# BVS

# BUSINESS VISIBILITY SUITE

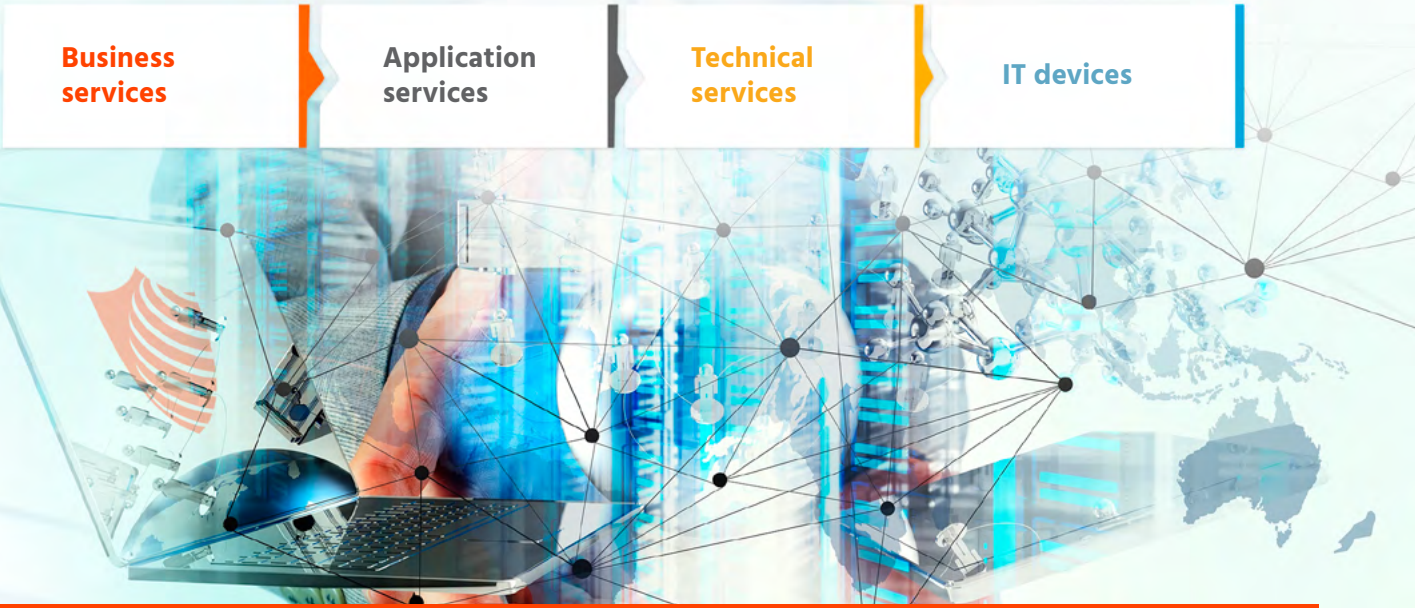
## Network & Business Edition

**A tool for unambiguous visualization of network communications and modeling of business services and IT infrastructure.**

IT asset management is the basic prerequisite for successful incident response in a rapidly changing cyber environment. Overview of relationships between IP devices in time provides both security analysts and SOC operators essential information for potential service interventions, rapid identification, and investigating security incidents in network infrastructure.

Novicom BVS uniquely combines the world of IT technology and the organization´s business services through intuitive modeling of dependencies between these layers. The key benefit of BVS is an automated metadata collection of network communication relationships between IT devices with the possibility of modeling provided business services of the organization.

**BVS ALLOWS YOU TO PRESERVE THE FOLLOWING RELATIONSHIPS**




**Business Visibility Suite is a tool for instant overview and visualization of IP device´s network communication to allow rapid incident response and identification of security incidents in the infrastructure. BVS also helps to understand the impact of incidents on provided business services and to prevent security threats.**

### Novicom BVS offers the two following modules:

**1. BVS Network Edition** – visualizing the current state of IT infrastructure and capturing communications between IT devices provide an image of network behaviour – what kind of traffic is in the given location.

**2. BVS Business Edition** – further extends capabilities of BVS Network Edition. It allows to model business services and their dependencies on IT infrastructure, provides an actual view on IT, gives an up-to-date view for the evaluation of the critical IT equipment, and its importance for providing the key services to end customers.

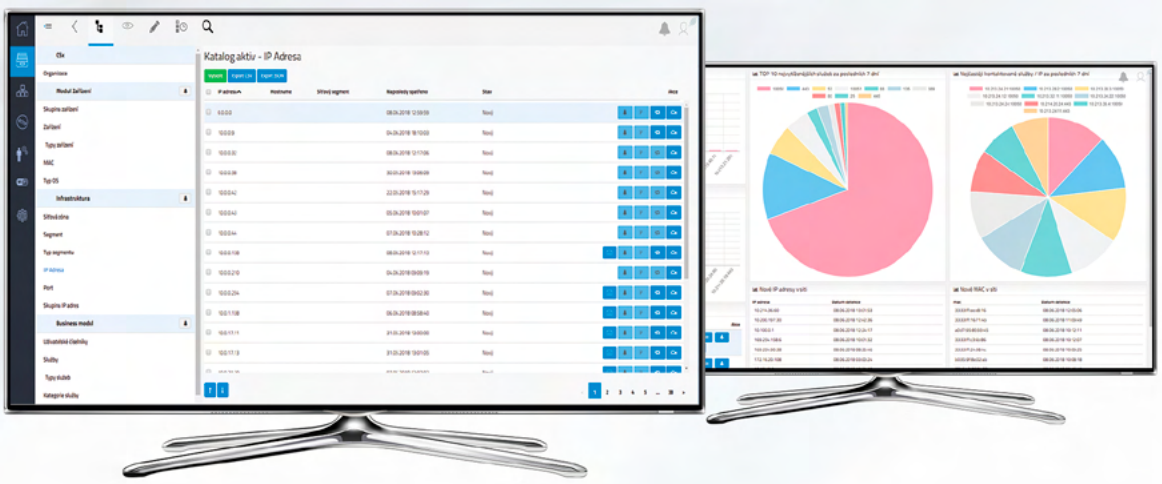
### Who can use BVS:

- IT (infrastructure optimization, day-to-day operation)
- IT security (analytical and forensic activities, investigation of attack propagation vectors)
- Security (equipment vulnerability, business services, risk, impacts, continuity)
- Owners of applications and business services
- Managers
- Security Operation Center (SOC)
- System integrators

**IT and SOC teams struggle with a quick incident response due to a lack of knowledge about the environment they are protecting.**

# Features and capabilities overview of Novicom BVS
## (Network & Business Edition)

| | |
|---|---|
| **Visualization of IT devices (assets) within the communication infrastructure** | Identifying relations between objects, which are a part of network communication. Business edition additionally includes visual modelling of the dependencies between services, applications and devices. |
| **Graphical interface** | Possibility to move through the relations hierarchically from the main nodes and network segments, through IP devices to the services ran on them and corresponding ports (drill-down). |
| **Alerting** | Infrastructure change alerts. Asset owner notifications. Notification about new unauthorized devices to proactively avoid security incidents. |
| **Automated metadata collection from devices in the network and their communications** | Using the autonomous probe to extract metadata about network communications and its visualisation almost in real-time. Basic information about communication links (network segment, IP source, IP destination, protocol, destination service - destination communication port). |
| **Option to tag new nodes (devices)** | For grouping elements falling within the same audit requirements or internal directives, it is possible to add custom tags. |
| **Visualization of inbound / outbound communication of an IT device** | IP address communicating to ports of other device - incoming communications to services ran on the ports of the IP address. |
| **Repository of asset information** | • Asset name<br>• Asset type<br>• Asset identifier (based on active type, e.g. IP address, MAC, port...)<br>• Asset administrator<br>• Custom user-defined metadata |
| **Organisation asset overview** | Export to XLS, CSV. |
| **Timeline** | Compare the current infrastructure status with a time segment from the past (e.g. by highlighting newly identified assets). |
| **Event overview** | Alerts for new unapproved devices will prevent incidents (alerting). |
| **Central fulltext** | Search for devices using any attribute. |
| **Data retention and performance** | Handling and storing large data volumes on the input (over 10 GB of data per day) and storing the key metadata required for incident investigation for the required period of time. |
| **Customizable access to specific application parts** | User authentication, secure access to specific parts of the application based on user-roles. |



# BVS Network Edition

The basic module **BVS Network Edition** answers the following questions:

- Which devices are currently in the network?
- Are these devices authorized?
- Which devices in the network are no longer used? (dead woods)
- Which connections are newly established and which devices are attempting to communicate? Are any of these connections having signs of a device with malicious behaviour?
- Who is the device administrator?
- What services run in the network?
- What other devices will affect the availability of the monitored device?
- What is the communication history (profile) of the given device and what changes were made on it?
- What is the set of affected devices that communicated with the given IP in the selected time span?
- What are the latest changes made on a device (open ports, change of risk, vulnerability, etc.)?

### BVS Network Edition use cases:

1. **Migration of the ICT infrastructure into the cloud**
   > Asset location (segment, owner, risk)
   > Identification of all services and dependencies
   > Device communication matrix export
2. **Identifying the scale of a cyber incident**
   > Organization will receive information about a possible compromise on its information system
   > IP address of the system is listed as an identifier
   > BVS visualizes all affected devices in the selected time frame
3. **Implementation of NAC**
   > Immediate orientation in the current network environment will allow faster deployment of NAC tools, including ADDNET by Novicom

### BVS Business Edition use cases:

1. **Support the work of the SOC team**
   > Prioritization of incident investigation according to the criticality of the asset.
   > Prediction of attack in relation to the criticality of assets
   > Rapid identification of the cyber incident scale
   > Business services level reporting

   Among other things, SOC operators are immediately informed about whether an infected device may be adversely affecting the high-critical service.
2. **Planning infrastructure changes with impacts on service continuity**
   > Prioritizing IT equipment repairs and patching
   > Fast creation of Business Impact Analysis
   > Identification and easy maintenance of information on the existence of the asset and its link to specific operated services
3. **Inputs to optimize IT infrastructure**
   > Input to separate critical and non-critical assets
   > Identification of „Single Point of Failure “
4. **Documentation of risk management**
   > Information on whether certain critical business services are dependent on highly vulnerable devices

# BVS Business Edition

**BVS Business Edition** with its focus and functionality is suited to SOC staff, IT managers, and IT security, who need to keep track of provided services, their availability, including links to supporting IT resources and possible risk factors.

### BVS Business Edition offers the following options:

- Creating logical assets representing the organization's technical, application, and business services.
- Notification of changes in IT assets and their impact on defined services.
- Visual modelling of dependencies between business services, applications, IT services, and IT assets (Business Impact Analysis) with automated asset identification and asset behaviour.
- Identify the impact of operational events on the organization's business services (what-if scenarios).
- Information on identified vulnerabilities. BVS obtains the data from vulnerability scanner outputs.
- Possible impact overview of vulnerabilities detected in IT technical support assets on the services provided (to prioritize the elimination of risks with the highest impact on critical services).
- Ensuring continuity of services through a better overview of the support infrastructure.

## The Added Value of Novicom BVS – Business Visibility Suite

- Simple and intuitive tool with significant support for tackling cyber incidents faster.
- Fast orientation in a complex network communications environment.
- Mapping the behaviour of customer ‘s communication and network infrastructure to quickly launch SOC services.
  - Network infrastructure and device identification, e.g. eliminating “shadow IT“.
  - Wi-Fi and network communications monitoring.
- Fast identification of network communication relationships between IT devices to reduce implementation time and setting of Network Access Control tools.
- Integration with NAC allows a comprehensive view from top business services to the level of physically identifiable devices.
- Minimum requirements for customer interaction, it is sufficient to provide basic information about address ranges that contain communicating elements.
- Identify and easily maintain relationships and dependencies between business services /applications and infrastructure - quickly find out which services are at risk of security threats.
- Clear and seamless migration of cloud infrastructure through an overview of the communication dependencies between the systems to be migrated and the main IS. This ensures reliable migration of all necessary systems and prevents downtime of services.
- Better planning of device management costs regarding what business services and the risk they are running on.
- The evidence of basic contextual information directly on an IT asset means saving time (it is not always necessary to find information in multiple tools).
- Quick identification of current „health of infrastructure„ and identification of potential security threats (prevention from uncontrolled triggering new network services, etc.).
- Integration with vulnerability scanner class tool outputs.
- Displaying details of detected vulnerabilities directly under the IP address.
- Automatically updated vulnerability records for IP addresses and ports.
- Vulnerability records repository.
- Possibility to export business services, including the total risk to XLS (by use of the existence of links to service supporting equipment).
- Supporting highly efficient business impact analysis (of IT infrastructure).

## BVS and Active SOC

**Novicom BVS is an important part of the Active SOC** (Security Operation Center) strategy, which Novicom, together with its SOC partners, is trying to promote on the market. **Novicom BVS**, together with the **Novicom ADDNET** (solution for efficient management of network services and network access control) and the **Novicom ELISA** (a tool for intercepting and evaluating cybernetic security events) **form a unique portfolio that prepares customers for fast and seamless connection to the SOC service.**

## Technical resources for Novicom BVS

**The following devices are installed in the customer environment:**

- Physical probes to monitor network connections (standard 1U in a rack, with 2 network interfaces – for SPAN data / 10Gbit / network switches monitoring interfaces + 1Gbit / for BVS server communication)
- Optional physical Wi-Fi probes for Wi-Fi spectrum monitoring (standard Mini PC devices compatible with most Wi-Fi standards)
- Management and collector on HW equipment delivered together with BVS solution or customer ‘s own resource
- Support for VMware and physical devices
- Proven Novicom APPLIANCE hardware is used Novicom BVS implementation
- The implementation follows the Novicom Implementation Methodology (NIM) best practices
- In the first phase, the necessary BVS infrastructure is deployed to the customer ‘s network and the BVS Network module is launched
- The BVS Business module can be efficiently used after business impact analysis Co-operation on tasks during Novicom BVS implementation
- Probes connection to monitored infrastructure switches (for IT infrastructure module)
- Scope definition for monitored segments
- Interpretation of selected communications subject to analysis
- Ensure connection between BVS component
- Providing access to core network services – DNS and NTP
- Remote access for 2-way communication and access to/from the device (BVS device operator > Customer environment; Customer environment > BVS device operator)

novicom

Novicom, s.r.o.
Prague, Czech republic

www.novicom.eu
sales@novicom.eu

BVS

NVC ENG 2020-09