

Secuguard UVM

Unified Vulnerability Management

As the internet users are increased and network grows rapidly, hacking/security incidents are rapidly increasing every day. To protect the system from these various external environments, administrators need to run periodic vulnerability assessment scans and update system continuously. However this job requires special knowledge domain and dedicated work hours for administrators to invest newly coming hacking methods and technologies.

Secuguard UVM(Unified Vulnerability Management system) shares vulnerability assessment result to vulnerabilities assessment tools(host scanner, network scanner, web scanner, pc scanner, etc) and builds an organized vulnerability assessment management system.



UVM Features



User-friendly User Interface

Intuitive and localized Window Explorer-like user interface



Organized Asset Management

Structured management of the organization's systems, network equipment and PCs



Secure User Management

Various user privilege management(super admin, group admin, machine admin, user)



Cooperation with Vulnerability Assessment Tools

Operating with SSE, NSE, and WSE or mySSE various vendors' vulnerability assessment tools available



Centralizing Security Vulnerability Management

Centralized security vulnerability management for scan, remedy and result



Vulnerability Knowledge Base/Center

Providing technical support, security alert, update information, technical document, vulnerability remediation procedure, vulnerability information, etc.



Efficient and Convenient User Management

Single group(single group member) and virtual group(multiple group member) provided



Remote Vulnerability Assessment Tool Console

Predefined vulnerability assessment recipes on remote console's web GUI and remote console



PC's vulnerability assessment with mySSE(Optional)

Testing Individual PC's vulnerability over UVM, review the result and remedy



Various Management Resources

Searchable various statistical information with conditional operations such as Top 10 vulnerability topic by period



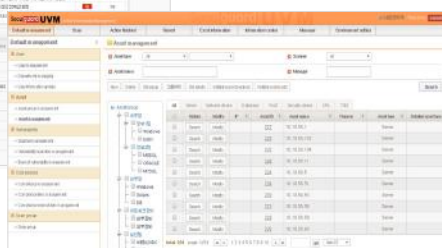
Workflow Management

Vulnerability workflow management from scan request, scan, scan result to remedy and record history

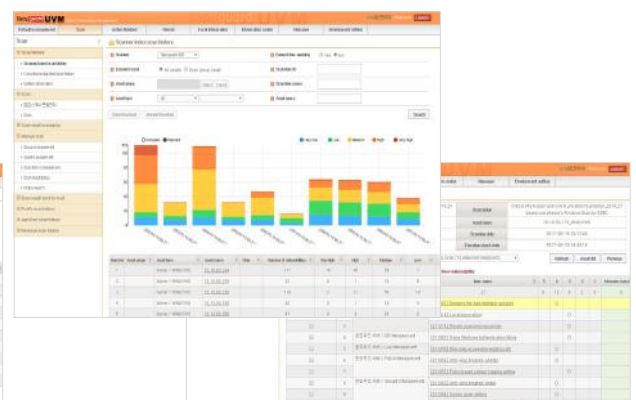
UVM Screen Shots



▲ Main

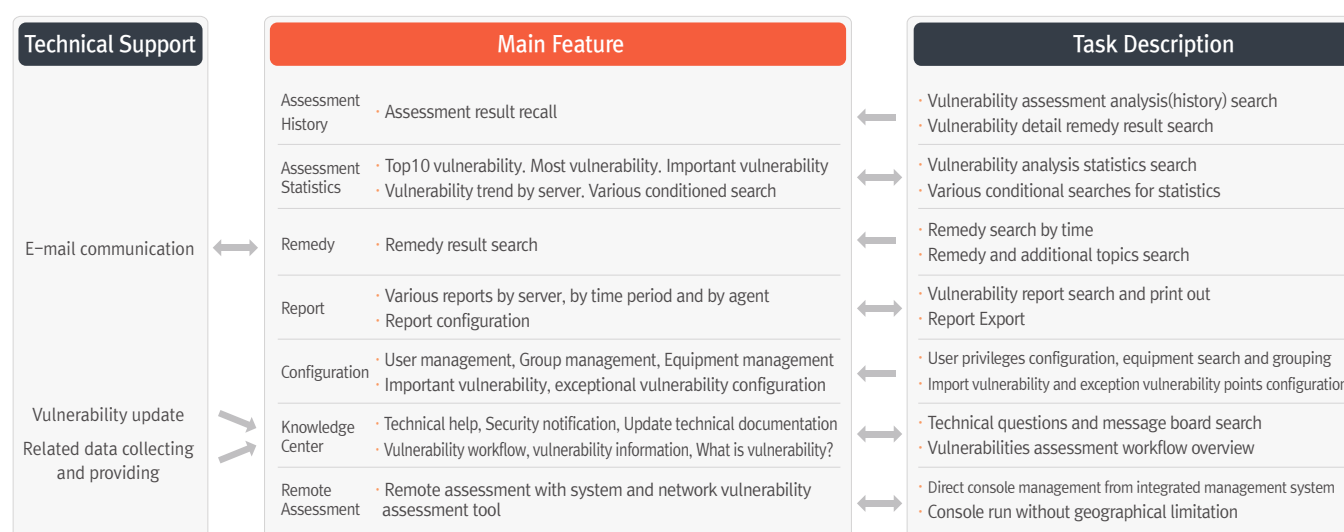
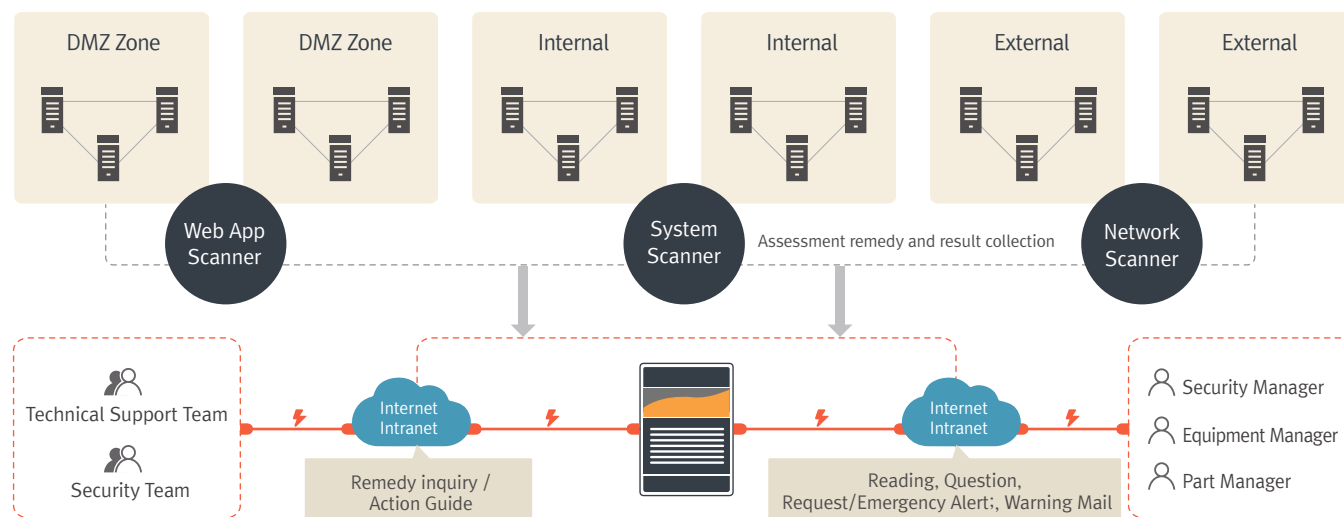


▲ Equipment management



▲ Fullfillment measure lookup

UVM Architecture



UVM Features Table

Features	Description	Features	Description
Vulnerability Assessment	<ul style="list-style-type: none"> Operating with SSE, NSE, and WSE or mySSE. Also operation can be run with other vendor's vulnerability assessment tools 	Exceptional Vulnerability Management	<ul style="list-style-type: none"> Can applied to confrontational action, assessment statistics and report
Configuration	<ul style="list-style-type: none"> User management, group management, equipment management, console management, user information update, password reset, SMTP configuration, report logo, vulnerability DB update 	Remote Assessment Console	<ul style="list-style-type: none"> Remote run for SSE, NSE, WSE Integration with other vendor's vulnerability assessment tools
Assessment History	<ul style="list-style-type: none"> Various information search available: assessment equipment, assessment history, priority by vulnerability, agent IP, operation system, assessment administrator, total assessment item number, priority, latest assessment date, vulnerability list, vulnerability description 	Vulnerability Analysis	<ul style="list-style-type: none"> Whole system, group based, operation system based, equipment based assessment statistics and analysis (vulnerability item number changes, priority changes, item number by priority changes, target equipment state, vulnerability state, vulnerability by priority state and number of assessment)
Remedy	<ul style="list-style-type: none"> Lifecycle management: system scan, scan result analysis, remedy, remedy check, record history Whole system, group based, equipment based, and time period based remedy and remedy check 	Vulnerability Information Center	<ul style="list-style-type: none"> Security bulletins, security notification, confrontational action questionnaires, FAQ, update, technology documentation shares, message board, vulnerability workflow, vulnerability information
Email, Update and Online Help	<ul style="list-style-type: none"> Email scan result to corresponding manager Product update, vulnerability DB update Detailed online help for the all features 	Vulnerability Report	<ul style="list-style-type: none"> Assessment summary, priority report, vulnerability list by equipment, vulnerability list by equipment level, vulnerability list by check item, action list by check list, periodic statistic report, vulnerability distribution statistics report, Itemized vulnerability report by equipment, vulnerability description by priority, detailed report by prioritized vulnerability, detailed report by itemized vulnerability, Etc