NISE

Neusoft Integrated Security EDR

Next Generation Endpoint Security Product

EPP + EDR + Endpoint Management

Neusoft

Product Overview

NISE is a security product that protects endpoints such as PCs from all security threats and helps to ensure the enterprise business continuity.
It enhances the enterprise security with a unified cloud management platform and a lightweight endpoint security agent.

Customer Values

- Protect PCs from new viruses and unknown threats with real-time protection (PC resident) and cloud-based threat intelligence detection.
- Strengthen security measures via PC vulnerability diagnosis and automatic remediation.
- Implement multi-leveled security measures for the entire network through correlation with UTM which protects the enterprise network at the exit.
- Remote desktop connection makes it easy to investigate, manually quarantine, and perform maintenance on PCs at risk of infection.
- Reduce operational burden with automatic post-infection response, automatic quarantine, alert notification and report analysis.
- Improve the security operation efficiency with internal assets detection, cloud management and classification by security level and category.

NISE ››› Highlights

Endpoint security of the "EDR + EPP + Endpoint Management" type

Enhance security with EDR and EPP, and manage your IT assets holistically.
Manage your enterprise network efficiently by listing device names, IP addresses, MAC addresses, organization information, asset information, etc.

Multi-functional and lightweight malware detection engine

Traditional signature-based scanning uses a huge signature database, so it occpies a lot of memory resources and puts a heavy load on your computer. NISE can detect malware more quickly and accurately by reducing the load on endpoints with multiple engines such as lightweight signatures, AI cloud engine, and behavior detection.

Remote desktop management

NISE uses a cloud-based management platform to remotely connect to endpoints, detect threats, block and delete viruses, and conduct investigations.
In addition, file copy operations are prohibited during remote desktop connection, preventing the spread of threats to non-infected endpoints.

IT asset management and vulnerability diagnosis

NISE can list all connected PCs and installed software and assess security vulnerabilities in real time.
If a vulnerability is detected, an alert will be sent to the administrator and an update will be ready.
In addition, you can manage them efficiently and comprehensively by visualizing internal IT assets.

UTM correlation

NISE can be correlated with Neusoft UTM - NISG.
Synchronize endpoint information to UTM so that communication can be automatically blocked if a threat is detected.
Communication will also be automatically cut off if an unmanaged PC without an NISE agent installed is connected to the internal network.

NISE ››› Features

[Main Features] NISE

- Real-time protection
- Malware protection
- Anti-phishing
- Anti-ransomware
- Remote VPN access
- Asset management
- Security settings
- Device discovery
- UTM correlation
- Alerts/logs/reports

[Security defense methods] NISE

Auto control of PC access via UTM correlation

Correlating NISE with Neusoft UTM NISG makes the security defense more advanced. The correlation can be easily configured on the NISE management platform and UTM management webUI. Through the correlation, access of unmanaged PCs to the network will be automatically blocked.
In addition, access control can be configured per user according to the security policies.

Configure on NISE Management Platform

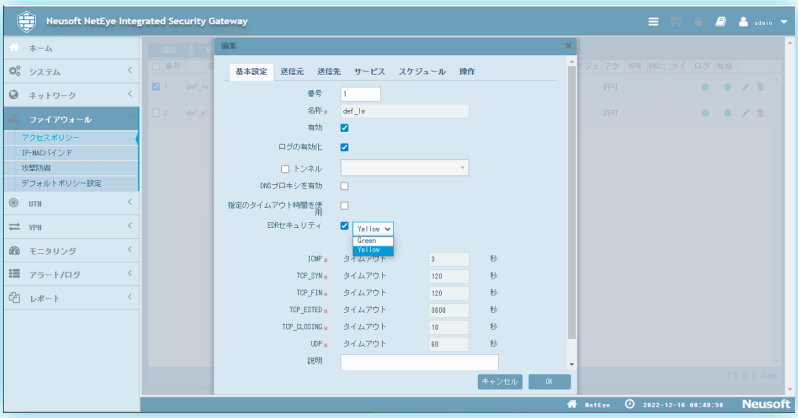
Register the NISG and the key information to the NISE management platform.

Configure the UTM

Register the NISE management platform and the key information to NISG.

Set access control matching security policy

You can set the access control on NISG according to the security policy.

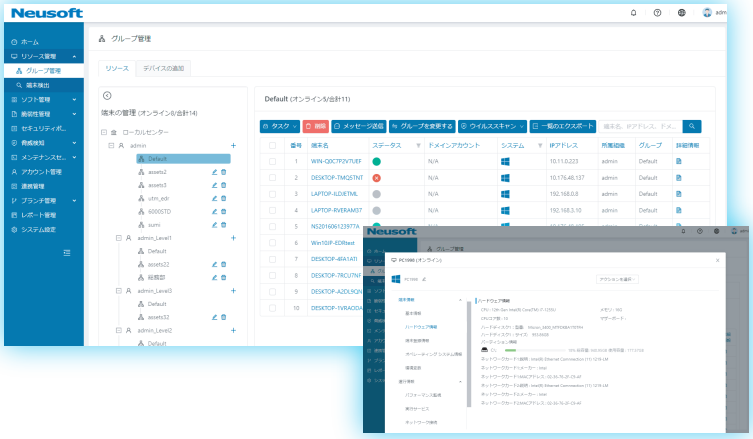


Reduce the workload of IT asset management

You can check the status of PCs and NISE agents installed on these PCs. In addition, remote vulnerability scanning can be easily done on Windows hosts.

Check the utilization of managed PCs

Monitor the utilization of managed PCs with NISE agents installed.
Manage IT assets by checking PC hardware resource information, Windows OS update management, etc.
Find abnormal high load conditions and network connections caused by malicious software.
If an abnormality is confirmed, the endpoint can be shut down or restarted immediately to prevent the threat from spreading.

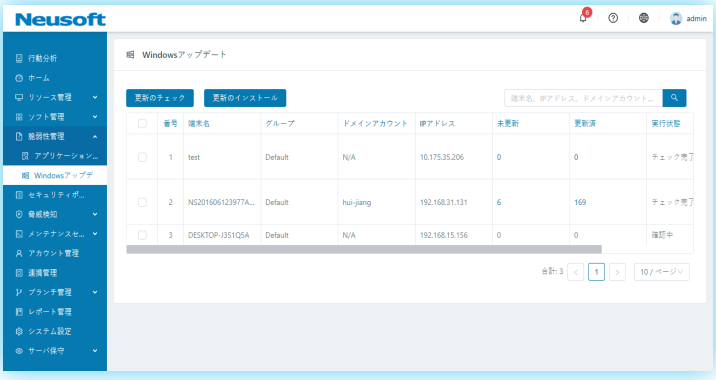


Monitor the software running on PCs

Indentify and monitor the software installed on managed PCs with NISE agents installed.
Unauthorized installation of unauthorized software can be quickly confirmed and dealt with.
You can also control and manage the installation of software by registering software in blacklists and whitelists.

Windows vulnerability management

You can extract and manage the vulnerability information of Windows OS, and check the update status.
Vulnerability updates can be performed remotely if desired.



Prevent threats with a high performance engine

Multiple engines are used to detect various threats more quickly and accurately, including a lightweight signature-based detection engine, a behavior detection engine and a brute force attack detection engine. You can set detection settings in security policies according to your business needs.

Set asset management policies

You can set asset management policies for your company. End users can register and change asset information which will be transferred to the NISE management platform, reducing the burden on administrators. NISE can also prevent users from terminating or uninstalling the NISE agent. It can prevent the NISE agent from stopping due to user's erroneous operations, so as to keep endpoints in a safe state at all times, even for external PCs.

Set security policies

You can set policies for malware detection and brute force attacks detection according to your environment. In addition to the real-time protection of the anti-malware engine, scheduled scanning automatically executes scan tasks reducing the user effort. The real-time brute force attack defense prevent the spread of threats by automatically blocking network communications for a certain period of time upon detection.

External device access control

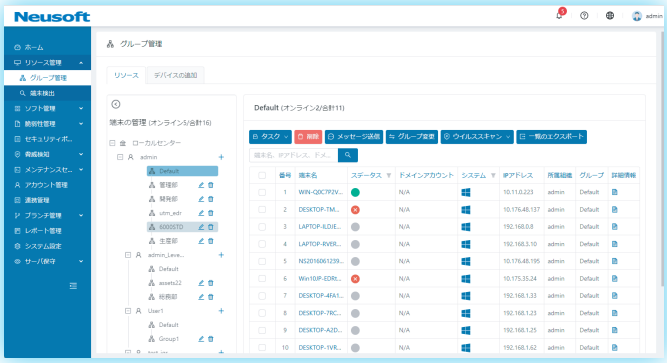
You can prevent threat intrusions and information disclosures by controlling endpoint connected devices, such as USB devices and printers.
You can set it according to your business needs.

Reduce the burden by remote operations

You can perform various operations remotely via the management platform. It can scan files, block network access, restore quarantined files, etc. Further investigation can also be performed via remote desktop.

Remote operations

You can perform various tasks remotely using the management platform on the cloud. You can finish daily maintenance without going to the site, such as restarting and shutting down terminals, virus scans, and remote desktops.

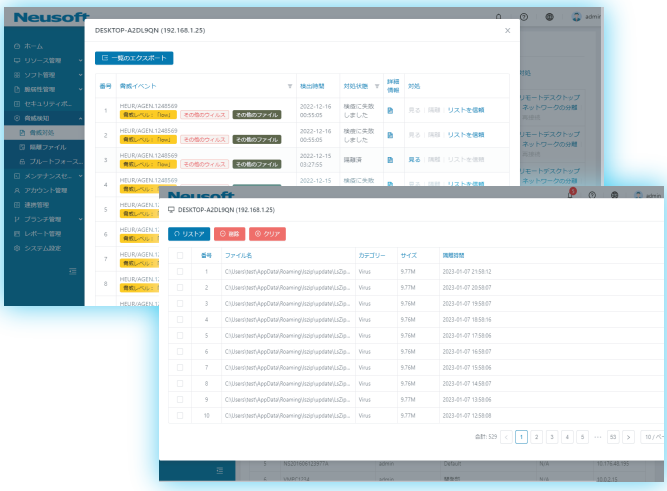


Block network access remotely

If a threat is detected on a terminal, you can quickly and remotely disconnect it from the internal network, blocking the unauthorized access and preventing the spread of threats. Even when disconnected, you can still access the terminal via remote desktop and investigate the event via the unified management platform.

Unquarantine files in case of false positives

If you accidentally quarantine a good file, you can remotely unquarantine it or add it to the whitelist.



NISE ››› Scenario

Cloud management platform
+
Lightweight agent

Centralized management
of endpoints
in various environments

Internal PC

Public cloud

Private cloud

Hybrid cloud

Internal Server

Physical PC, Server, and IPC

Cloud desktop

Protect your office network and data center resources
with a unified management platform.

Endpoint protection	Malware and ransomware countermeasures, unauthorized intrusion prevention, unauthorized RDP access control Automatic quarantine and removal of malicious software, windows vulnerability update USB/Bluetooth device discovery and control
Endpoint management	Collection of endpoint information on: 1) hardware and installed applications 2) resource (CPU, memory, storage) utilization 3) performance, running services, and network connections 4) startups and scheduled tasks
Endpoint operations	Reboot, shutdown, network communication interruption, remote desktop connection Virus scan, software quarantine, software uninstall
Supported OS/ Required resources	NISE agent Microsoft Windows 11/10/8.1/8/7 Windows Server 2019/2016/2012/2008 Memory capacity: 4GB or more Disk space: 128GB or more

Neusoft

Neusoft Corporation (Headquarters)
No.2 Xin Xiu Street, Hun Nan New District,
Shenyang, Liaoning, PRC
Zip Code: 110179
Email: securitybz@neusoft.com
Website: www.neusoft.com