
CSP
COMPUTER SECURITY PRODUCTS, INC.

SECURITY | AUDIT | COMPLIANCE

CSP
COMPUTER SECURITY PRODUCTS,INC.

NONSTOP RISK MANAGEMENT & COMPLIANCE WITH CSP

Presented by Peter Mehta
Head of Sales, CSP

Vulnerability Management

Ongoing practice of managing vulnerabilities in your IT systems.

An important pillar of cybersecurity, vulnerability management is a critical part of any organization’s overall security and digital resilience strategy.

Every system has vulnerabilities. Do you know where yours are?



- Weak spots are prime targets for threat actors.
- Providing opportunities for them to steal sensitive data.
- Cause damage to the network.
- Deny access to authorized users.
- Vulnerability Management is the key to reduce these weak spots, mitigate risks and improve your security posture

DORA Defines IT Risk Management as a key pillar

DORA: THE EU'S NEW REGULATORY FRAMEWORK ON DIGITAL OPERATIONAL RESILIENCE

The Digital Operational Resilience Act is in effect since January 2025.

ICT RISK MANAGEMENT IS 1ST KEY PILLAR

The requirement is defined as a comprehensive risk management framework for ICT systems including policies, procedures, regular assessments and programs

CSP has developed several tools to help you improve your security posture, including:

IDENTIFY, ANALYZE, & RESOLVE SECURITY VULNERABILITIES

- CSP Vulnerability Scanner

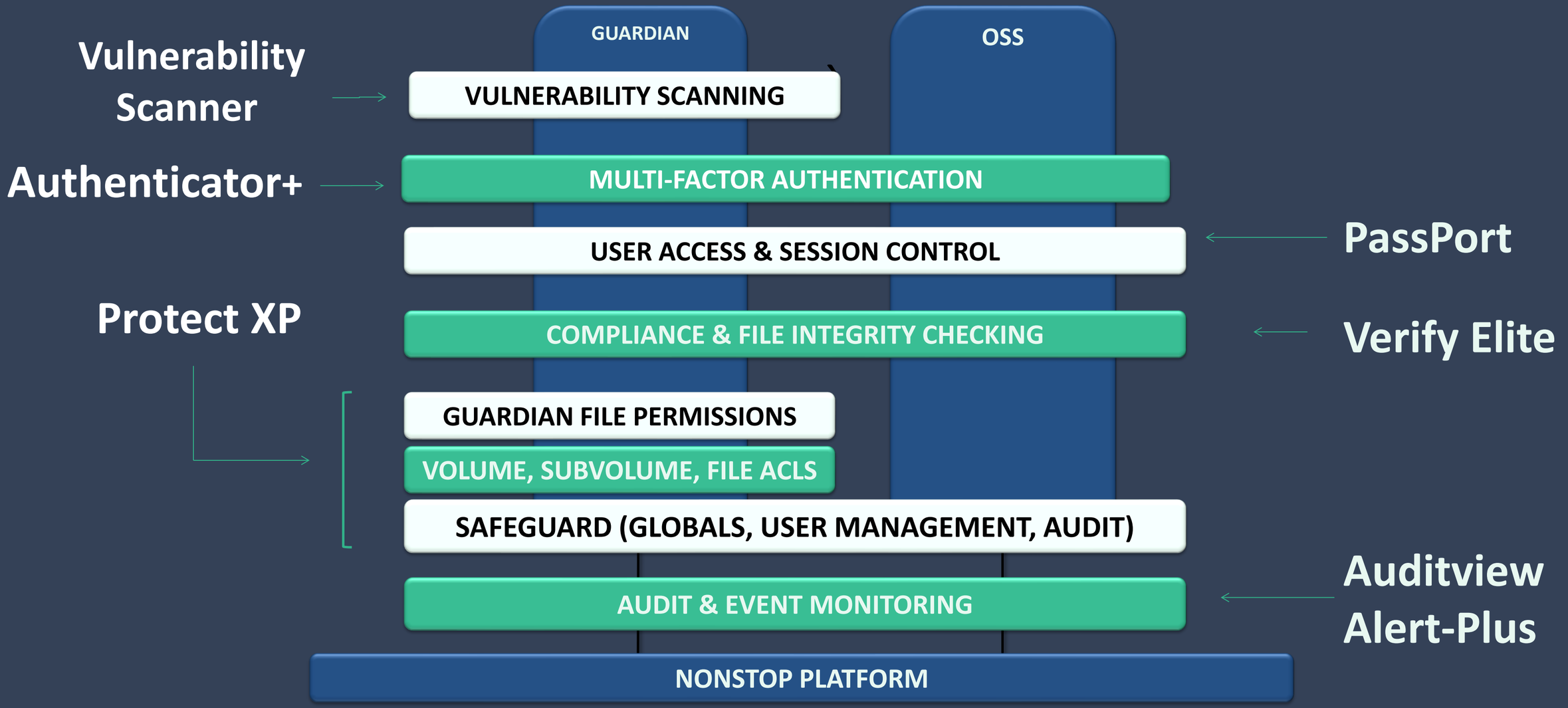
VERIFY FILES & RUN COMPLIANCE REPORTS

- Verify Elite

MANAGE & AUTHENTICATE USERS

- CSP Authenticator + v 5.0

CSP Solution Suite



Protecting Sensitive Data

VULNERABILITY SCANNING



PRESERVING THE INTEGRITY OF YOUR NONSTOP

What is Vulnerability Scanning?

The practice of identifying security weaknesses in systems, networks, and applications by conducting regular scans. Organizations can proactively address vulnerabilities, reducing the risk of cyberattacks and data breaches.

Vulnerability scanning also helps organizations maintain compliance with industry regulations and security standards, as many frameworks require periodic vulnerability assessments.

Perform Scans to Identify Vulnerabilities

MINIMIZE DATA LOSS

Prevent & reduce data loss in case of unauthorized breaches, cyber attacks, or unintentional errors.

IDENTIFY PRIVILEGE CREEP

Identify and rectify privilege creep and reduce the exposure of sensitive data.

IMPROVE SYSTEM SECURITY

Get recommendations for improving system security, restricting access, and address compliance requirements.

CSP VULNERABLITIY SCANNER



Vulnerability Scanning & Reporting solution
for NonStop Systems

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

WHAT'S NEW IN VERSION 3.0

1. **Pathway Files Reports: List files containing Pathway commands and TPS objects**

2. **Compare History of Pathway Files added/deleted: Summary Report & Details Report**

3. **OSS Reports, including :**

- OSS File Verification Report
- OSS User Access Report
- OSS Orphan Files Report
- OSS SetUID/SetGID report
- OSS Directory Contents report
- OSS Symbolic Links report

VS-1

```
$D2 PTVS300A 2> run vsreport

   * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
   *         Vulnerability Scanner Report Generator v3.00          *
   *   Copyright (c) 2022-2024 - 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.
     8. Object Verification Report.
     9. New Program Discovery Report.
    10. Orphan Files Report.
    11. Weak Passwords Report.
    12. Pathway Files Report.
    13. OSS Report.
    99. Quit.

Please select a report type:
```

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

It presents 13 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.

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

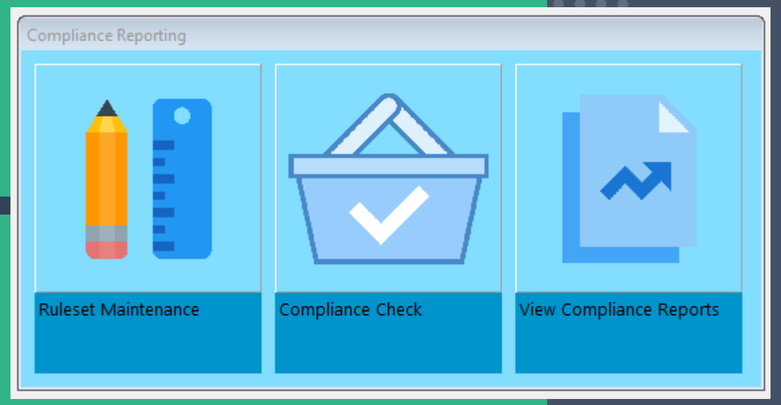
Provide detailed compliance reports as required.

THE REDESIGNED VERIFY ELITE®



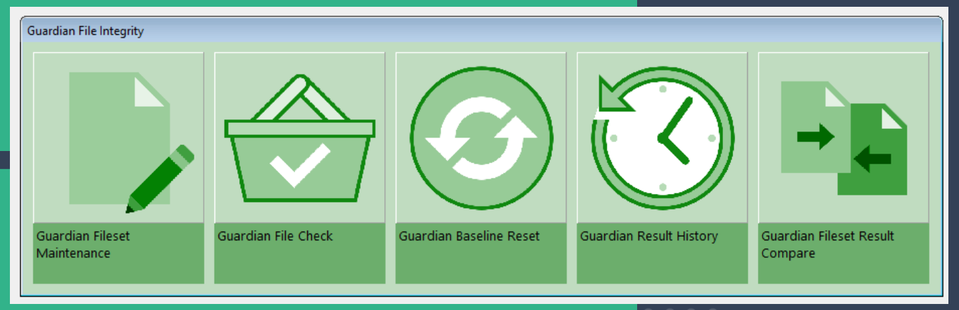
VERIFY ELITE® KEY FEATURES

1. Pre-Built Customizable Compliance Rules
2. Monitors Both Guardian & OSS Files
3. Schedule periodical checks
4. Real Time Notifications with Alert-Plus



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®

SUMMARY OF NEW 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.





Q&A

CSP

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

CSP

COMPUTER SECURITY PRODUCTS,INC.