umv

WARSS

Website **A**ttack **R**estoration **S**ecurity **S**olution

Real-time website security

Contents

umv

UMV Inc.

Founded in 2008

Seoul, South Korea

Web-Focused Solutions

Real-time web server security

Prevent

Stolen data, interrupted web services, website defacement, persistent attacks

Motto

“The security chain is only as strong as its weakest link”

Why WARSS?

https://www.youtube.com/watch?v=6gY1NWw9CJA&t=12s

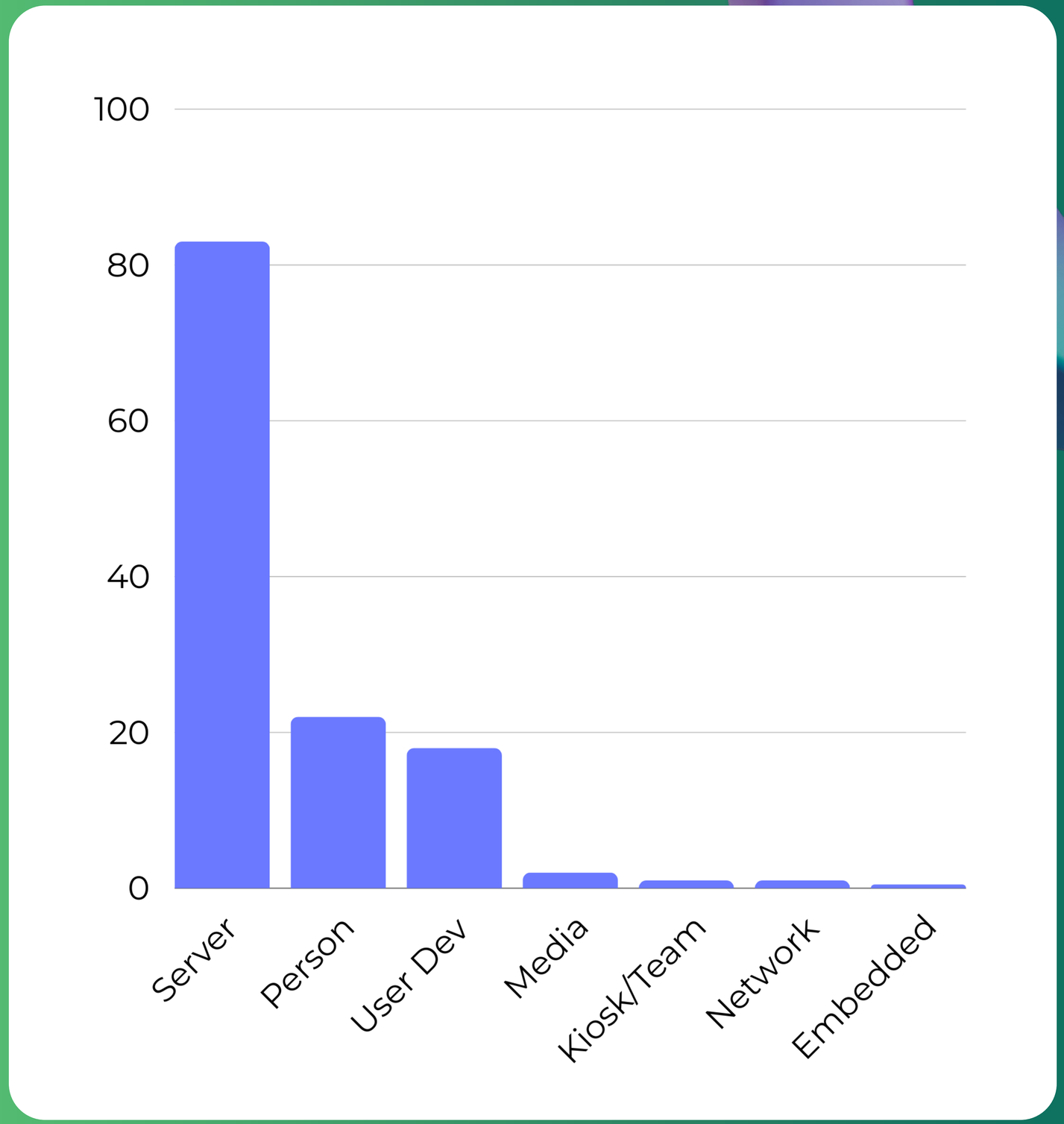
Web Hacking on the Rise

Verizon analyzed a record-high **TWO-FOLD** increase in the number of verified **security breaches** between 2022-2023

2024 Verizon Data Breach Investigations Report

Assets affected in breaches

2023 Verizon DBIR



Ukrainian & Russian Websites Defaced

Fake News

Feb. 2024-Present: Russo-Ukrainian War accompanied by continuous cyber attacks on one another and allies

Misinformation & Data Harvesting

Targets include SMBs, media outlets, government institutions, OT, and other entities possessing personal/sensitive information

Distrust: The Key to Cyberwarfare

Publicizing hacking attacks breeds fear, distrust of authorities, and misinformation amongst civilians

Image Source: The Record

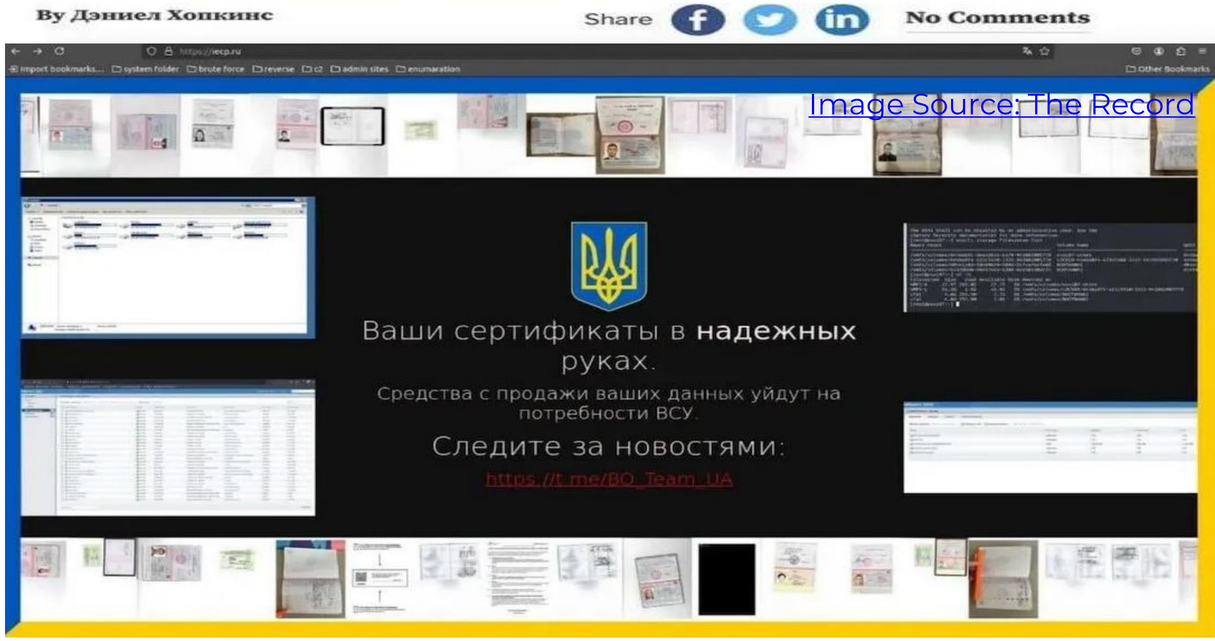


Image Source: The Record

- https://therecord.media/ukrainian-news-outlets-attacked-by-russian-hackers
- https://therecord.media/russia-osnavanie-digital-signatures-cyberattack-ukraine

Internet Archive Attacks

Round 1: DDoS, Defacement, Data Theft

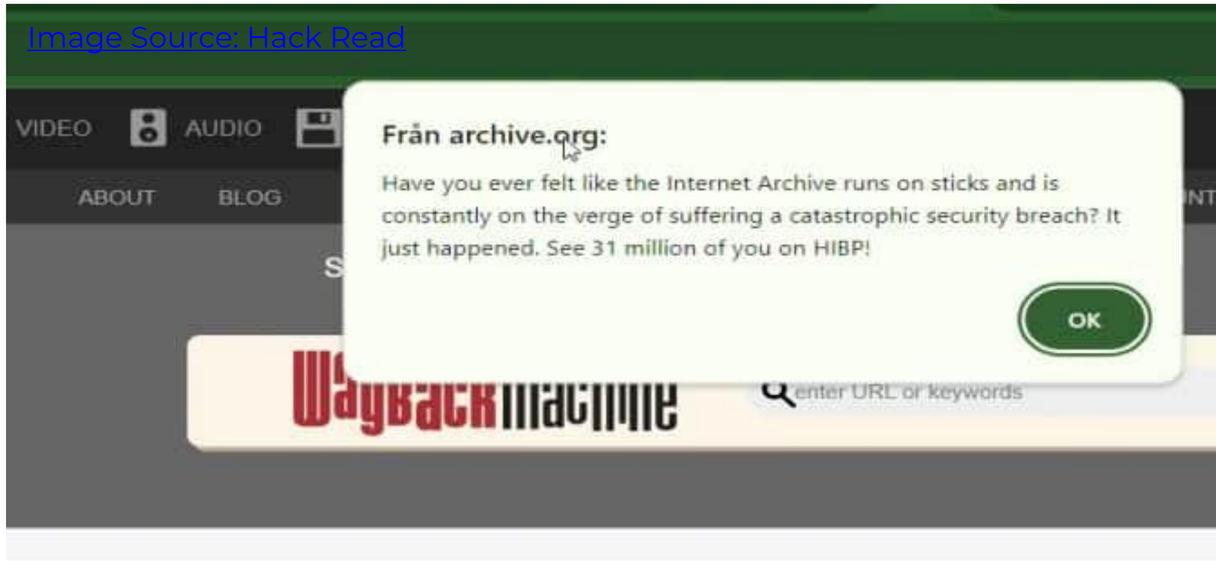
Oct 9, 2024: DDoS attack takes down site; website **defaced with JavaScript** alert; usernames, emails, etc. for **31 million user** accounts leaked

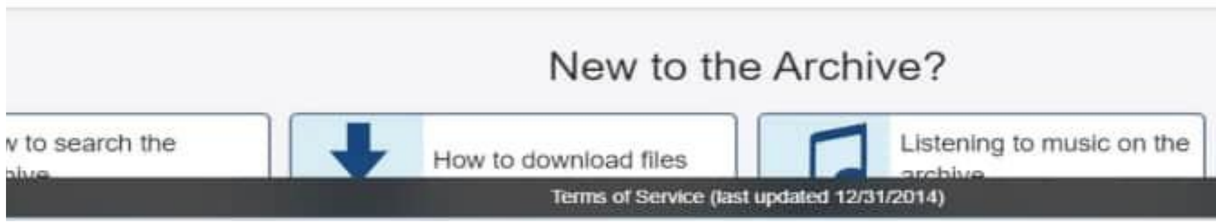
Back to Normal

Oct 18, 2024: IA confirms that data is safe and services restored

Round 2: Unsecured Digital Keys

Oct 20, 2024: Exploit unrotated access tokens to gain access to Internet Archive's Zendesk support platform; accessed **800K+ support tickets** going back to **2018**





- https://www.cbc.ca/radio/asithappens/internet-archive-hack-1.7359959
- https://therecord.media/internet-archive-data-breach-ddos-defacement
- https://hackread.com/internet-archive-archive-org-hacked-accounts-compromised/

Trend: Hacktivism and Cyber Terrorism

- Hacking to promote **political** or **religious** beliefs
- Increased availability of **encrypted communication platforms** (i.e. Telegram, Rocket Chat, Discord, etc.) and **cryptocurrency**
  - **TRON** accounted for **~90% of funds** associated with **terrorist financing** since 2021 (INTERPOL New Technologies Forum, October 2023, Merkle Science)
- **Cybercrime-as-a-service** (DDoS, ransomware, credentials, data, etc.)

- *Beneath the Surface Report* (June, 2024)
UN Counter-Terrorism Centre (UNCCT)

Image Source: Malcontent News

Image Source: POLITICO

- https://unicri.it/sites/default/files/2024-06/DW.pdf

The Problem

Defacement Methods

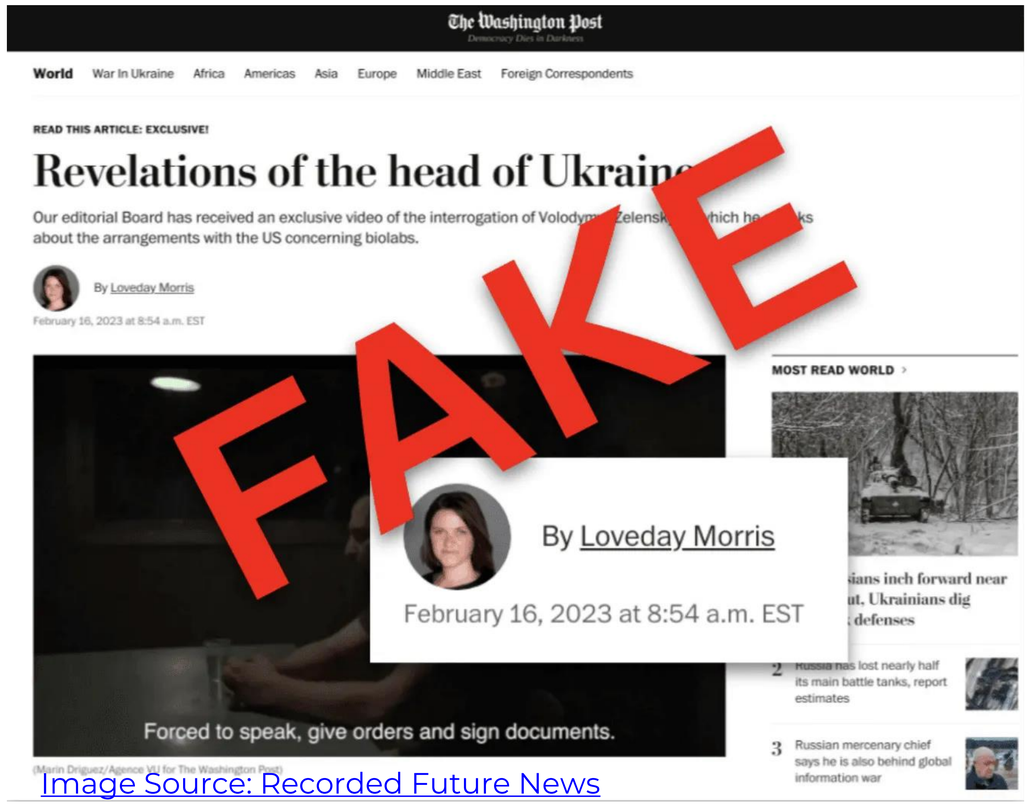
1. **Source Code Modification**

Image Source: alphavilleherald.com

Image Source: boannews.com

Defacement Methods

2. Content Spoofing/Injection



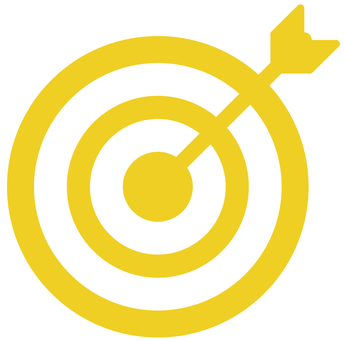
[Image Source: Recorded Future News]

[Image Source: National Post]

Why Defacement?

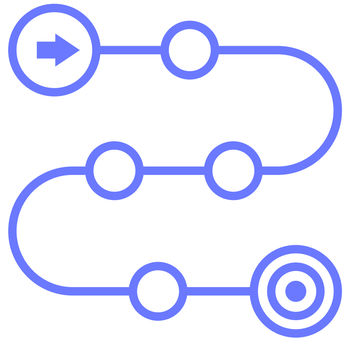
Motivation

- hacktivism
- embarrassment
- fame/recognition
- cyber terrorism



Target

- government institutions
- healthcare
- large companies
- targets of convenience

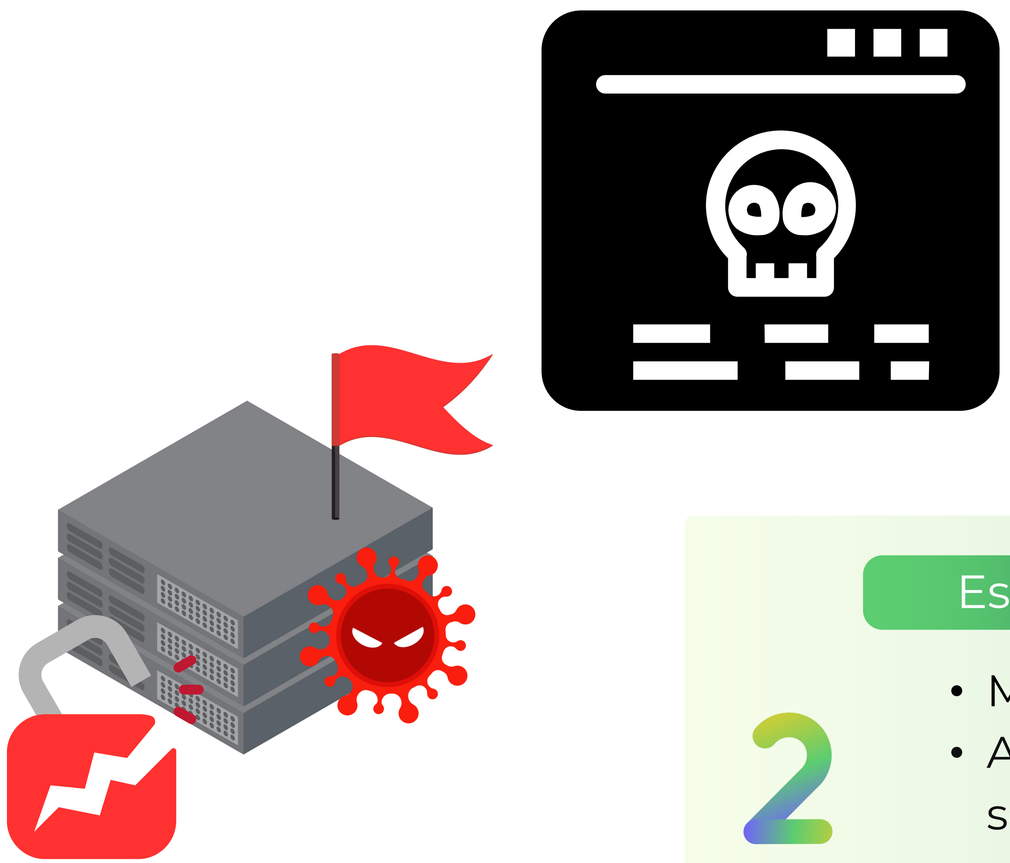


Method

Exploit weaknesses in web-based components:

- web server
- web applications
- websites

The Anatomy of a Web Attack



3

Impact

- Defacement
- Source code and content forgery

2

Escalation

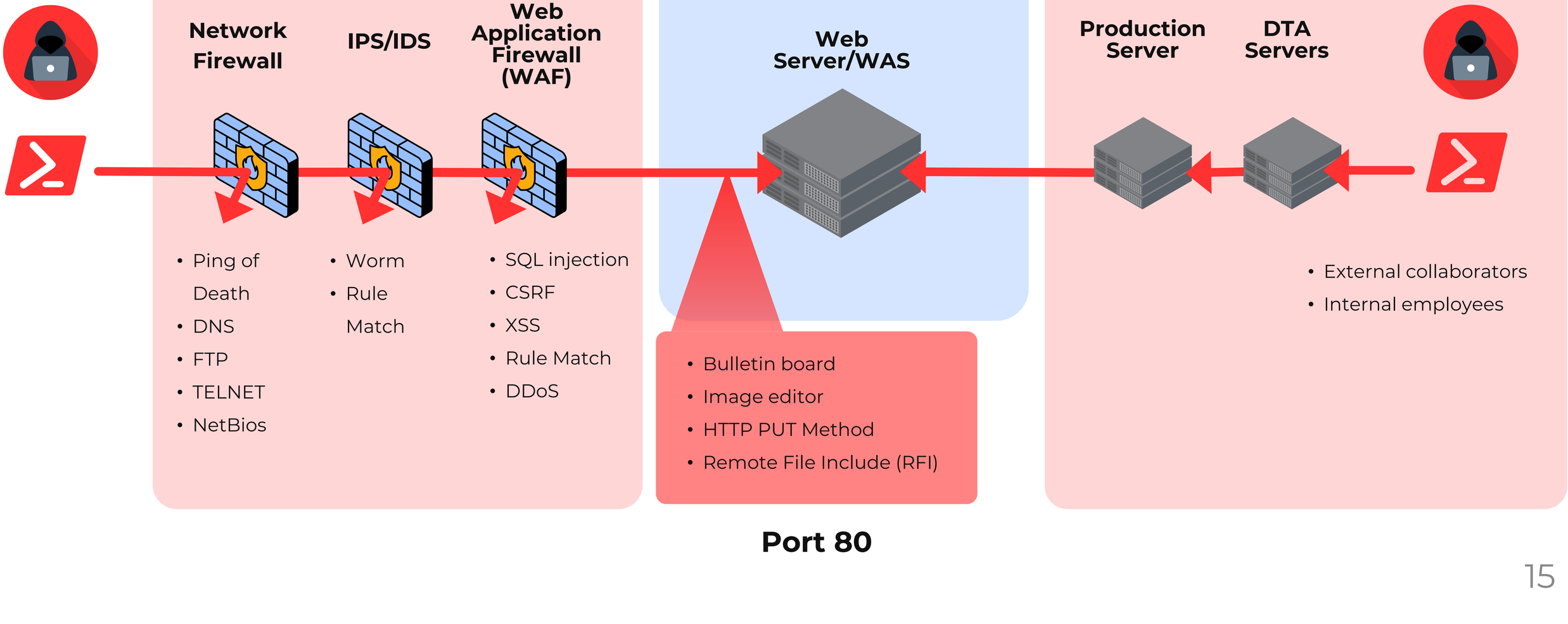
- Malware uploaded on web server to establish presence
- Additional malware (payload) executed to change web server files

1

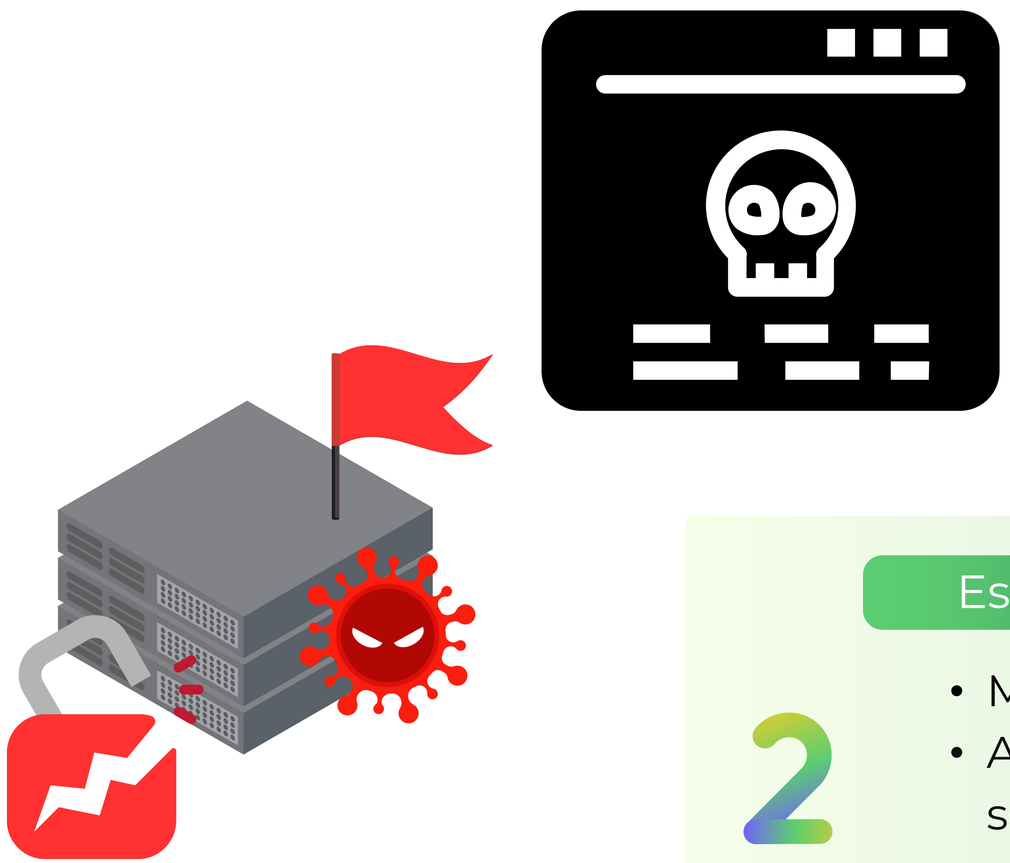
Infiltration

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing

The Status Quo



The Anatomy of a Web Attack



3

Impact

- Defacement
- Source code and content forgery

2

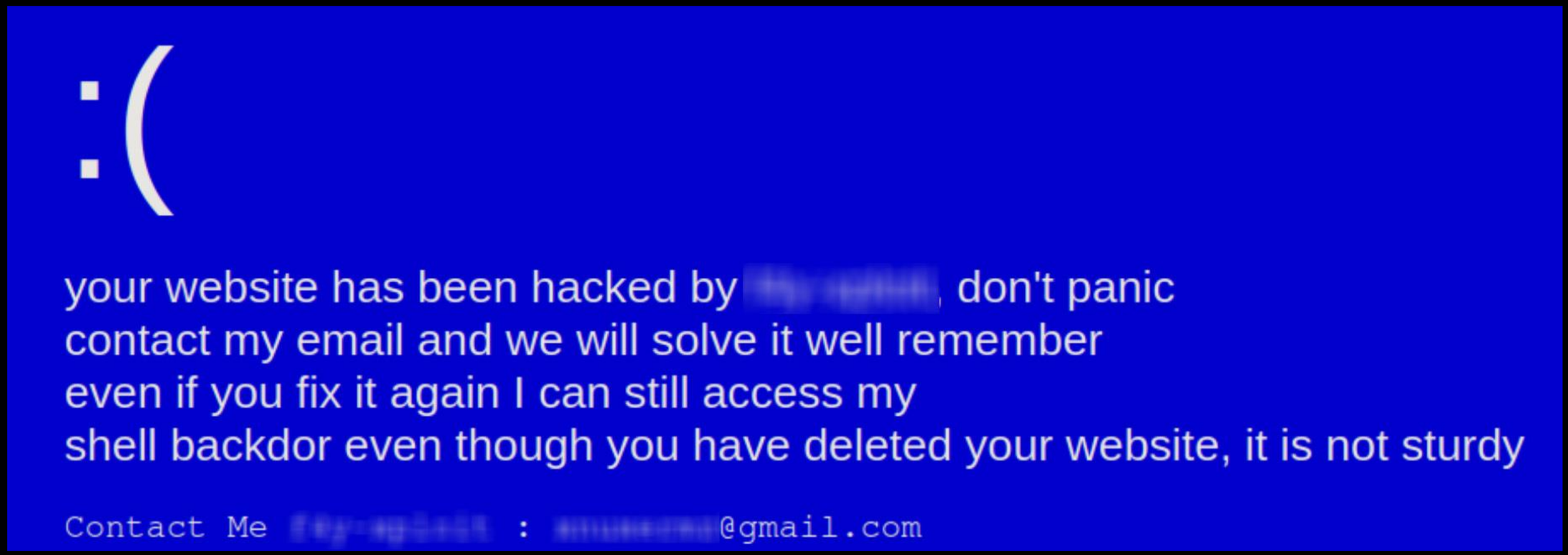
Escalation

- Malware uploaded on web server to **establish presence**
- Additional malware (payload) executed to change web server configuration files

1

Infiltration

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing



https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg

The Key:
Real-time Detection & Response

All attacks start with one of three **changes**:

1
File Addition

2
File Modification

3
File Removal

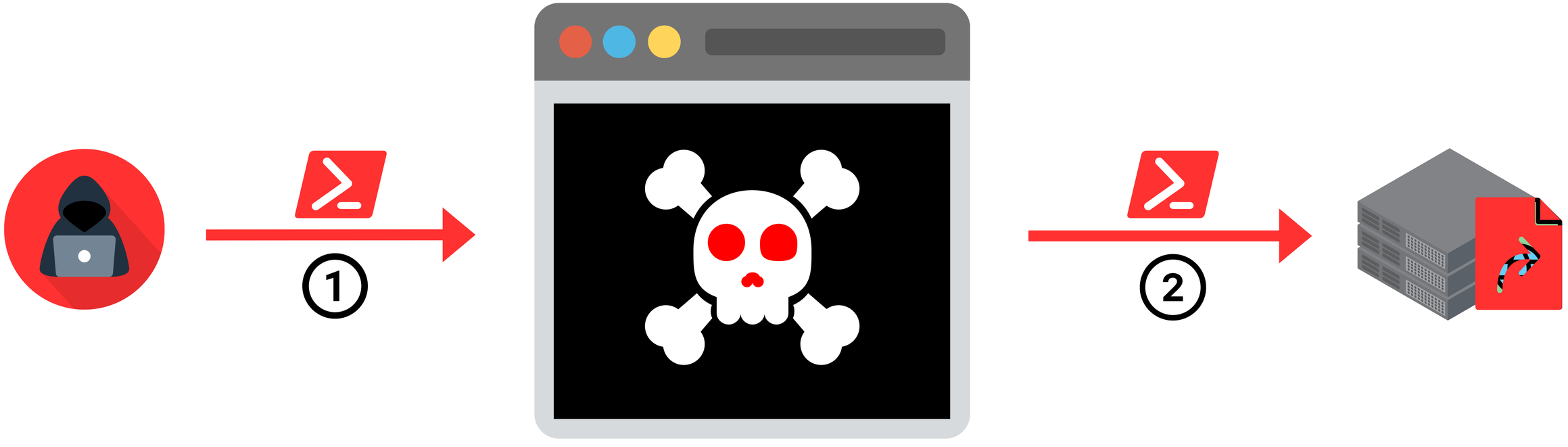
Website **A**ttack **R**estoration & **S**ecurity **S**olution **(WARSS)**

Web server security booster solution that **detects** unauthorized changes to a website and **restores** the original files in **real-time**

How Does Website Defacement Happen?

vulnerable website

web server

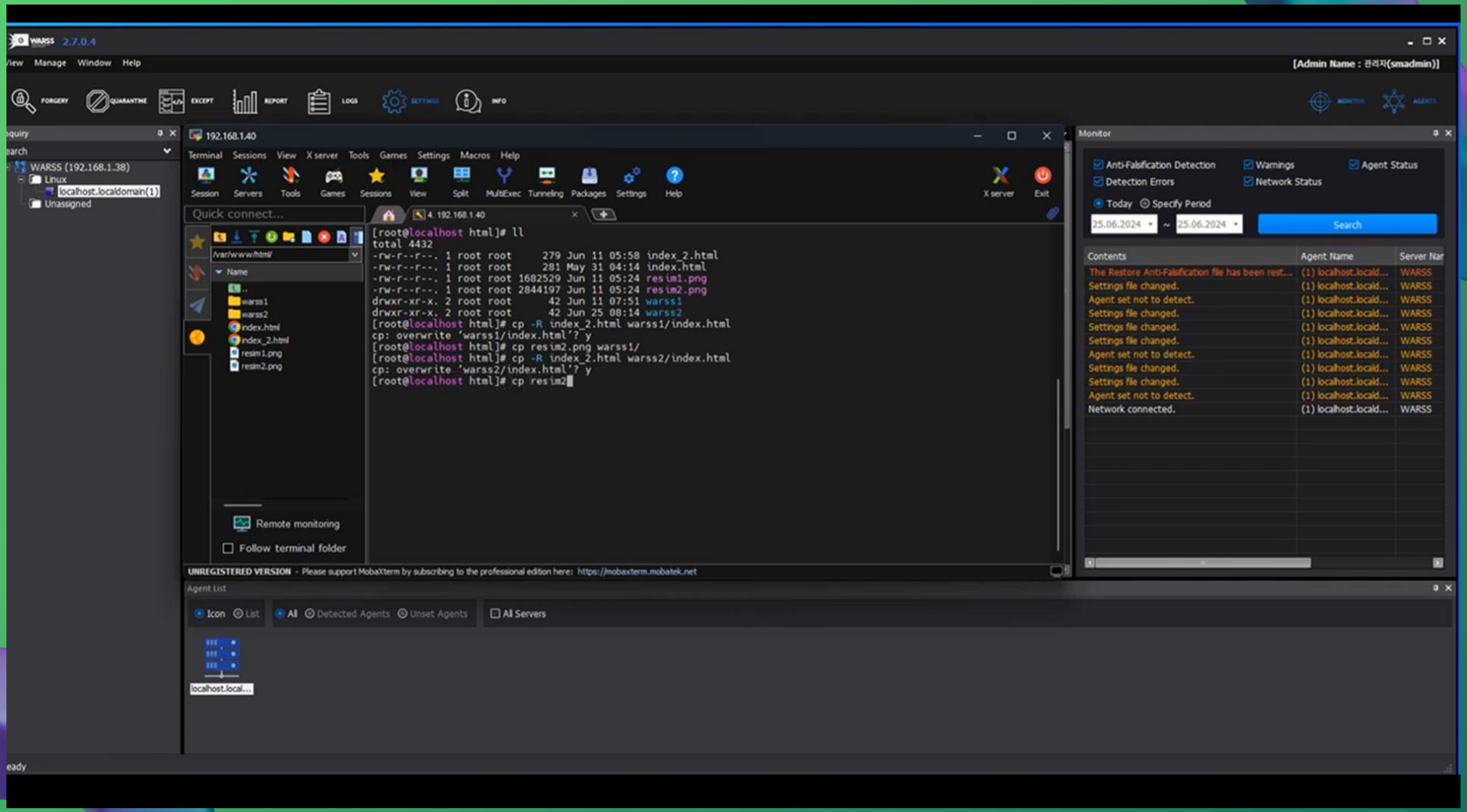


How Does WARSS Work?

vulnerable website

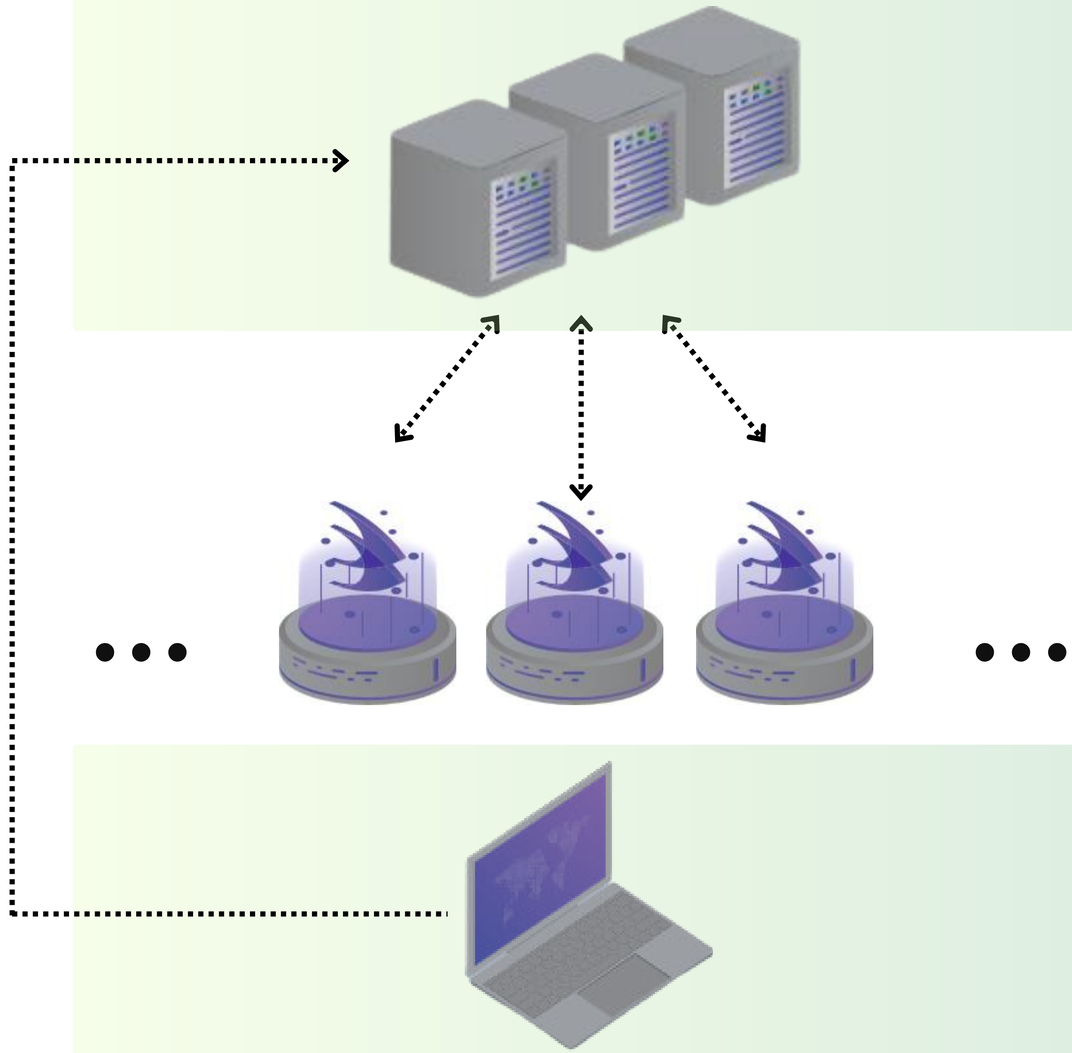
web server

Demo



https://www.youtube.com/watch?v=B20LDk0iAJQ

WARSS Configuration



WARSS Management Server(s)

- Server software installed on HW/VM
- Remotely manages and controls Agents
- Saves detection history
- Distributes updates and settings changes to Agents

WARSS Agent(s)

- Program installed on web server/WAS
- Detects file modifications
- Compatible with Unix, Linux, Windows NT O/S (must support JDK 1.5+)

WARSS Manager Program

- Program installed on administrator PC
- Controls settings for: detection, remote action, environment, and reporting
- Access management, statistics & reporting settings

How WARSS is Different

	WARSS	Web Crawlers
		
Detection Method:	**Real-time,** pattern-based	**Periodic** detection
Load:	**Optimized** resource usage **(~1% CPU)**	**Agentless**
Detection Target:	**Server files** (source code, data, contents)	**Compiled URL units** and **data files**
Mitigation:	**Real-time, automatic** restoration	**Manual mitigation** upon breach

Real-time
detection

Protect
source code
and contents

Lightweight

Immediate
restoration & recovery

ZERO TRUST

1. “Never trust, always verify”

2. Least-privilege access

3. Assume breach

ZERO TRUST

3. Assume breach

Real-time detection

Streamlined management

Rapid mitigation

Real-time file change monitoring

Real-time alerts and reports

Automated restoration & recovery

Availability

information is accessible when needed

ISO/IEC 27001 Principles

Confidentiality

information only accessible to authorized parties

Integrity

information is accurate and protected from corruption

ISO/IEC 27001 Compliance

Applicable Requirements:

8.1 Operational planning and control

8.3 Information security risk treatment

9.1 Monitoring, measurement, analysis and evaluation

ISO/IEC 27001 Compliance

Applicable Annex A Technological Controls:

- **8.4** Access to source code
- **8.6** Capacity management
- **8.7** Protection against malware
- **8.8** Management of technical vulnerabilities
- **8.12** Data leakage prevention
- **8.13** Information backup
- **8.15** Logging
- **8.16** Monitoring activities
- **8.23** Web filtering
- **8.26** Application security requirements

GS (Good Software) Level 1 Certified

- **Test Standards:**

  ISO/IEC 25023, 25051, 2504

- **Tested for:**
  - Functional suitability
  - Performance efficiency
  - Compatibility
  - Usability
  - Reliability
  - Security
  - Maintenance
  - Portability

Use Cases

Government Defense Institution

Security Shortfalls

Dissatisfied with “W” web-based forgery detection software’s performance and ease of management

Their Checklist

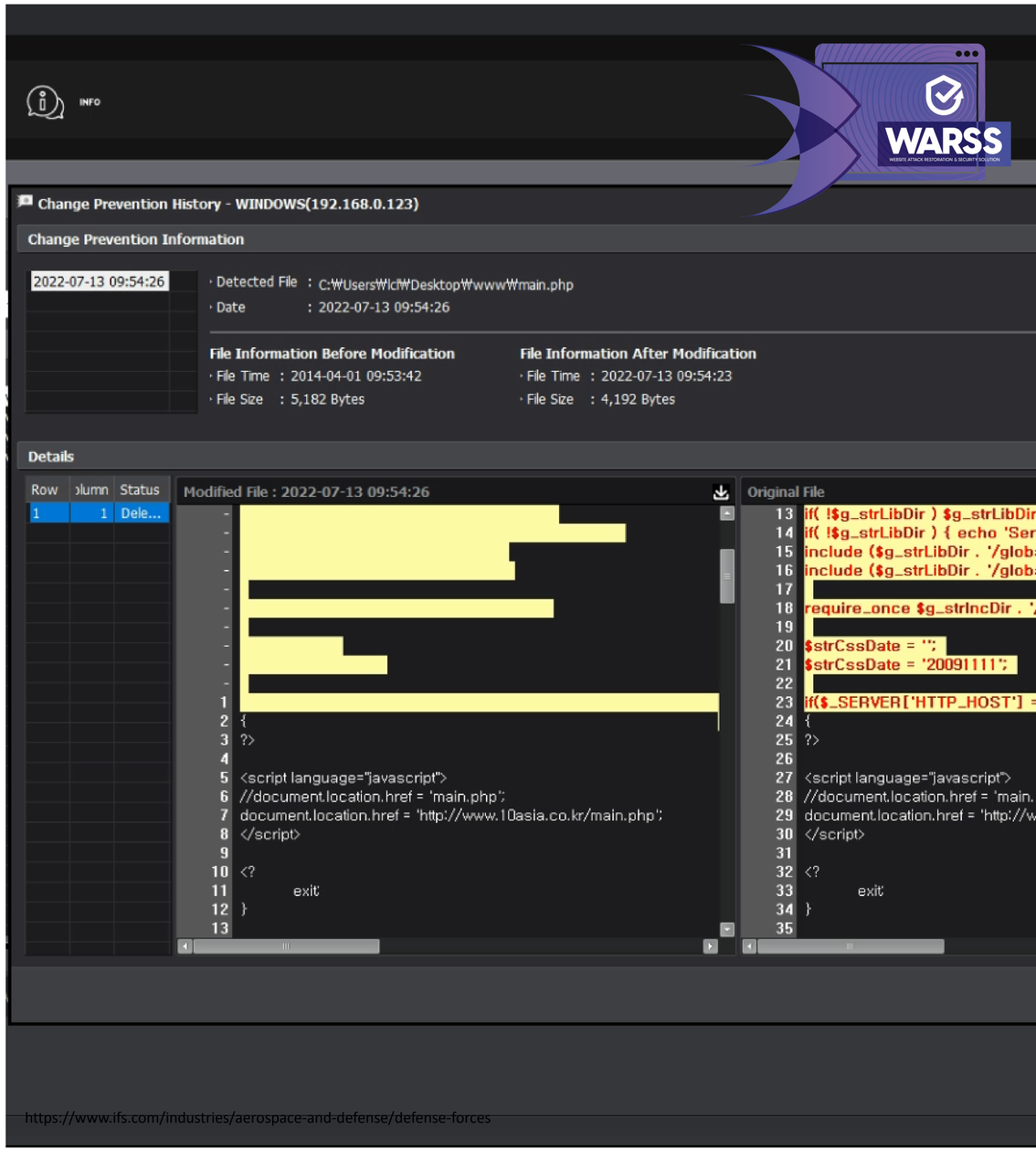
Were specifically looking for an Agent-based solution that offered automatic restoration and efficient management

2023 WARSS Implementation

Installed 50 WARSS Agents on all web servers

Their Feedback

Delighted with WARSS’s automatic home directory detection feature, allowing for easy detection configuration without manually inputting URLs



https://www.ifs.com/industries/aerospace-and-defense/defense-forces

Transportation Agency

Content Forgery Concerns

Operating website with educational content (images, videos); tried and failed to outsource development of proprietary anti-forgery solution

Why WARSS?

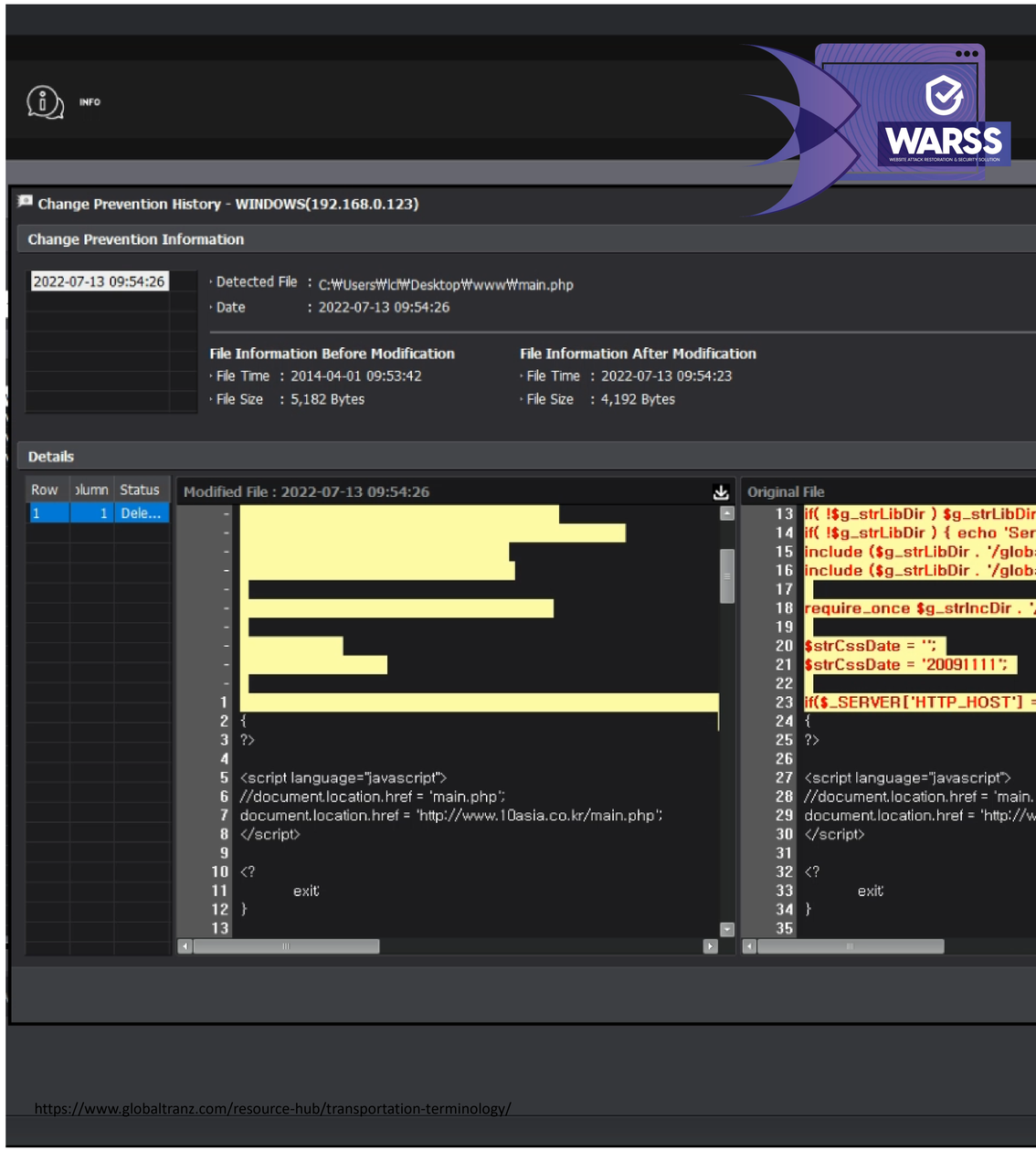
Compared to all other anti-forgery solutions they tested, WARSS was the only one that offered source code, image, and video forgery protection

Why They Chose WARSS

Installed 100 WARSS Agents on all web servers

Continuous Protection

WARSS has prevented any forgery incidents since; customer continues to purchase Agents each time they add servers to their system



Who Uses WARSS?

WARSS protects the reputations of several national companies and institutions.

대 한 민 국
청 와 대

대한민국육군
Republic of Korea Army

한국지역난방공사
KOREA DISTRICT HEATING CORP.

국 방 과 학 연 구 소
Agency for Defense Development

ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute

서울특별시
SEOUL METROPOLITAN GOVERNMENT

영남대학교
Yeungnam University

LS ELECTRIC

한전원자력연료
KEPCO NUCLEAR FUEL

... and more!

Hundreds of Customers

UMV products has been providing safe and stable protection for hundreds of customers' web servers for over a decade.

SAMSUNG

13+ years

amazon web services

13+

ebay

7-8

Hanwha

13+

NongHyup Bank

10+

Prudential

13+

TOYOTA

STARBUCKS

dun & bradstreet

SUPREME COURT OF KOREA

Seoul Metro

S-OIL Corporation

Ministry of National Defense
Republic of Korea

OFFICE OF THE PRESIDENT
THE REPUBLIC OF KOREA

HYUNDAI

Deloitte.

iMBC

... and many more!

Thank you

Contact Us

UMV, Inc.

Seoul, South Korea

+82 2 448-3435

sales@umvglobal.com

www.umvglobal.com

Appendix

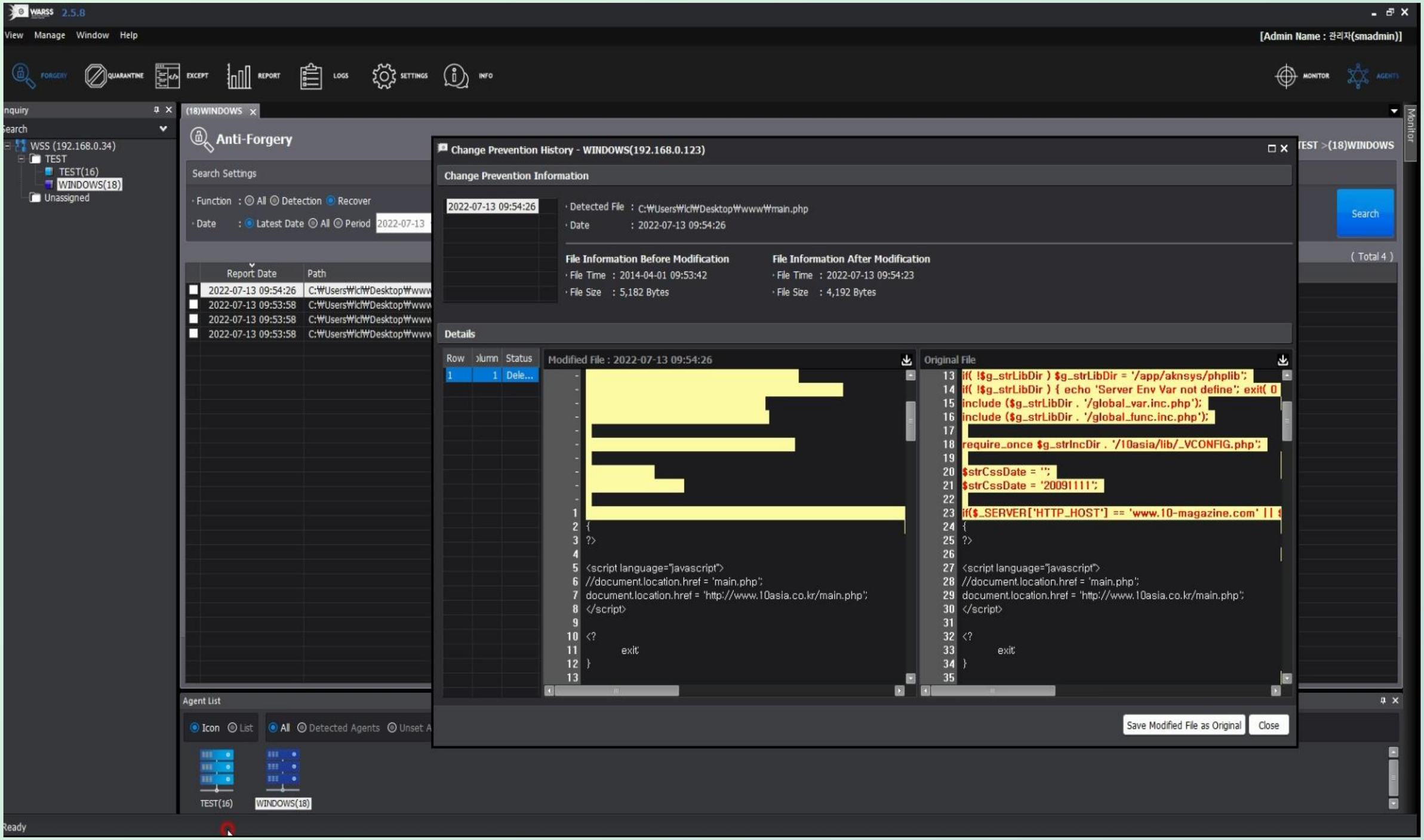
WARSS Functions

Forgery Detection and Restoration

Function Name	Description
Forgery Detection	Detection and notification of forgery and alteration of website source files and data
Forgery Restoration	Real-time restoration of original files when forgery is detected
Re-Assign Original	Re-assign baseline/original files when legitimate changes must be made

Forgery Detection View

Forgery Detection and Real-Time Restoration



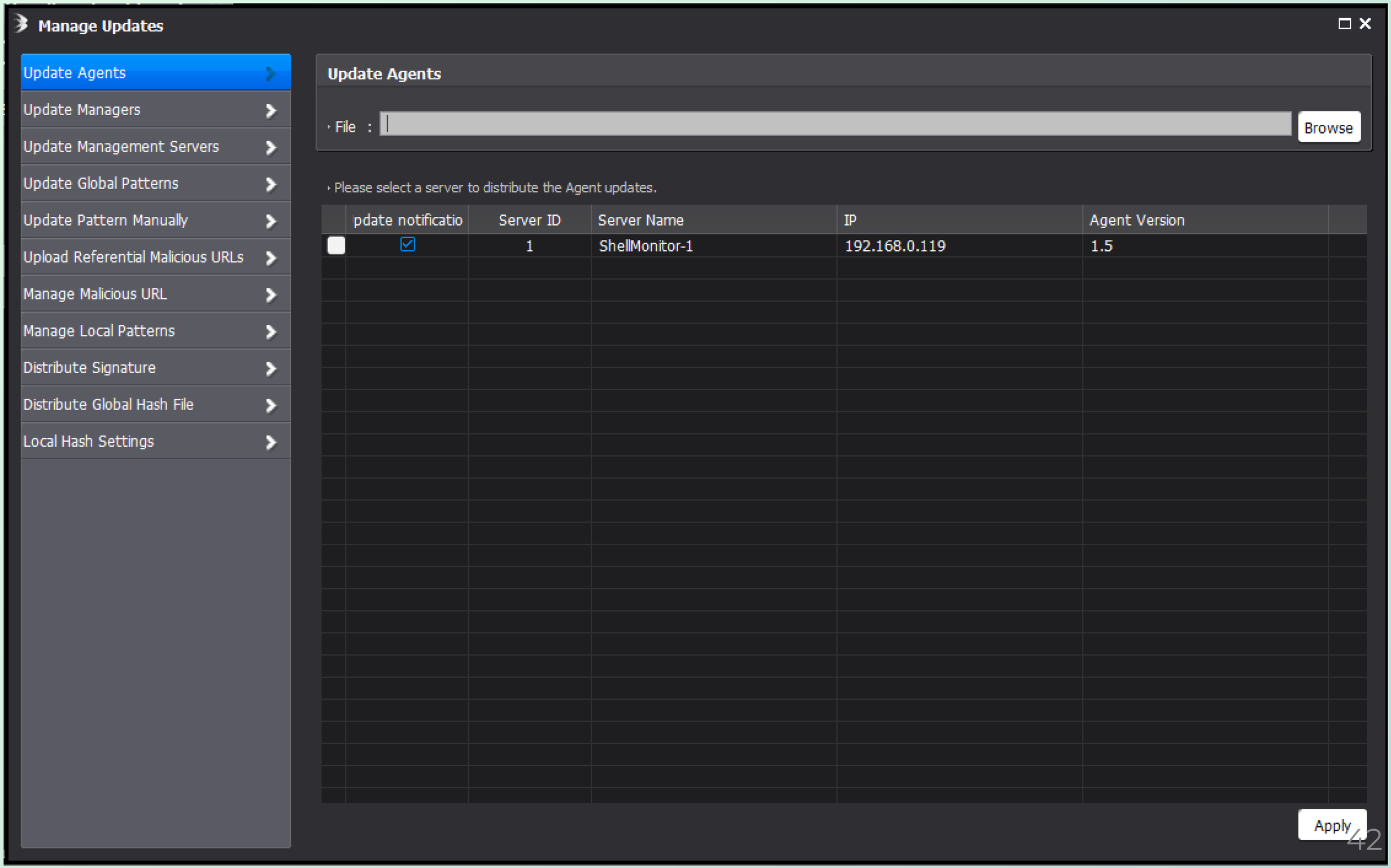
WARSS Functions

Management Features

Function Name	Description
Update Management	Agent & Manager updates, version management
Permissions and Reporting Management	• Permissions management by account and user • Interfacing with external systems (ESM, SMS, E-mail, etc.) • Reports and statistics
Stability	• Resources usage control • Customizations to suit server environment
Attacker IP Detection	Execution IP reports for forgery files (available when only detection function is activiated)
Preferences Management	Web/WAS configuration file management and change detection settings
Dedicated Safe Uploader	• Specify safe upload target directory for each user account • Check for presence of malicious code in files uploaded using Safe Uploader too

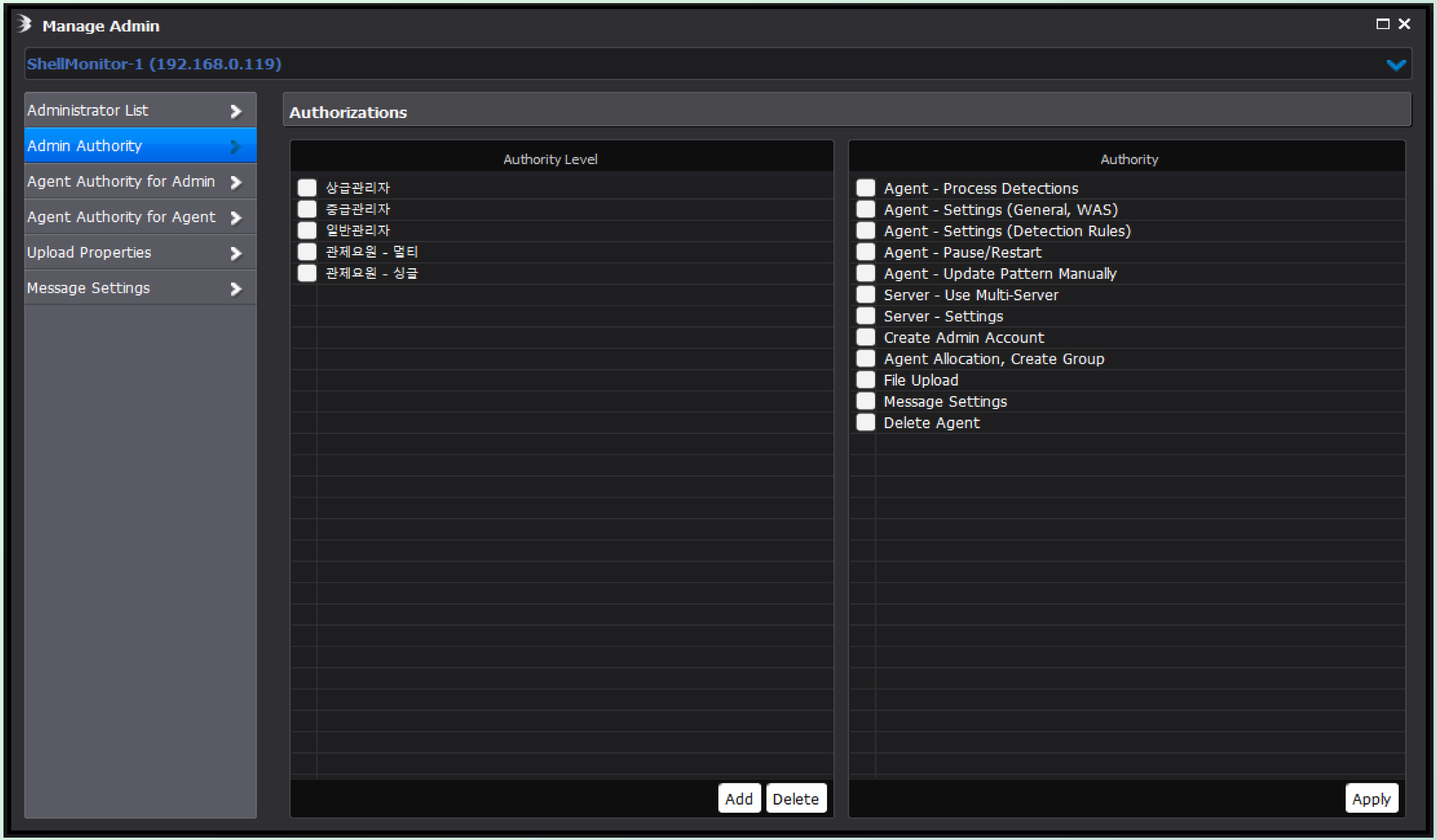
Management View

Update Management



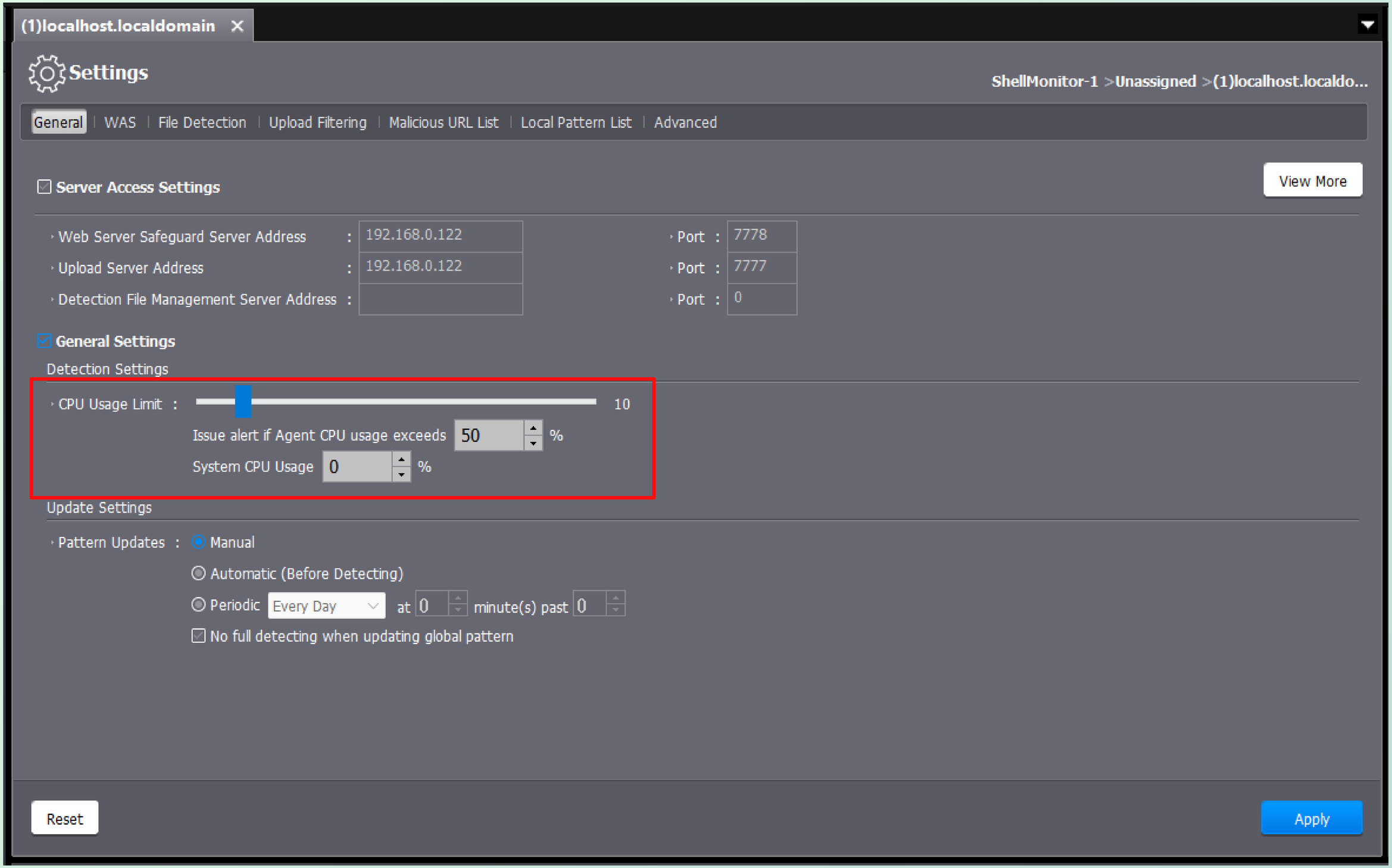
Management View

Administrator Permissions



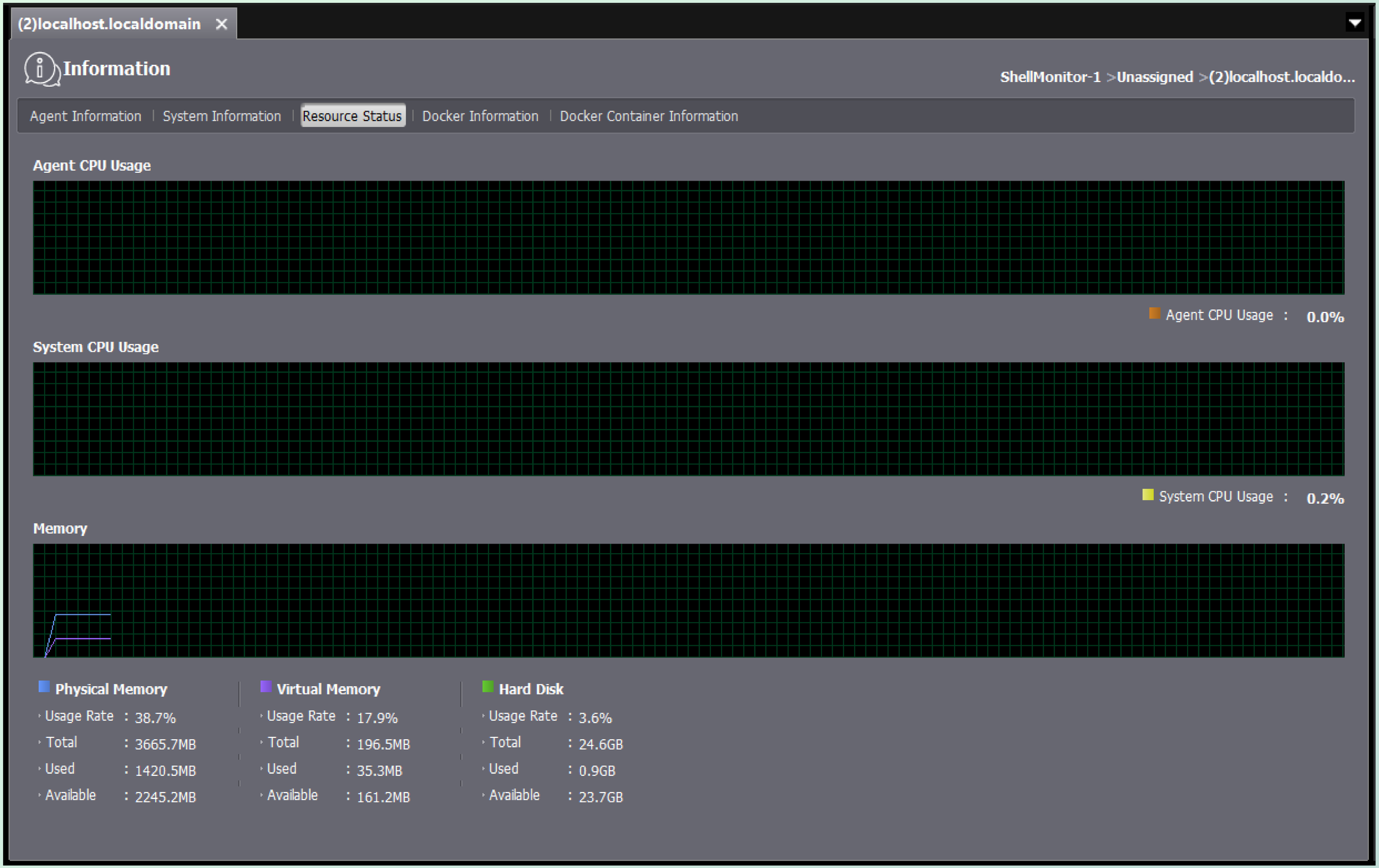
Management View

Stability



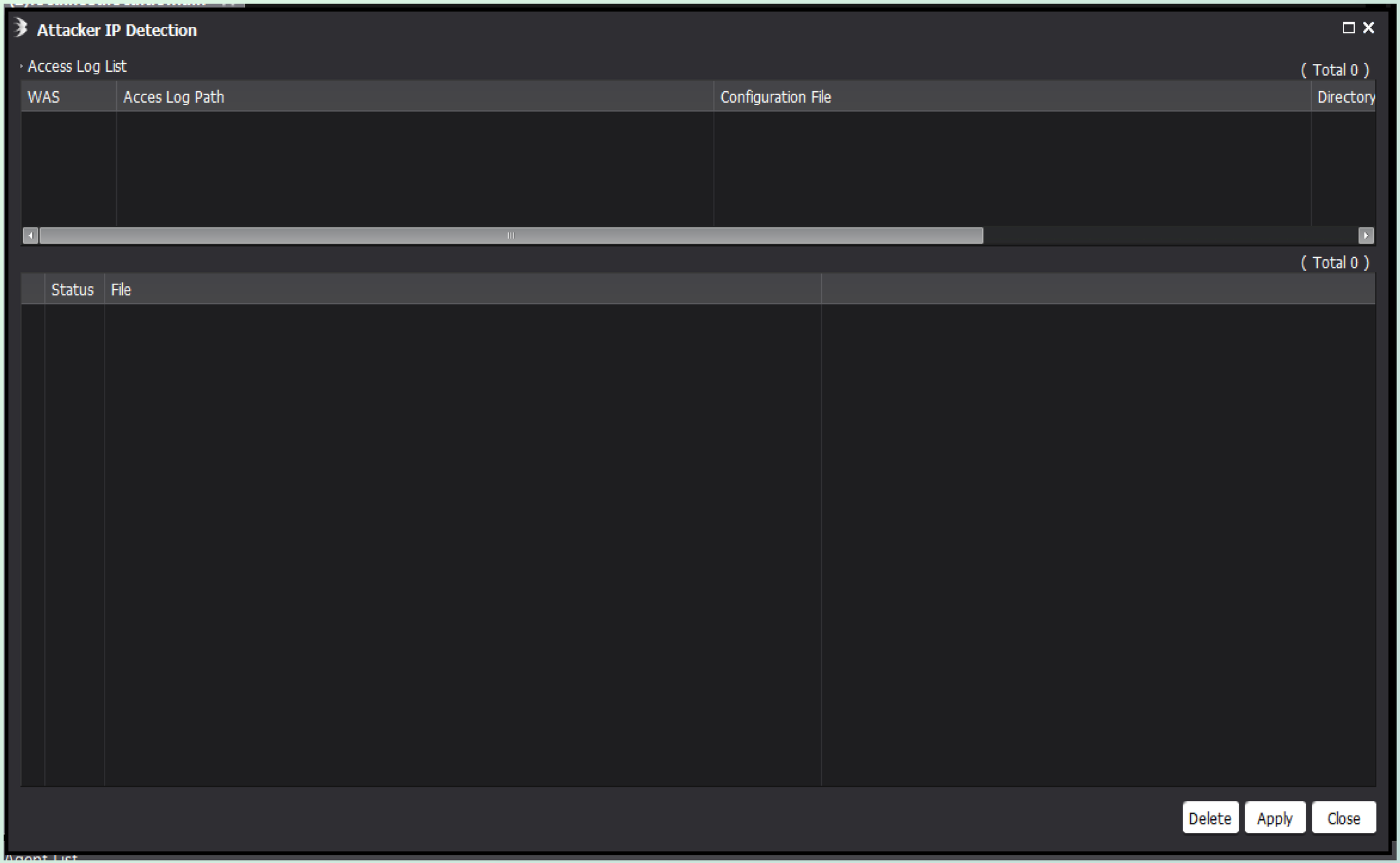
Management View

Resource Status Monitoring



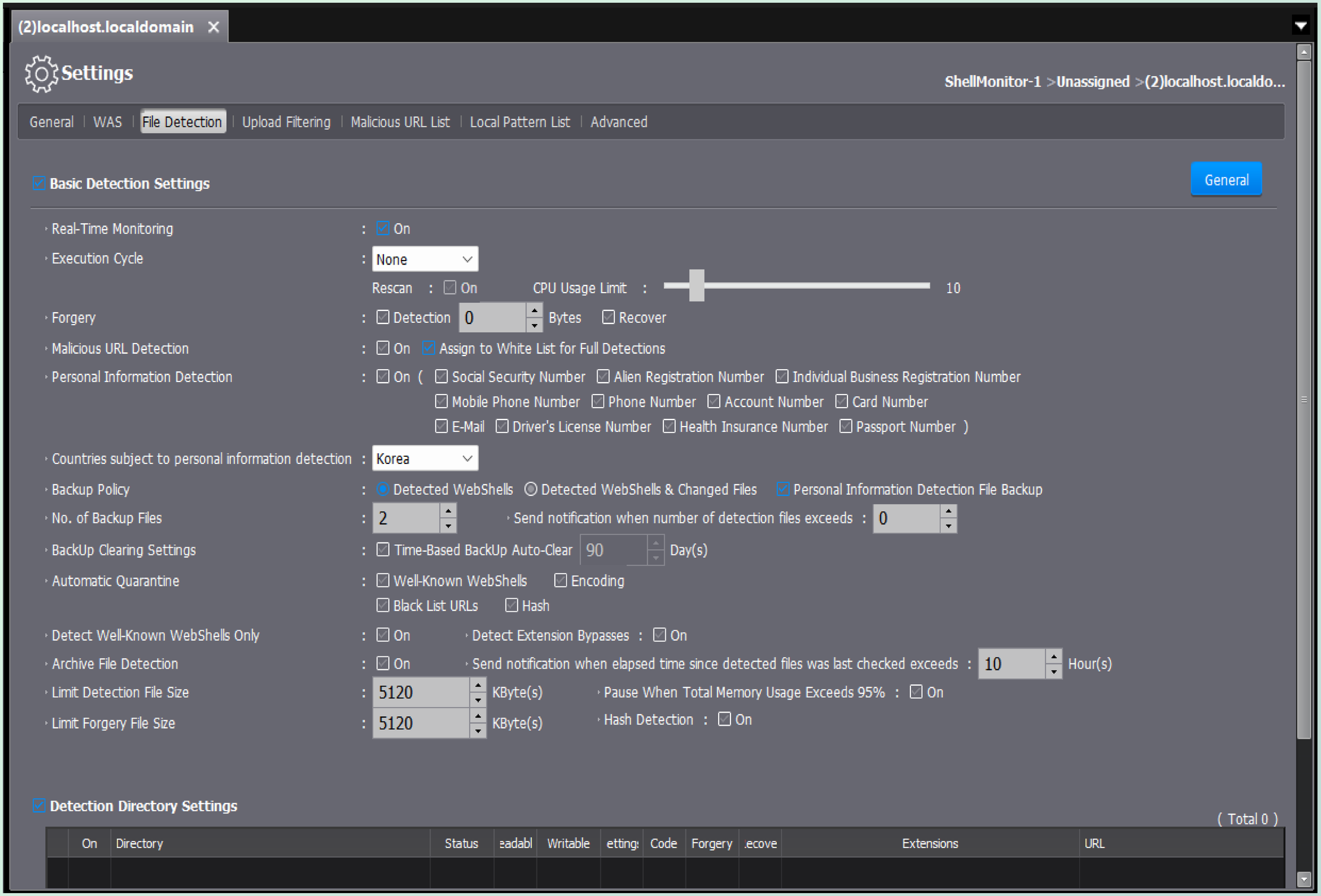
Management View

Attacker IP Detection



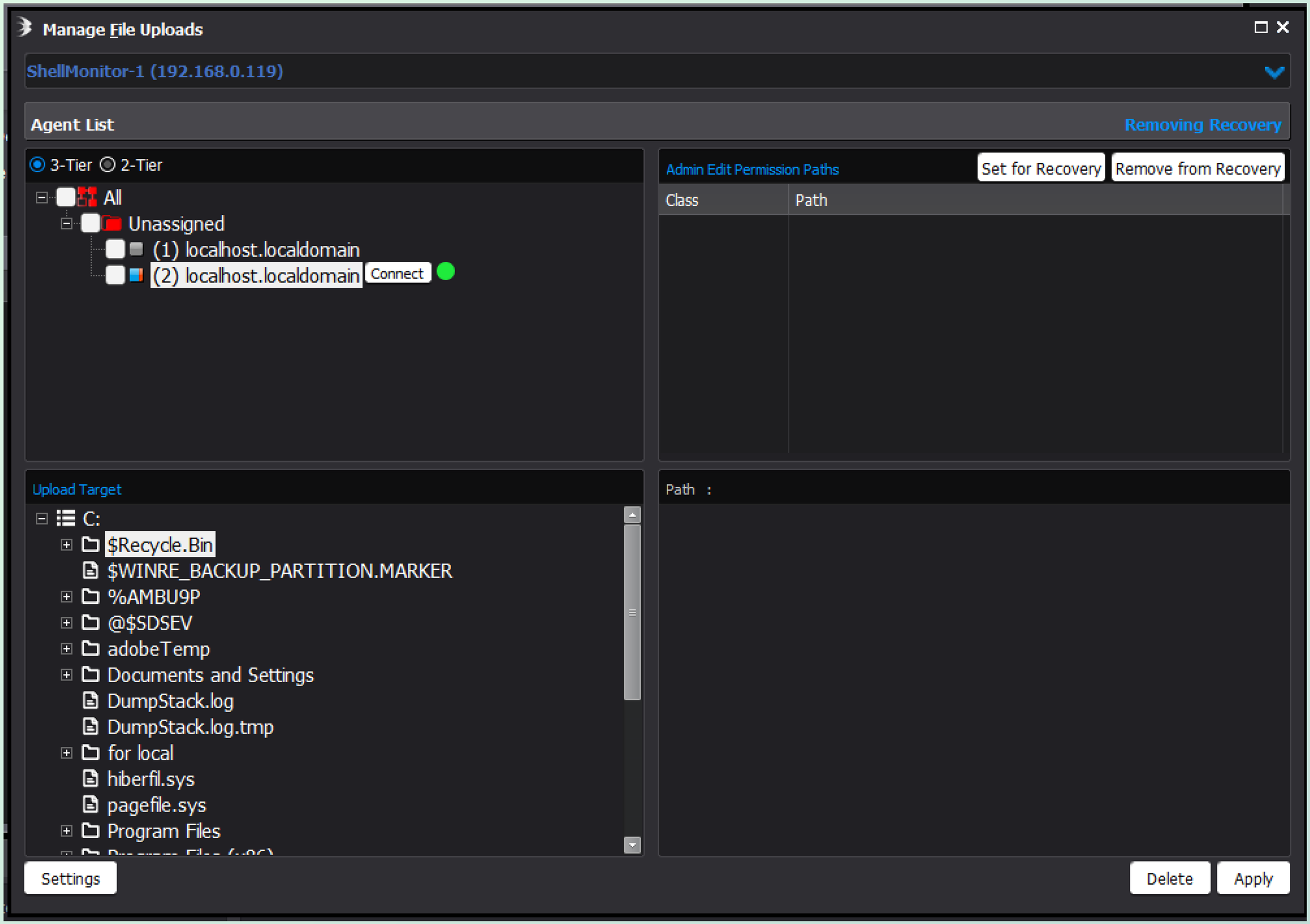
Management View

Preferences Management



Management View

Dedicated Safe Uploader



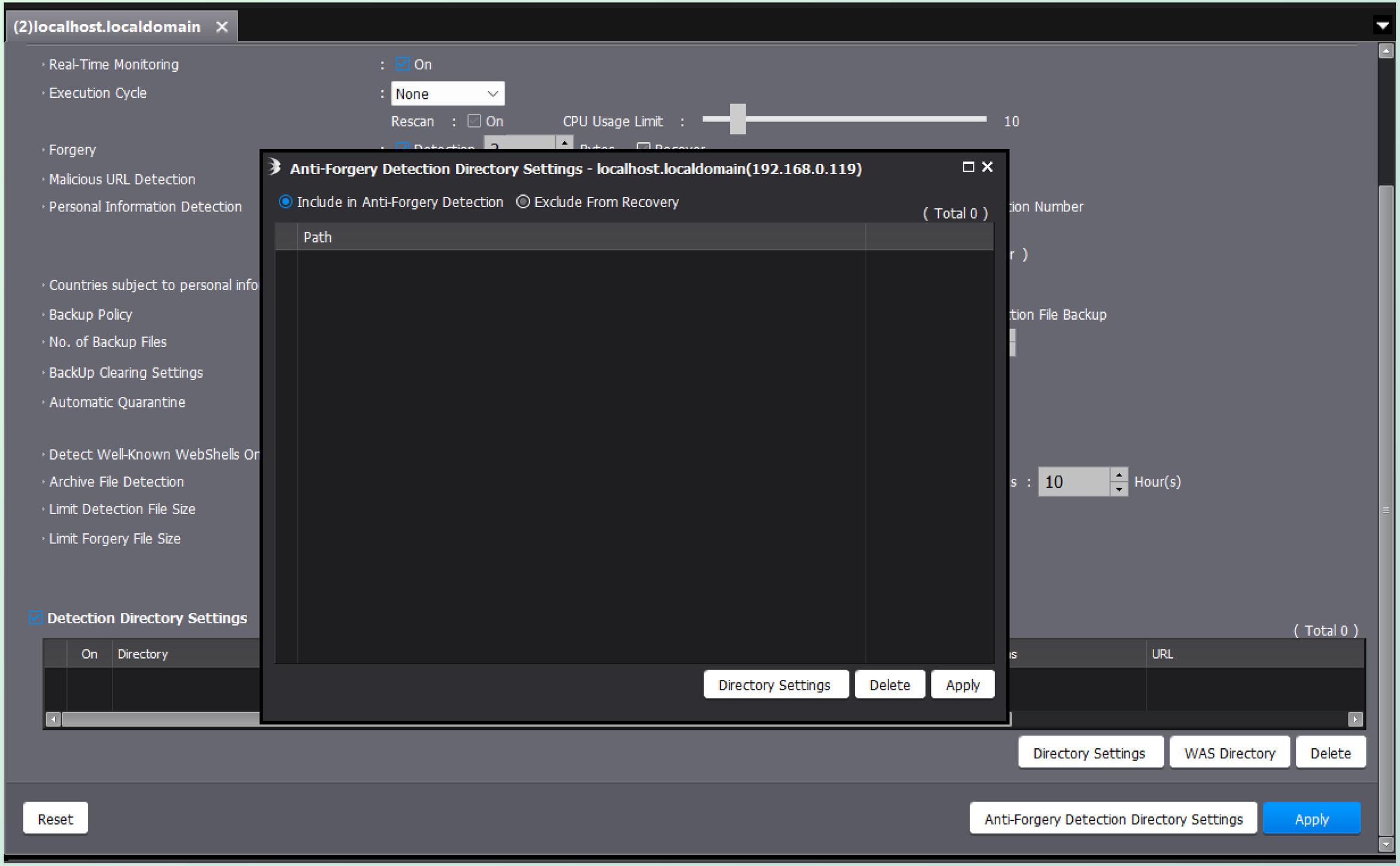
WARSS Functions

Cloud Computing Support

Function Name	Description
Scale In/Out	• Auto-registration of new detection targets on scale out; detection begins automatically • Automatic backups of detection/change/deletion logs to management server for deleted Agents on scale in
Home Directory Search	• Schedule detections to find changes/additions to web/WAS home directory • View addition/change history of home directory
History Management	Agent operation status and history management (installation, deletion, start/stop, etc.)
Event Duplication Prevention	Prevent duplicate detection events from occurring in redundant systems when home directory is included in NAS area

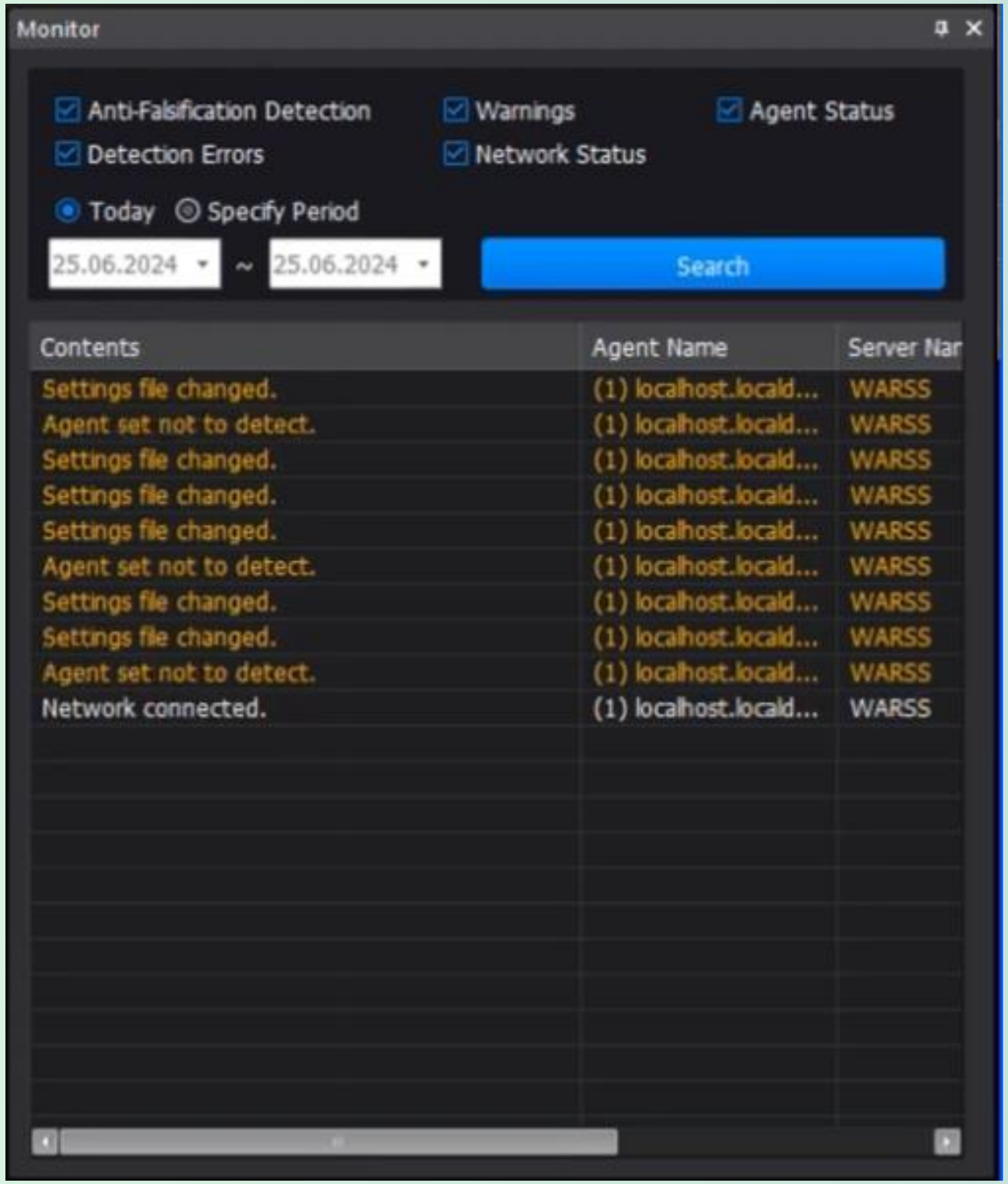
Cloud Settings View

Home Directory Search



Cloud Settings View

Logging/History Management



WARSS On-Premise Configuration Diagram