ADDNET

novicom

Integrated DDI/NAC. A unique operational and security tool providing full network visibility, highly efficient IP address space management and advanced network access control.

ADDNET is a unique instrument which greatly improves and simplifies the efficiency of IP address space management and secure network access in large distributed networks. This is accomplished by integrating powerful network monitoring, IP address space management (IPAM), core network services (DHCP, DNS), network access control (NAC), and communication with networking hardware. By integrating these, conventionally independent services, a new level of network administration and network security is achieved.

ADDNET provides robustness, superior operational reliability, security and flexible implementation as a result of Novicom innovative technologies, such as the internal SGP grid platform, SDP communication protocol, or the internal Novicom appliance system.

Comprehensive network visibility, easy integration of ADDNET with other security tools, and the ability to be combined with the Security Operation Center (SOC) deliver a new option for fast response to detected security incidents.

NAC · DDI · L2 monitoring · Switch Interoperability · Dashboard & reporting · Network visibility · Active SOC · BYOD · Integration · Advanced network policies · DACL · Alert center

ADDNET KEY BENEFITS:

- **Highly powerful L2 monitoring** with the option to determine the physical localization of a device by integrating with cable records
- **Introducing an efficient IP address space management (DDI)** saves a significant amount of network administrators' time and workload
- **NAC introduction** – network access control management with the use of 802.1x or MAC authentication and authorization (VLAN assignment)
- Fully **automated administration of BYOD and mobile devices** and their clear network
- Standardization of network administrator's activities and possibility to centralize the administration of large distributed networks
- Significantly **improved operational reliability and performance of DNS, DHCP and NAC** through the utility of multiple redundancies and premium scalability
- **Cost Reduction** – efficiency is achieved on account of labour reduction and long-term monitoring of networking hardware port utilization
- **Full heterogeneity** and flawless interaction with networking hardware of leading technological manufacturers

- Unique **distributed network model support** – a guarantee of L2 monitoring / DDI / NAC operations even from remote locations or in a scenario when a connection to the central location is lost
- Backup **operation data collection from remote locations** – syslogs, data flows
- **Flexible operation** – suitable for both centralized and fully distributed organizations
- **Simple implementation** – combines the initial network sniffing with Novicom implementation methodology based on best practices'
- Ready to be implemented in **OT/SCADA technological networks**
- **Integration of ADDNET with SOC** – ensures fast incident response (event collection / assessment / reaction)
- ADDNET is ready to be **integrated with other instruments, such as MS Active Directory, SIEM, Log management, NBA, DLP, etc.**
- **Alerting** – rapid notification system installed in case of potential problems in a network

ADDNET functionality scope:

Powerful L2 monitoring

Real-time monitoring provides comprehensive knowledge about the location of a device (IP and MAC address) in the network (including switch port and physical location) including visualisation of a physical location of the device on a floor plan. It also gives the complete history of network operations for auditing purposes.

Complete DDI (DHCP / DNS / IPAM)

Provides distributed and reliable core network services (DHCP and DNS). Easy to manage through the integrated IPAM tool. Its integration with L2 monitoring allows the system to find real-time solutions for contradictions between ever-changing connections in the operation and IP address plan, thus helping the address plan to remain in accordance with the operational reality at all times.

• IPAM

The IP administration system provides a versatile and user-friendly address space management tool with an integrated administration of all necessary components (DHCP / DNS / NAC). It is easy to add a new device or change network parameters of existing devices within the address planning process.

• DHCP

Standard DHCP services are designed for operations in large distributed networks and in networks where maximum operation reliability or performance are required. The integrated L2 monitoring provides extended operational options and flexibility, including the assignment of fixed IP addresses through DHCP according to known MAC addresses.

• DNS

Integrated DNS services ensure reliable operation in distributed networks. Due to its flexibility, ADDNET is also able to control the existing DNS infrastructure through dynamic DNS updates. This ensures full consistency of IPAM, DHCP and DNS environment.

Integrated NAC (network access control)

The advantage of ADDNET's NAC integrated solution is the fact manufacturer of the infrastructure is of no significance as the solution is independent. Possibility to operate 802.1x in a combination with MAC authentication and possessing an ability to implement in large distributed networks. Consequently, ensuring NAC functionality from remote locations, even if it is temporarily disconnected from the central location.

• Full 802.1x authentication

ADDNET ensures secure device authentication anywhere within the network. The authentication data can be fully administered in ADDNET or obtained through integration with Microsoft Active Directory or other sources (OpenLDAP, Novell...). All standard authentication modes are supported – any combination of client certificate/user ID/password.

• MAC authentication with protection

As an alternative for devices that do not support authentication through supplicants, MAC authentication is available with additional protection. The integrated L2 monitoring can evaluate multiple parameters by analysing DHCP packages and other criteria. ADDNET notifies the administrator about MAC addresses that have been changed. The advantage of this approach is time efficiency, eliminating the complex implementation and management of full 802.1x supplicant. There is no need to manage exceptions – all switch ports are constantly under control.

• Authorization

Once the authentication is completed, the authorization process determines which network (VLAN) the device belongs to. In a combination with L2 monitoring, ADDNET can secure a dynamic device authorization in any location within the large network.

• Real-time information from NAC operation

ADDNET offers synoptical visualisation of information about devices that attempt to sign in within the frame of NAC – when, what ID (in case of external authority user), in which switch or port and to which network was the device segmented into.
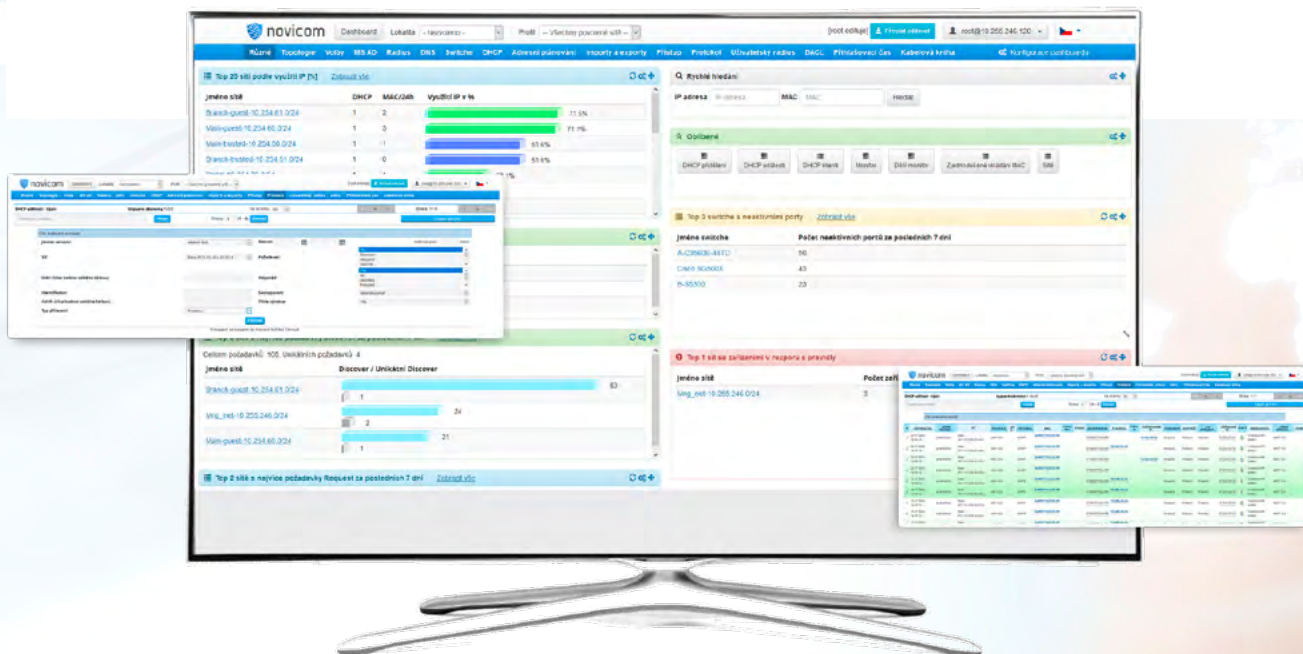
Emergency planning

ADDNET can define crisis sets and critical elements in the infrastructure of an organization. In the event of a security incident, it is possible to activate a crisis set with a single click and immediately disconnect all devices not listed in the defined set from the network.

Network administration and access control for BYOD and mobile devices

ADDNET provides complete IP management for wi-fi networks. The DDI/NAC administration model is complemented by a simple BYOD and mobile device management. ADDNET provides a self-service zone where new devices can be added easily to the network. It is also possible to create reception zones. The advantage of ADDNET's BYOD module is capability to support all types of user devices, regardless of the operating system and environment of the device.

Advanced communication with active elements

ADDNET provides clear information on active networking hardware in the repository. Continuous monitoring of the ups/downs states of ports allows ADDNET to monitor the port utilization and determine the number of unused networking devices. ADDNET also offers automatic backups of networking hardware configurations.

Dashboard

ADDNET presents the most important network and usage information in one place. With a single click, the user can move quickly from the dashboard data to detailed information in ADDNET. It is also possible to receive additional information on any IP/MAC at any time by right-clicking it and by using the drill-down technique to find any necessary information a user need. The dashboard is fully adaptable to the administrator/operator's needs.

Powerful reporting

ADDNET offers multiple ways to view device operations in the network. Along with the real-time information from L2 monitoring and detailed data from DHCP, it also provides information from individual switches. The combination of various sources in one unified user interface brings vast possibilities while obtaining detailed information on devices. This can be used in solving security incidents.

Advanced network policies

The interconnecting ADDNET functionalities allow simple implementation of advanced network policies while eliminating the more complex utilization of separate network administration tools. Some of these policies include:

- **Microsegmentation**

ADDNET effectively defines and administrate DACL policies on the majority of access switches. In practice therefore it is easy to adjust the global policies of the device to make it communicate in the network precisely to its correct functionality. Indicating it is allowed to communicate only in certain areas of the network, other sorts of communication are not allowed and this significantly increases protection from potential spread of ransomware infection type without the necessity to install an agent on stations.

- **Trusted Devices**

ADDNET supports trusted devices and trusted pools, allowing automated network configurations and access policies for large companies with remote branches. Along with their home network, trusted devices can also use different authentication, authorization and IP address assignment methods without having to execute any administrative interventions.

- **Login Time**

Organizations with fixed working hours can adjust ADDNET to operate only in certain periods (e.g. 7:00-19:00). This adjustment can also target specific devices or on the other hand grant chosen devices an exception.

Active SOC

Due to its functional flexibility and available distributed model, ADDNET is a highly sought-after complement to the Security Operation Centers (SOC). Along with the information obtained from monitoring, it provides SOC operators with information on core network services (DHCP/DNS and NAC). They can be further enhanced by reliable syslog and flow data collection from remote locations. SOC obtains complete information on the network and infrastructure operation of all network locations. The integration of SOC tools with ADDNET ensures an immediate incident response in the form of isolation or disconnection of the faulty devices by the SOC operator, without required cooperation with the local network administrator.

ADDNET

Integration

ADDNET is ready for several integrations which make network administration more efficient and ensure a fast incident response.

- **Operation data provision and collection**

ADDNET is a valuable source of assessment information using the most advanced tools of Log management or SIEM type. Operational information and information on non-standard situations are provided via the syslog interface. Additionally, ADDNET has the capability in the form of its extended applications to ensure continuous data collection of network operation (flow) or infrastructure status (syslog). These information are securely transmitted to be assessed via specialised applications (SIEM, NBA) in the central location.

- **Application integration**

ADDNET provides an interface for application integration with other tools, such as behavioural analysis (NBA), Log management, or SIEM. ADDNET is also ready to implement an interface for automated interventions. Credible detection systems, such as DLP, NBA, Anti-malware or IDS/IPS, can submit information and instructions necessary to execute administrative interventions.

Alert Center

ADDNET consists of an interface where the administrator/operator can administrate alerts on potential problems. The purpose of Alert Center is to simplify and automate the whole process of administration connected to the examination of alerts. The system integrates alerts from L2 monitoring (e.g. duplicated MAC), operation of NAC (e.g. unsuccessful authentication 802.1x), and more.

ADDNET AND ACTIVE SOC

ADDNET 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 ADDNET together with the Novicom BVS solution** (for visualization of network assets, including their connection to business services) and the Novicom ELISA (for intercepting and evaluating cybernetic security events) **form a unique portfolio that prepares customers for fast and seamless connection to the SOC service.**
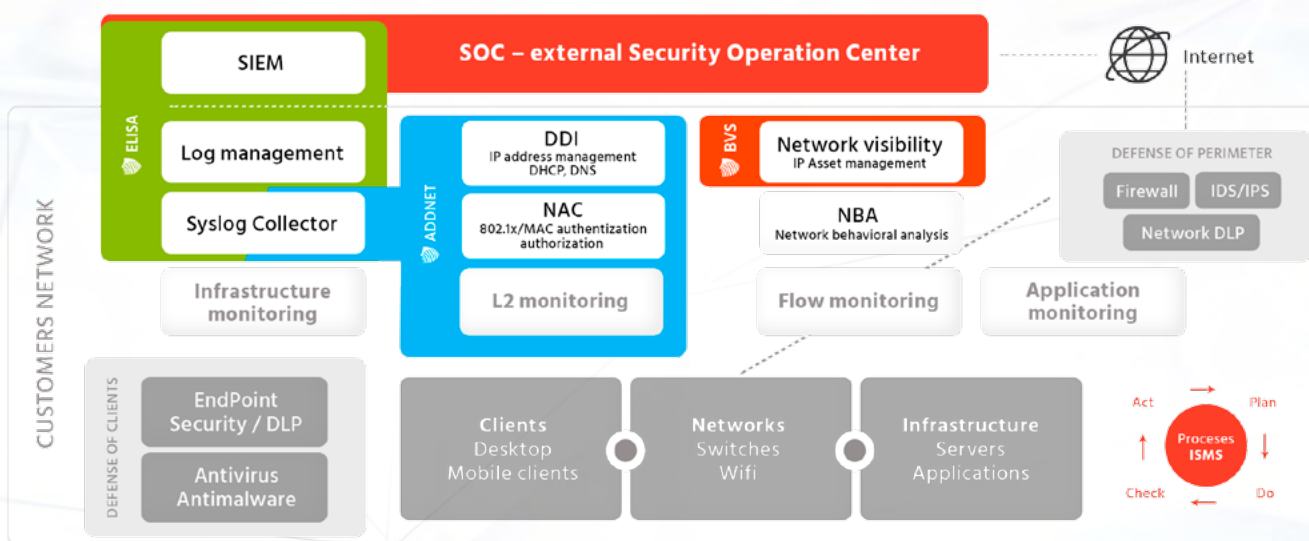
Customers using this product platform can then take full advantage of Active SOC's premium services. Thanks to this, selected SOC operators are able to guarantee a fully qualified active response to cyber-attacks in the 24x7 mode without the necessary cooperation with the system administrators at the customer.

This is fully in line with the current trend of using top security surveillance (SOC) as a service. This approach eliminates the economic disadvantage of acquiring a complete range of single-purpose technologies and the need to have an in-house highly specialized team able to face professional hackers at any time.

NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER