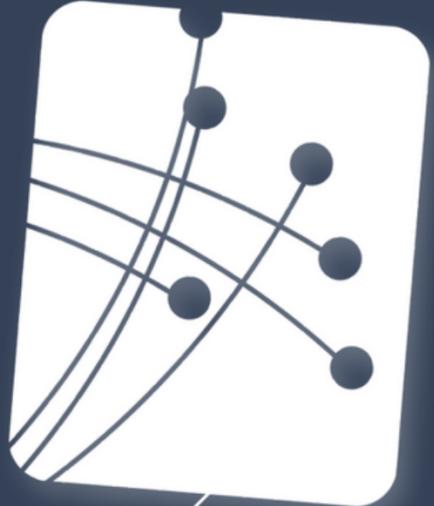




CSP 

COMPUTER SECURITY PRODUCTS, INC.

SECURITY | AUDIT | COMPLIANCE



**VULNERABILITY MANAGEMENT
& COMPLIANCE FOR
NONSTOP SYSTEMS**

Presented by Henry Fonseca
General Manager, CSP

How invulnerable are we, really ?



The Swiss Cheese Model



- We all have multiple defenses. We also have multiple vulnerabilities.
- If you think you are invulnerable, you're wrong. And your confidence in your invulnerability actually increases your risk.
- When an organization is compromised, all the holes in their defenses lined up and left them vulnerable.
- This kind of security failure is known as the Swiss Cheese Model.

Ransomware is on the Rise



InterContinental Hotel Group

Ransomware attack
affected booking and
other applications



Läderach Swiss Chocolatier

Cyber-attack affected
production, logistics, and
administrative operations



Irish Health System HSE

Ransomware attack
affected almost every part
of the Irish healthcare
system

**No
Organization
Is Immune to
Threats**





ZERO TRUST KEY PRINCIPLES

MULTI-FACTOR AUTHENTICATION

Additional layer to verify
authorized access

IDENTITY & ACCESS MGMT

Know which users have
access and what they can
see and change

DATA ENCRYPTION

Ensure critical data is
classified and encrypted

LEAST PRIVILEGED ACCESS

Users should only have
access to the specific
resources needed to
complete a given task

PCI-DSS 4.0

REGULATIONS

RULES - LAW

REQUIREMENTS

COMPLIANCE

STANDARDS

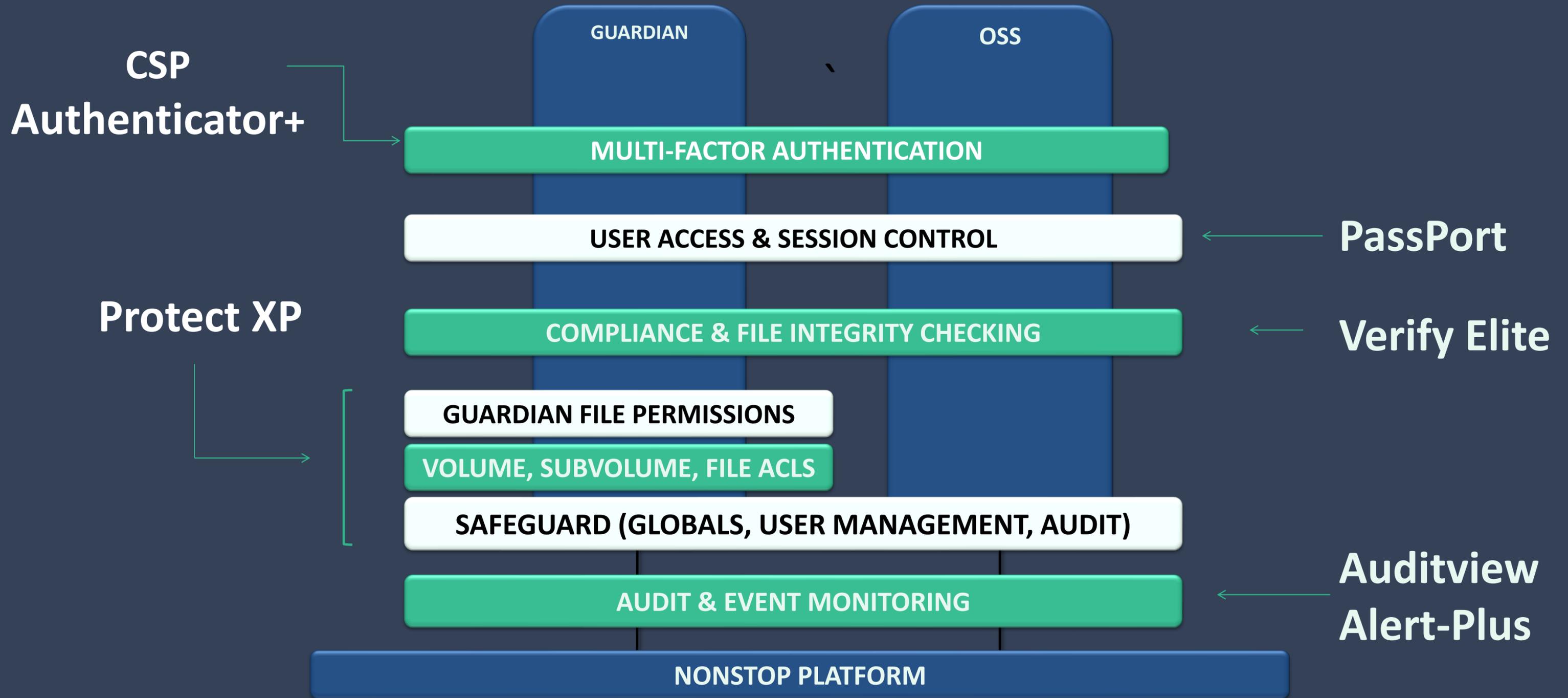
TRANSPARENCY

POLICIES

**And how can
we forget...**

**Compliance
Requirements**

CSP Solution Suite



PROTECTING SENSITIVE DATA

MULTI-FACTOR AUTHENTICATION



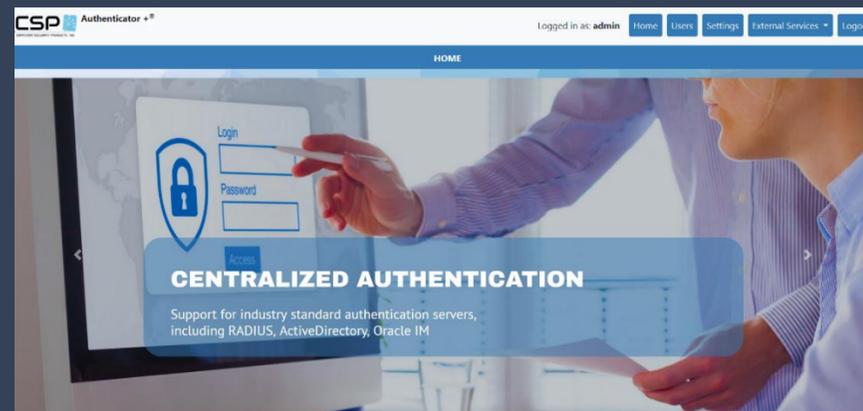
PRESERVING THE INTEGRITY OF YOUR NONSTOP

Why is MFA so Critical for NonStop?



1. Provides superior identity verification & security.
2. Ensures compliance with regulations.
3. Required for all access to the CDE (PCI 4.0; Req. 8.4).

CSP's Solution for MFA: CSP Authenticator+



CLOUD-BASED FRAMEWORK

New cloud-native application built using modern technologies



MULTIPLE AUTHENTICATION METHODS

Including Active Directory, RSA, Microsoft, RADIUS, OTP



PATHWAY SUPPORT

NonStop agent supports TACL, Pathway and Non-Pathway applications.

CSP

Authenticator +

AUTHENTICATION METHODS

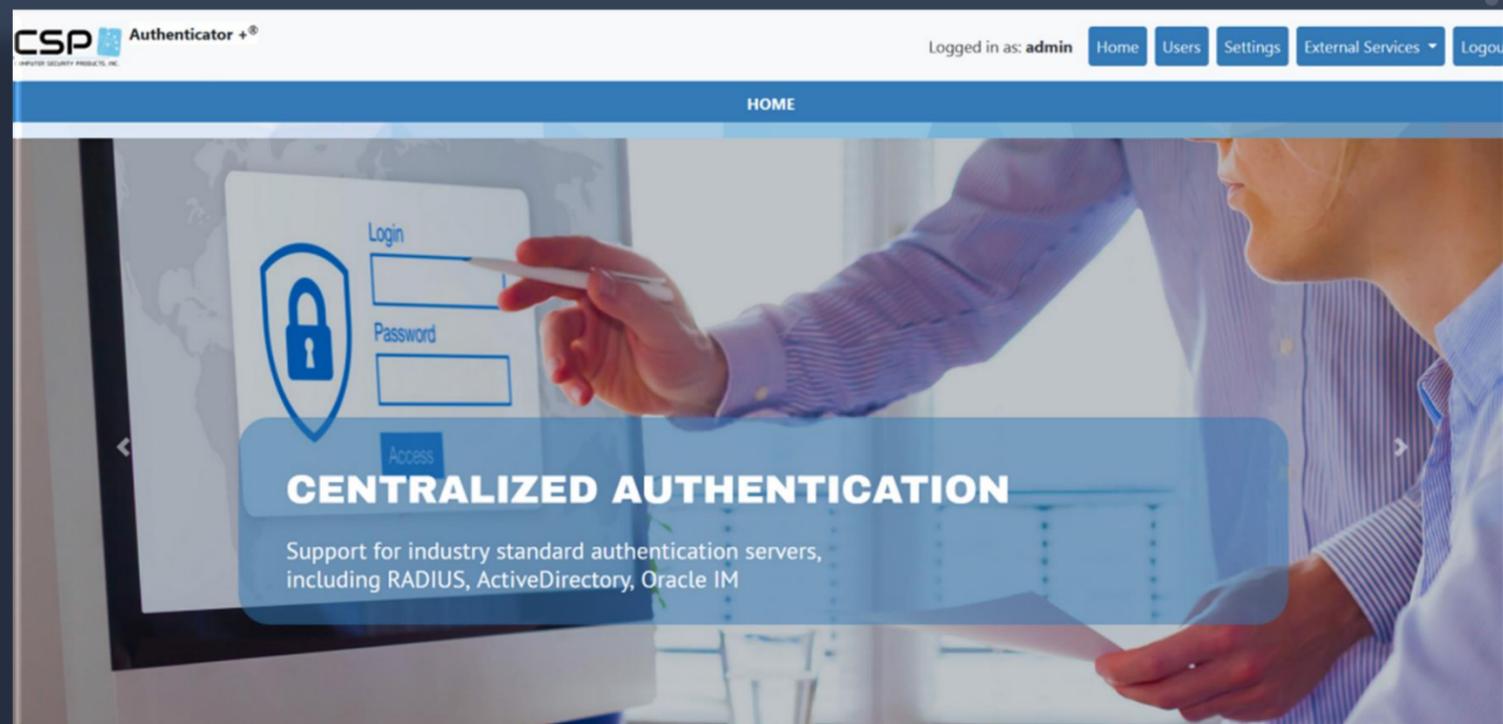
SUPPORTED METHODS
INCLUDE:

RADIUS

ACTIVE DIRECTORY

RSA, MICROSOFT, GOOGLE

OPEN LDAP, OTP





CSP AUTHENTICATOR+ KEY FEATURES

1

**Support for Various
Authentication Methods**

2

**Browser-based, User-friendly
Interface**

3

**Supports Kubernetes
framework & High Availability**

4

**Configure for All or Select
Privileged Users**

Protecting Sensitive Data

**FILE
INTEGRITY
MONITORING**



PRESERVING THE INTEGRITY OF YOUR NONSTOP



Monitor Changes to Sensitive Data

ENSURE COMPLIANCE

NonStop System security (Guardian & OSS) must meet industry standards and regulations (PCI DSS, SOX, GDPR).

IDENTIFY & TRACK CHANGES

Ensure that any unauthorized changes are immediately identified and reported.

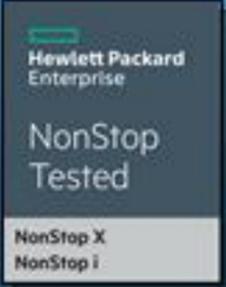
GENERATE COMPLIANCE REPORTS

Have the ability to provide detailed compliance reports.

**THE
REDESIGNED
VERIFY ELITE®**



Verify Elite® COMPLIANCE



Verify Elite® – Compliance at Your Fingertips®



VERIFY ELITE[®]

KEY FEATURES

NEW INTUITIVE DESIGN

Changes to the UI create an Enhanced User Experience.

COMPLIANCE MONITOR

Ensure your compliance by performing regularly scheduled compliance checks.

FILE INTEGRITY MONITOR

Execute file integrity checks to immediately identify unauthorized changes.

MULTI-NODE FILESET COMPARE

Compare filesets located either locally or across multiple NonStop nodes.

VERIFY ELITE®

Guardian File Integrity

				
Guardian Fileset Maintenance	Guardian File Check	Guardian Baseline Reset	Guardian Result History	Guardian Fileset Result Compare

OSS File Integrity

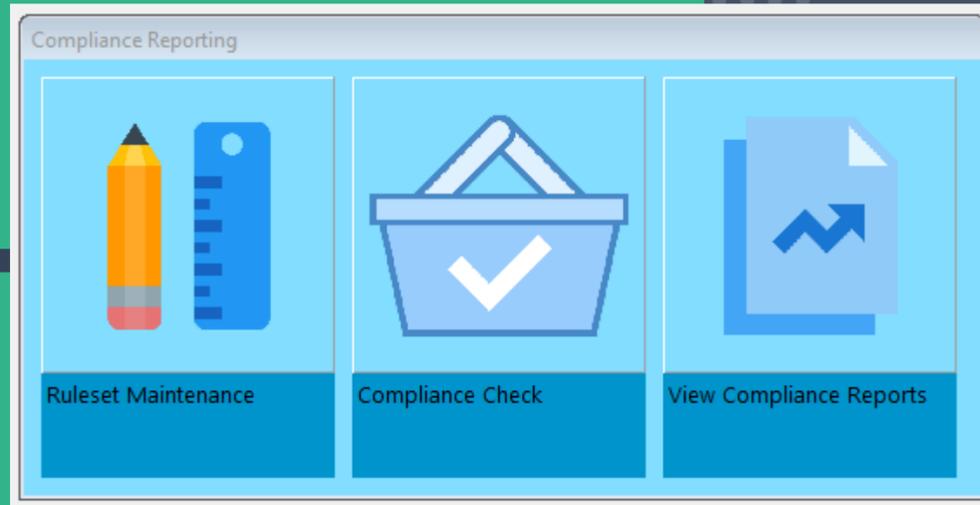
				
OSS Fileset Maintenance	OSS File Check	OSS Baseline Reset	OSS Result History	OSS Fileset Result Compare

Compliance Reporting

		
Ruleset Maintenance	Compliance Check	View Compliance Reports

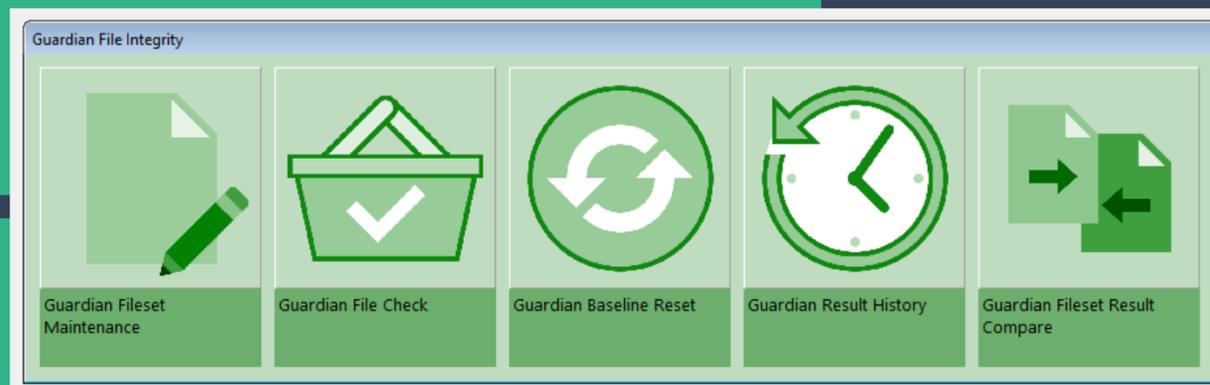
Utilities

				
Scheduler	Spool View	OSS Explorer	Guardian file Search	Archive and Restore



SECURITY COMPLIANCE MONITOR

Verify Elite's Security Compliance Monitor can ensure compliance with regulations and internal security policies by performing regularly scheduled compliance checks.



FILE INTEGRITY MONITOR

Verify Elite's File Integrity Monitor ensures that any unauthorized changes are immediately identified and reported by executing regularly scheduled file integrity checks.

Verify Elite®

Multi-Node Fileset Compare

Regular comparison of filesets across nodes should also be a part of the file integrity verification process.

MULTI-NODE FILESET COMPARE FEATURE ALLOWS YOU TO:

- Compare filesets situated either locally or across NonStop nodes.
- Compare any two selected filesets.
- Identify both the matches and differences between the file attributes in each fileset across nodes.
- If a discrepancy is found, investigation and possible remedial action can be taken.

VERIFY ELITE[®]

KEY FEATURES

1

**Pre-Built Customizable
Compliance Rules**

2

**Monitors Both Guardian & OSS
Files**

3

Schedule periodical checks

4

**Real Time Notifications with
Alert-Plus**



NEW PRODUCT ANNOUNCEMENT!

Introducing:

CSP Vulnerability Scanner

Vulnerability Scanning & Reporting solution
for NonStop Systems

CSP - Compliance at your Fingertips™



Why scan NonStops?

- Prevent & minimize data loss in case of unauthorized breaches, cyber attacks, or unintentional errors.
- Identify and rectify privilege creep and reduce exposure to sensitive data.
- Get recommendations for improving system security and restricting access.
- Address compliance requirements.

Vulnerability Scanner

Key Features



- Scan NonStops to identify vulnerabilities.
- Get recommendations to improve security.
- Quick to install and easy to use.
- Easily select from available reports.
- Export and share reports with Spoolview

Vulnerability Scanner

Key Report Types



- Security Analysis Reports
- Authorization Reports
- Explain Access to Objects
- Safeguard Globals Reports
- Group Members Reports
- Examine Sub-Volume Access Reports
- Show Access Reports

VS-1

```
$D2 PTVS100A 70> run vsreport

* * * * *
*          Vulnerability Scanner Report Generator v1.00          *
*    Copyright (c) 2022 - Computer Security Products Inc.      *
* * * * *

*****
Please choose from the following report types:
  1. Security Analysis Report.
  2. Authorization Report.
  3. Examine Subvolume Access Report.
  4. Explain Access to Object Report.
  5. Group Members Report.
  6. Show Access Report.
  7. Safeguard Globals Report.
  99. Quit.

Please select a report type: █
```

This is where you execute the VSREPORT macro from the installation sub-volume.

It presents 7 key report categories for selection.

VS-2

```
Please select a report type: 1
```

```
* * * * *
```

```
** Security Analysis Reports **
```

```
Please select one of the following reports:
```

11. Check ALL.
12. Check CMON.
13. Check Guardian.
14. Check Safeguard.
15. Check TACL.
16. Check users.
17. Check security for ALL files.
18. Check security for a file pattern.
19. Check file pattern for embedded LOGON commands.

```
Please select a report number: █
```

After a report number is chosen in the previous step, it presents the corresponding report types for further selection

VS-3

```
Please select a report type: 1
```

```
* * * * *
```

```
** Security Analysis Reports **
```

```
Please select one of the following reports:
```

- 11. Check ALL.
- 12. Check CMON.
- 13. Check Guardian.
- 14. Check Safeguard.
- 15. Check TACL.
- 16. Check users.
- 17. Check security for ALL files.
- 18. Check security for a file pattern.
- 19. Check file pattern for embedded LOGON commands.

```
Please select a report number: 13
```

```
- Report output is $S.#RPT13
```

```
MFB-00018 The report server process has completed.
```

After selections and entering any requested parameters, the job executes and report is produced.

**Announcing the
Global NS
Partner Alliance**

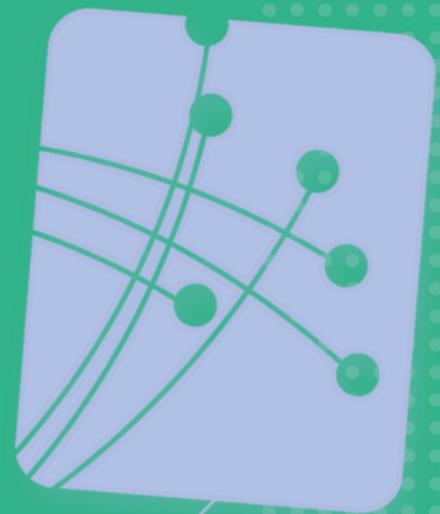




Q&A



CS&P



COMPUTER SECURITY PRODUCTS, INC.



ADDITIONAL RESOURCES



CSP WEBSITE

www.cspsecurity.com



CSP-WIKI

<https://wiki.cspsecurity.com/>



CONTACT US VIA EMAIL

Sales-CSP@cspsecurity.com

