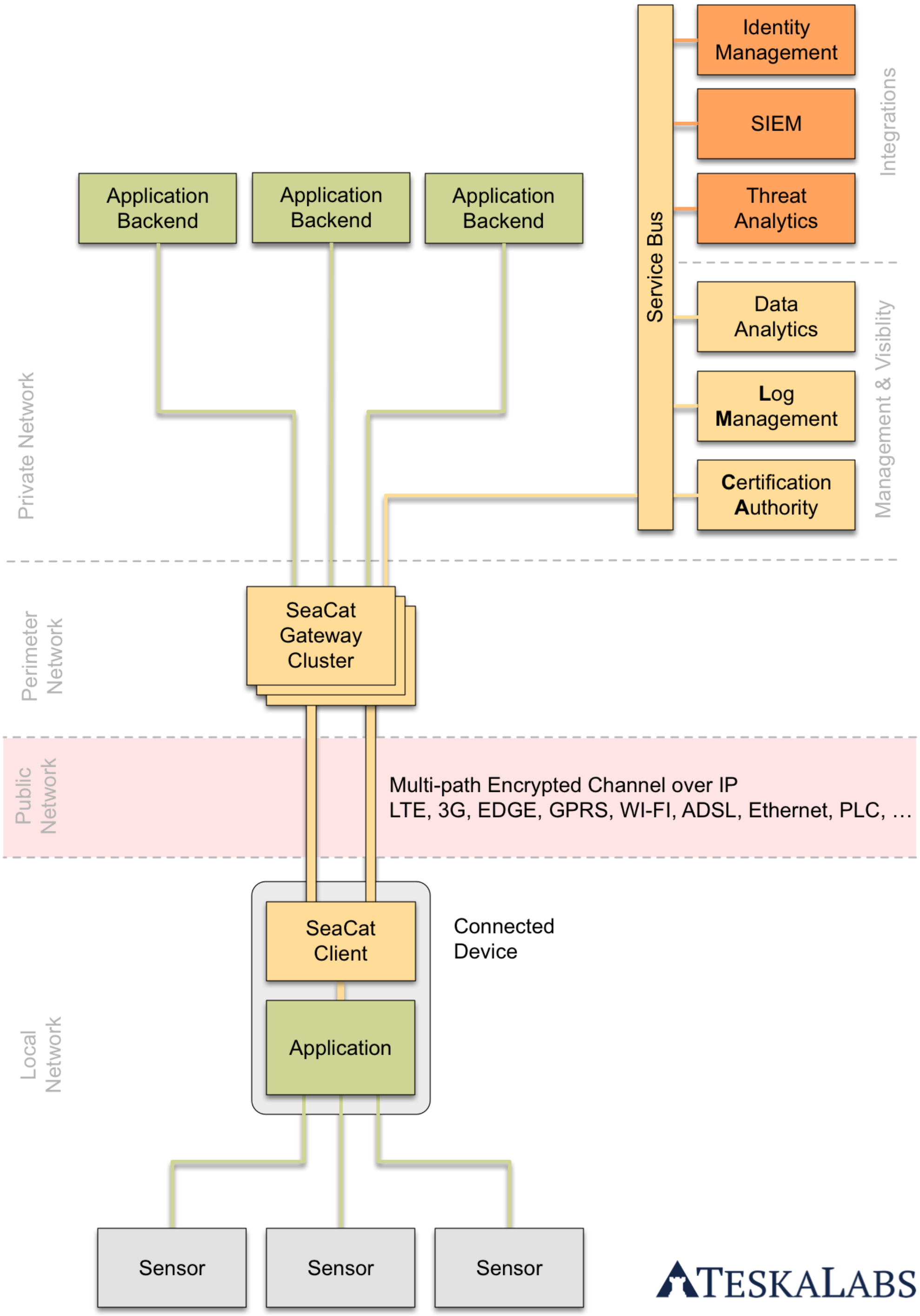


Figure 1: SeaCat concept diagram

Strong encryption and high security

Connected devices are preferred targets for cyber attackers. Cybercrime of connected devices and applications becomes an increasing risk. Without cybersecurity protection and secure management, people's private information could be accessed and stolen. As a response, SeaCat technology is designed with security in mind to comply with a wide range of industrial regulations.

Enterprise-grade cryprography

SeaCat Application Gateway encrypts the data channel between the application and the SeaCat Gateway. SeaCat technology uses OpenSSL cryptographic library and follows FIPS 140-2 security standards. To further improve the level of security, SeaCat exclusively uses TLS 1.2 and a limited set of cyphers:

- ECDHE, RSA, AES256, GCM, SHA384 (default settings)
- ECDHE, RSA, AES256, SHA384
- ECDHE, RSA, AES256, SHA256

SeaCat implements 4096-bit RSA key length and optional elliptic curve to uniquely identify the device or application.

It also uses mutual SSL authentication of communicating peers to protect against Man-in-the-Middle attacks. The basis of mutual SSL authentication is a certificate verification on both sides of the connection - this means that the client verifies the gateway certificate, and each gateway verifies the certificate of the clients. This approach ensures the confidentiality, integrity and authenticity of data sent between the Client and the Gateway. This approach also uniquely identifies every device and application. No other Client except the whitelisted one is authorised and uses the connection with the Gateway.

SeaCat uses TLS for TCP (stream) or DTLS for UDP (datagram), allowing many options of suitable transport protocols for specific network conditions.

Operational and security surveillance

SeaCat provides outstanding operational and security surveillance capabilities, thanks to telemetry and transaction meta-data collected by both SeaCat Gateway and SeaCat Client. The security and operational surveillance is made available via the Grafana web interface on the first level (operator) and Kibana on the second level (analytical).

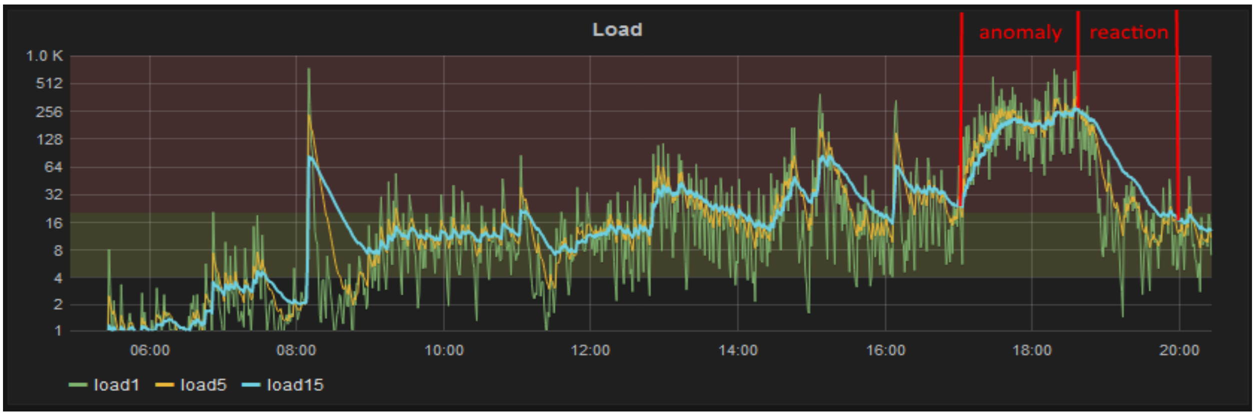


Figure 2 - Monitoring screen showing load anomaly to enable immediate reaction from operators

High visibility, effortless management

The commercial success of a connected product is tightly linked to the organisation's ability to manage and control their devices and applications in a flexible manner. Inefficient management or a total lack of management of connected devices poses a severe risk to growth, revenue, brand, and reputation. Proper management and operation practices consist of performing remote analysis of behaviours of connected devices, fixing bugs, shipping new features, deploying new configurations, and remotely monitoring and patching security issues. All these tasks are crucial for the sustainable and safe operation of connected products.

Centralised management of connected devices

SeaCat management console (Admin Panel), with its user-friendly interface, allows operators to manage all connected devices and applications from their web browsers. Operators can visualise complex statistics of in real-time, dive into detailed information of managed devices and gather the overall status of applications. They can remotely provide support from anywhere and at any time and resolve issues quickly and simply.

The Admin Panel can be integrated with an existing identity management service such as Active Directory to automate the identity management of connected products.

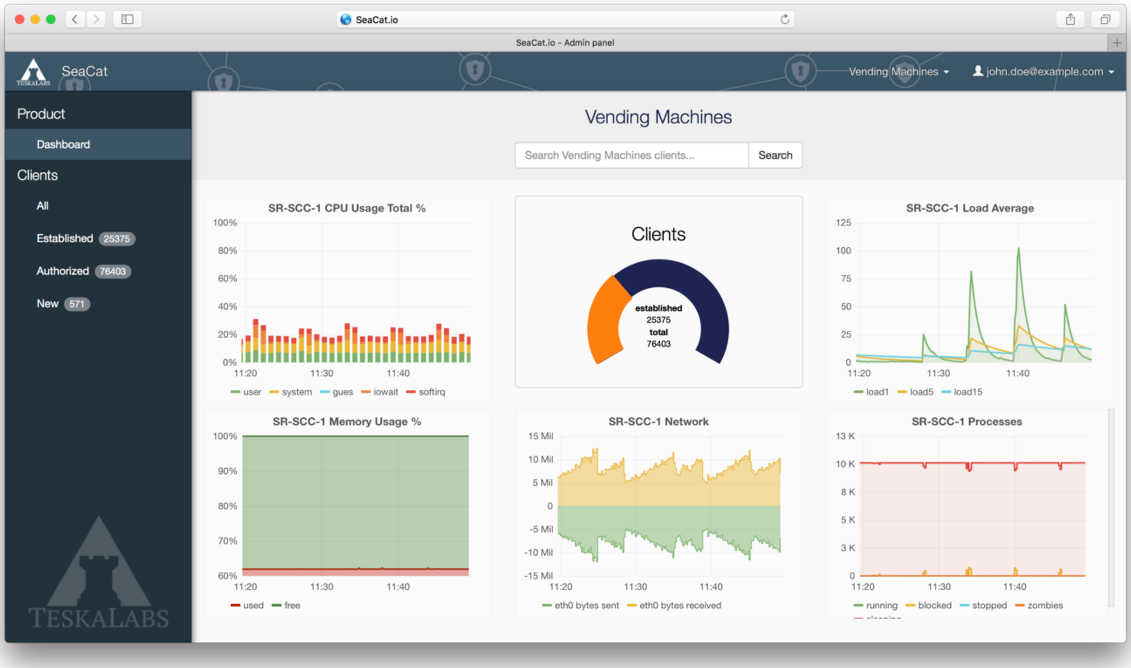


Figure 3: An example screen from SeaCat Admin Panel

Automated availability monitoring

TeskaLabs Availability Monitor (AvailMon) performs automated uptime and availability monitoring, 24/7. AvailMon immediately alerts operators of imminent or impending service unavailability and helps them maintain a high service level and quality. It also provides helpful options on how to measure key indicators set by the Service Level Agreement (SLA).

Advanced log management

SeaCat technology provides detailed visibility into the data flow and activities of all connected devices and applications, as well as actions made by these apps. This stream of data is called the audit log. SeaCat Gateway's audit log contains a detailed description for every transaction performed at the SeaCat Gateway and Client. The log also tracks other behaviours that can affect the application and the application backend such as availability, health status, and response time. To process this extensive audit trail, SeaCat Application Gateway features an advanced full-text search engine, ElasticSearch and statistical visualisation tool, Kibana.

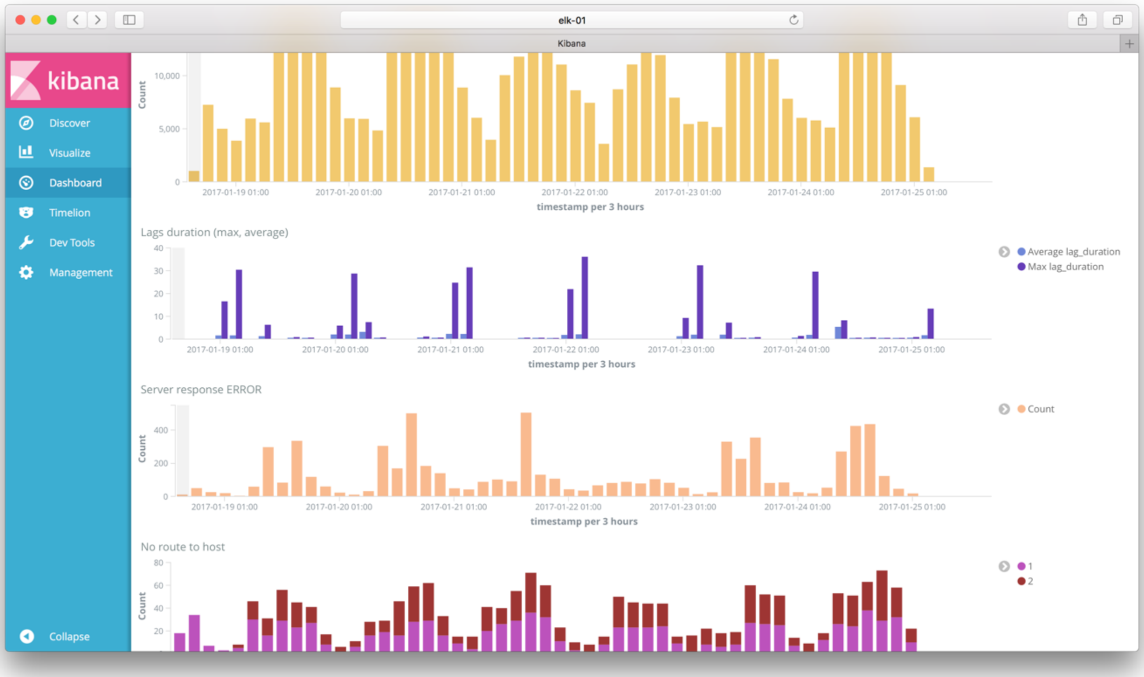


Figure 4 - Reporting and analytics via Kibana

Reports and statistics in real time

Administrators are provided with detailed reports and statistics about their connected devices and applications. They have access to a complete list of managed devices, network activity, and configurations, along with detailed information about the device and application activities. Administrators can customise the content and layout of each reports and export them to HTML, CSV, Excel, PDF and other formats.

Low Total Cost of Ownership (TCO)

SeaCat Application Gateway is designed to be a cost-effective connected device management technology. It leverages existing resources, integrates smoothly with current infrastructure, operates on a massive scale, and consumes lower data bandwidth. This adds up to a low TCO and gives a quick return on investment.

Frictionless integration

SeaCat is designed to fit smoothly into existing IT infrastructures and easily integrate with new and existing applications without any impact on existing backend systems or applications. Integrating an application with SeaCat is done by adding the SeaCat SDK to the application through a few lines of code – this process only takes around a day to complete. SeaCat client is equipped with many bridges to allow for integration with almost every major programming language and platform including Java, Objective-C, Python, iOS Swift, Android SDK, Xamarin, PhoneGap and ReactNative.

Leveraging existing Identity and Access Management

All connected devices require some form of authentication. Often, access credentials are stored locally on the devices themselves – an unsecure approach to user access management. Instead, SeaCat uses a centralised identity and access management (IAM) for flexible and more secure user authentication. SeaCat can integrate with 3rd-party IM software such as Active Directory and/or LDAP servers to automate the access right management and more.

SeaCat Gateway also supports LDAPS and other SSO technologies based on XML/SAML, so that it is as widely applicable as possible. Alternatively, SeaCat provides its own IM function without relying on an external Identity and Access Management.

Leveraging existing IT personnel

TeskaLabs works closely with internal IT personnel and third-party vendors to make the best use of their existing knowledge and skills. We can perform the integration either by ourselves, alongside internal staff, or train the staff to carry it out themselves entirely. We make sure that the IT infrastructure, systems and applications not only function just as they did before but also with the added benefit of protection. We ensure that the internal team has all the knowledge and tools necessary to utilize our technology successfully.

Case study - O2’s eKasa Project

SeaCat Application Gateway was integrated into the eKasa application for O2 Czech Republic a.s. and the Security Expert Center (SEC) managed by O2 IT Services.

This technology is currently used by over 30,000 simultaneously connected cash registers or Point-Of-Sales (POS) terminals. The current configuration is designed for used by up to 50,000 simultaneously connected POS terminals, and it is easy to scale to hundreds of thousands terminals if needed.

The POS terminals are connected via the O2 cellular network utilizing Wi-Fi, LTE, 3G or GPRS, depending on the availability at the site. The connection with these terminals is persistent and easily copes with changes in mobile network signal strength. One terminal processes approximately 15,000 transactions a day, which adds up to astonishing 450 million transactions per day.

Deployment of SeaCat technology consists of not only the central servers but also management (Admin Panel), telemetry collection (InfluxDB and Grafana) and analysis (ElasticSearch and Kibana) tools.

Each SeaCat Gateway produces an audit log and sends it via syslog (RFC5424) in the Log Management Tool and eventually into the Security Information and Event Management (SIEM) tool. The log stream is also simultaneously sent into ElasticSeach for advanced traffic analysis. Each SeaCat Gateway also provides telemetry and audit data of their operations.

From an operational point of view, our integration with O2’s SEC enabled the customer to significantly increase the problem solving capabilities when it came to issues related to the operation of the protected application. O2 operates the first and second level support, while TeskaLabs operates the third level support. This third level involves advanced traffic analysis and responses to operational and security issues with significant impact on the day-to-day business.

O2 teams monitor the technology using the SIEM tool and audit logs for security and log management tools for operation. Regular meetings were held between O2 and TeskaLabs teams to discuss the current and long-term findings. Furthermore, TeskaLabs prepared a regular monthly report which contained a summary of all important operational and safety events of the month. These reports allowed eKasa’s management to objectively steer the growth of the product.

Experience from O2 eKasa deployment

A vital phase in the project was in the period between SeaCat deployment and eKasa's commercial launch. Thanks to the vast amount of operational intelligence gathered by SeaCat about the application and communication over the cellular network, O2 was able to identify various operational issues. These issues were promptly resolved in close cooperation with the O2 teams. This led to a smooth and uninterrupted launch period, which was otherwise very intensive due to the commercial success of eKasa. This POS product quickly became the fastest selling POS system in the Czech Republic.

Figure 6: SeaCat is integrated into O2 IT Security Expert Center in Prague

"It's been a positive experience working with TeskaLabs. We needed to implement application security into our POS application very quickly, and we operate this service for our customers in a secure way thanks to TeskaLabs."

Michal Ruda - Head of Business and Product Development, O2 IT Services

To learn more about the case study:

visit this link https://teskalabs.com/customers/o2-ekasa

Conclusion

This Evaluator’s Guide has shown how the SeaCat Application Gateway technology meets the requirements of today’s enterprises including:

- A highly available, scalable architecture that can be scaled up to support millions of connected devices.
- Strong encryption and high security that meet all industry regulations and prevent cyber attackers from exploiting weakness in systems to steal customer data or disrupt businesses.
- High visibility and effortless management of connected devices and applications through the use of a web-based admin panel, automated availability monitor, advanced log management, and real-time reports and statistics.
- Achieve a lower Total Cost of Ownership through leveraging existing business and system resources.

About TeskaLabs

At TeskaLabs, we believe that the digital world has to be safe – and it’s our duty to keep it that way. As enterprises move toward mobile and Internet of Things (IoT), we are here to help them build and operate mobile and IoT applications securely.

TeskaLabs is an award-winning product company committing to creating the world's most comprehensive application security technology for mobile and IoT apps. We are a proud member of Microsoft BizSpark Plus, a strategic partner of O2 Czech Republic, and a Cisco Preferred Solution Partner.

TeskaLabs operates from our headquarters in London, United Kingdom, with an additional office in Prague, Czech Republic. More information is available at www.teskalabs.com.

To know more about managing and operating large fleets of connected devices

contact us at info@teskalabs.com today