
HAFS
Distributeur à valeur ajoutée
VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES
EXPERTISE
Des solutions adaptées à chaque environnement
CONFIANCE
Un partenaire fiable à vos côtés
PERFORMANCE
Des infrastructures sécurisées et évolutives
SUPPORT
Un accompagnement technique de qualité
HAFS
Distributeur à valeur ajoutée
Des solutions IT innovantes pour un monde connecté et sécurisé
WIRELESS RADIO
Connectivité sans fil haute performance
RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés
VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives
CYBERSECURITY
Protéger vos données et vos systèmes
VIDÉO PROTECTION
Solutions de vidéosurveillance intellligentes
HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité
SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

SECPOINT®
www.secpoint.com

SecPoint® Penetrator™

Vulnerability Scanner & Assessment

With the SecPoint® Penetrator™ Vulnerability Scanner, you can secure your entire network with advanced scanning technology. It detects vulnerabilities, performs thorough penetration tests, and delivers detailed reports for enhanced protection. Featuring dark web search, customizable profiles, and two-factor authentication, the Penetrator keeps your network safe from threats with timely insights and actionable solutions.

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

INTERFORCE

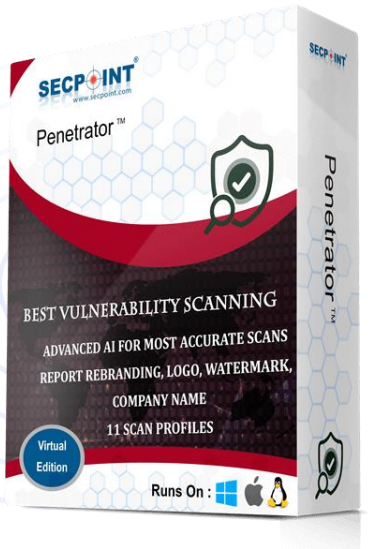
CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

CYBERSECURITY MADE IN EUROPE™

European DIGITAL SME Alliance — Issued by the European DIGITAL SME Alliance

SC MAGAZINE | Web App PENTESTING | network SECURITY | CVE | HIPAA COMPLIANT

e-mærket | trust ECOMMERCE EUROPE | Trustpilot TrustScore 4.9 | 121 reviews



SECPOINT®
www.secpoint.com

About SecPoint®

SecPoint®

- A European cyber security company pioneering the latest cyber security technology
- Serving customers and partner in more than 140 countries
- Offer friendly, easy to use cyber security products
- Providing the best 24-hour support for exceptional customer experience
- Incorporate the latest advanced cyber security feature and technology

SECPOINT®
www.secpoint.com

Product

SecPoint® Protector™
UTM firewall appliance

SecPoint® Penetrator™
vulnerability scanner
and assessment

SecPoint® Portable
Penetrator™
WIFI pen testing

SecPoint® Cloud
Penetrator™

History

2007 — Released the SecPoint® Portable Penetrator™ WIFI pen testing software to combat WIFI security risks . SecPoint® protector awarded the best anti-spam and mail archive solution in DTL data Testlab and infosec magazine, surpassing multiple competitors.

2008 — Pcworld SecPoint® Portable Penetrator™ review. Launched the SecPoint® VIP partner portal to support the increasing number of resellers and distributors.

2005 — Protect star award for SecPoint® Penetrator™. Released the SecPoint® protector firewall, featuring award-winning anti-spam, mail archive, anti-virus, and intrusion prevention.

2011 — Made all SecPoint® products available for download as virtual images, supporting multiple platforms. SecPoint® Protector™ and Penetrator™ RECEIVED A 5-STAR SC magazine review and a 5-star Trustpilot Rating.

2004 — Exhibited at CeBIT Hannover, Germany.

2012 — SecPoint® Penetrator™ Appliance and Cloud Penetrator™ reviewed in hacking magazine. SecPoint® Portable Penetrator™ WIFI pen testing software reviewed in network security magazine.

2003 — Released the SecPoint® Penetrator™ vulnerability scanning appliance, offering node scanning, report branding, and multi-user support.

2015 — Introduced High Availability (HA) IN SecPoint® PROTECTOR™.

2001 — Released the SecPoint® Cloud Penetrator™ as a Software as a service (Saas) solution

2016 — ENABLED Blocking or allowing Social Media on the SecPoint® Protector™ UTM Firewall. All products became available AS 64-BIT.

1997 — Founded by Victor M. Christiansenn V0.1 of SecPoint® Penetrator™ Scanner

2017 — Received e-market and trust ecommerce Europe certificates.

SECPOINT® www.secpoint.com

History

2025

Dark Web Search Feature 4.0

SecPoint® Penetrator™ V65 with over 144,000 vuln checks
Authenticated scanning across Cisco devices & major Linux distributions

26 Languages & 33 Vulnerability Scanning Profiles

2024

Dark Web Search Feature
SecPoint® Penetrator™ Version 61 with over 133,000 vulnerability checks.

20 Languages & 30 Vulnerability Scanning Profiles

2023

Released SecPoint® Penetrator™ Version 57 with over 120,000 vulnerability checks.

Received the cybersecurity made in Europe label.

Launched SecPoint® Protector™ UTM FIREWALL VERSION 62.

Released SecPoint® VIP Partner PORTAL 2.0.

2022

Released the SecPoint® Cyber Security Book

2021

Added the new SecPoint® RBL List to all products.

SecPoint® Penetrator™ expanded to 19 VULNERABILITY Scanning Profiles.

Introduced SecPoint® Lethal Attack Technology

Aggressive Blind SQL Injection, Reflected Cross-Site Scripting, Command Execution CRAWLER.

2020

Added High-Performance VPN module in SecPoint® Protector™.® products now support 2FA login protection.

LAUNCHED A New Fully Transparent Data Privacy page in SecPoint® Protectort And Penetrator™.

SecPoint® Penetrator™ NOW Supports 17 languages in the report.

2019

INTRODUCED new Al Machine Learning Technology in SecPoint® Penetrator™.

2018

SecPoint® PRODUCTS now support 2FA login protection.

Released new improved interface 2.0 on SecPoint® Protector and Penetrator™.

Achieved full GDPR compliance in all sSecPoint® products.

Added Scada ICS plc checks in SecPoint® Penetrator™ and SecPoint® Protector™.

History

2025
AND
BEYOND

SecPoint® Protector™ V68

SecPoint® Book release “How they hack you?!”

SecPoint® at Homeland Security, Dalo Days, DDAC, Showcase for Commerce

SECPOINT®
www.secpoint.com

Risk About Getting Hacked

Top 10 Ways

Business & Organizations Are Blackmailed By Ransomware Gangs

Using Hidden Identities 01

Taking Control Of Data 02

Double Encryption 03

Layered Encryption 04

Side – By – Side Encryption 05

Making Threats For Ransom 06

Exposing Sensitive Data 07

Cyber Extortion 08

Risk of Liability 09

Exposing Stolen Data to Family and Friends 10

SECPOINT®
www.secpoint.com

Top 10 Ways

Business Organizations Get Hacked and Breached

01 Exploiting Zero-Day Vulnerabilities

02 Social engineering

03 Weak or Breached Passwords

04 Phishing Attacks

05 Malware and Ransomware Infections

06 Unpatched Software and Misconfigurations

07 Insider Threats

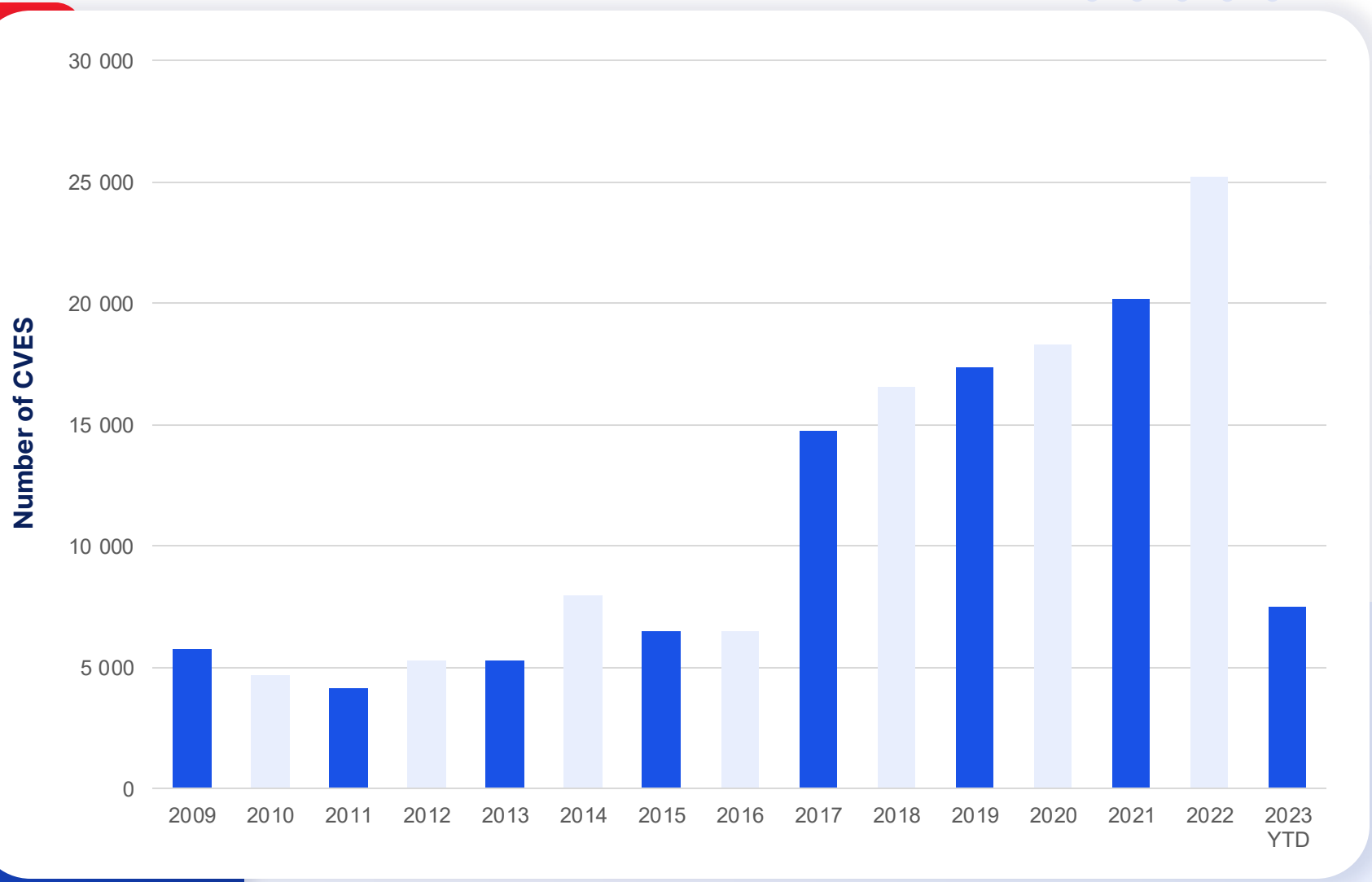
08 Third-Party Risks and Supply Chain Attacks

09 Physical Security Breaches

10 WIFI Hacking

New Vulnerabilities Discovered

In 2022, internet users worldwide discovered over 25 thousand new common IT security vulnerabilities and exposures (CVEs), the highest reported annual figure to date. Between January and April 2023, this number amounted to 7,489.



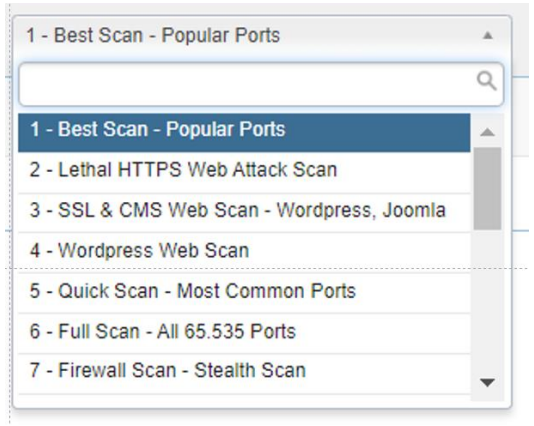
SECPOINT®
www.secpoint.com

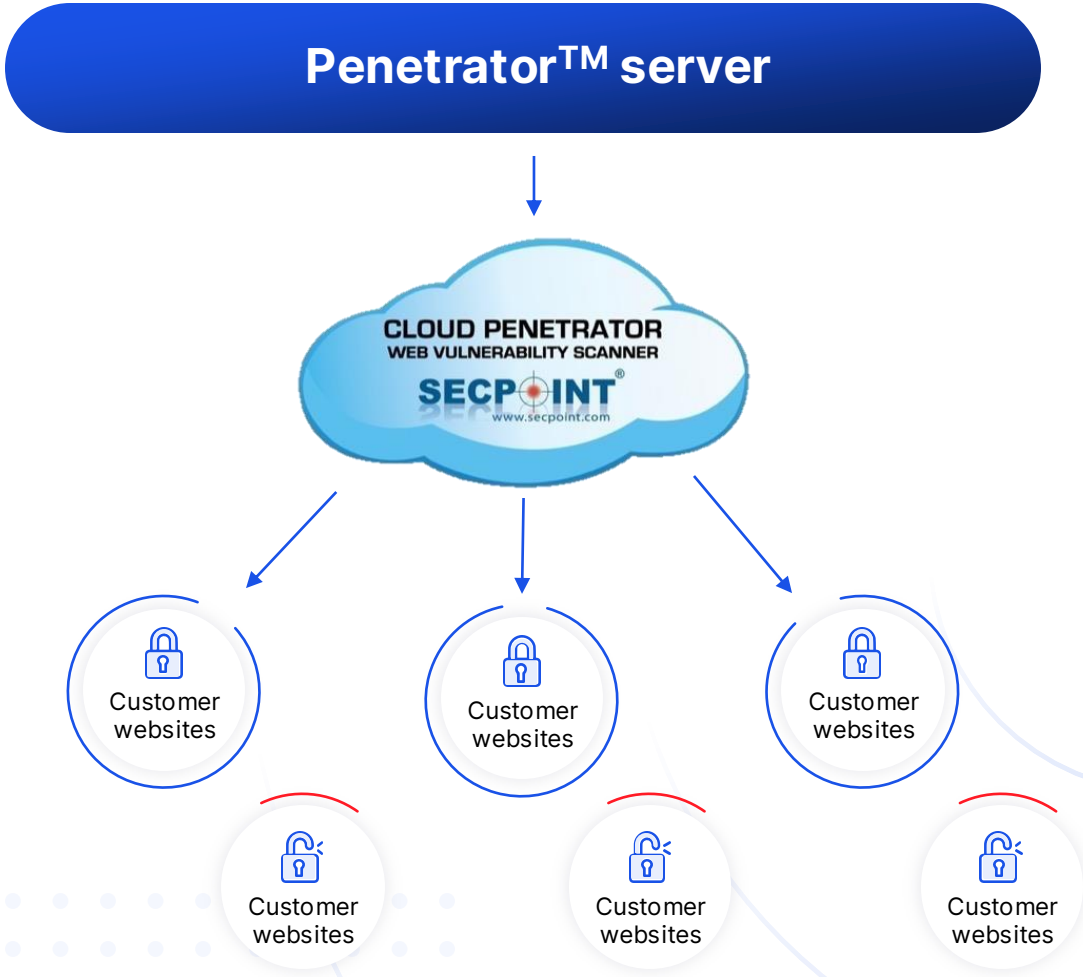
SecPoint® Penetrator™

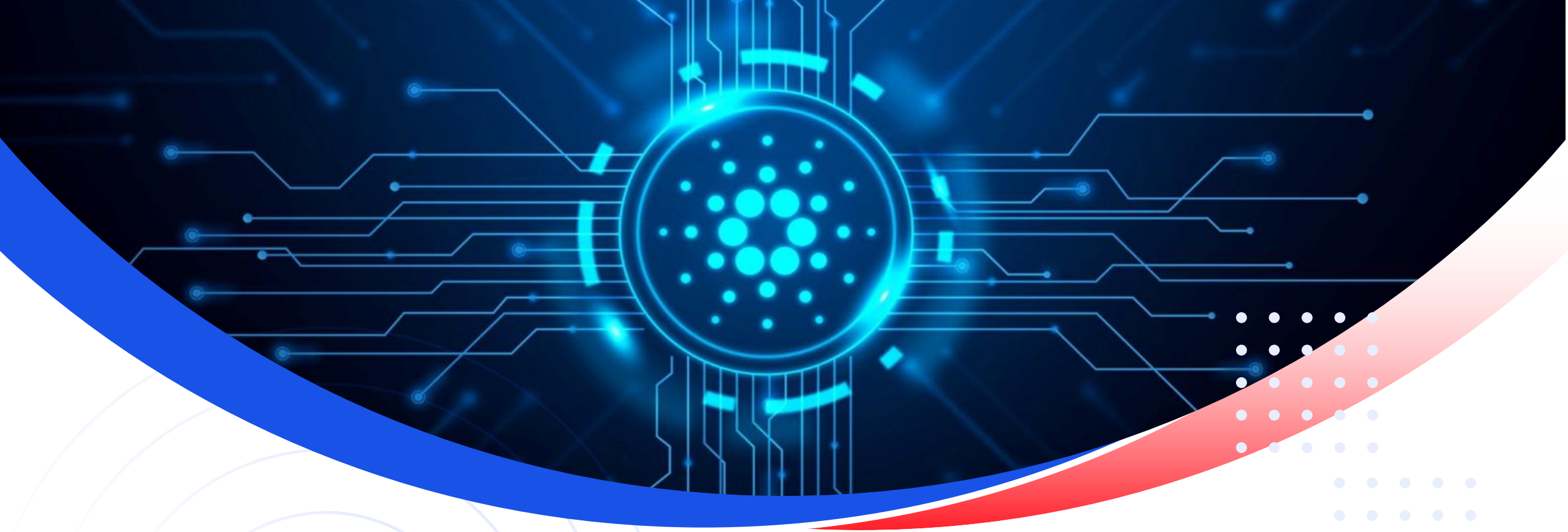
Cloud Penetrator™ in operation

Scanning for:

- SQL Injection
- XSS Cross Site Scripting
- Format String Vulnerabilities
- Command Execution
- Joomla,Wordpress Security Scanner
- Google Security Scanner
- SEO Blackhat Scanner
- Username Guessing
- Denial of Service DoS
- 141.000+ Security Checks.
- Profile Scanning
- Information Disclosure



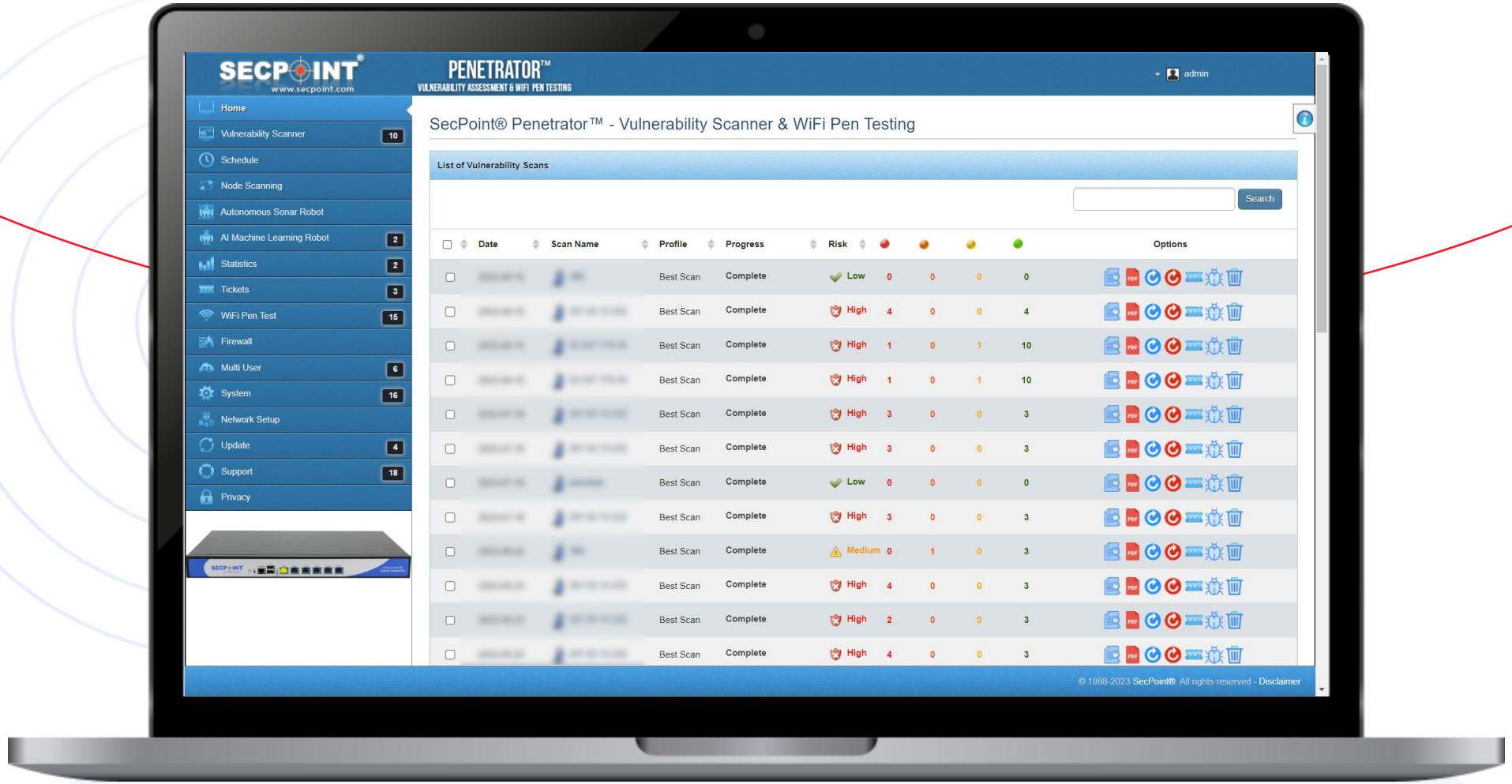




SECPOINT®
www.secpoint.com

Key features in the SecPoint® Penetrator™:

Vulnerability Scanner & WiFi Pen Testing



https://Penetrator.SecPoint.com/spscan/new_scan.php

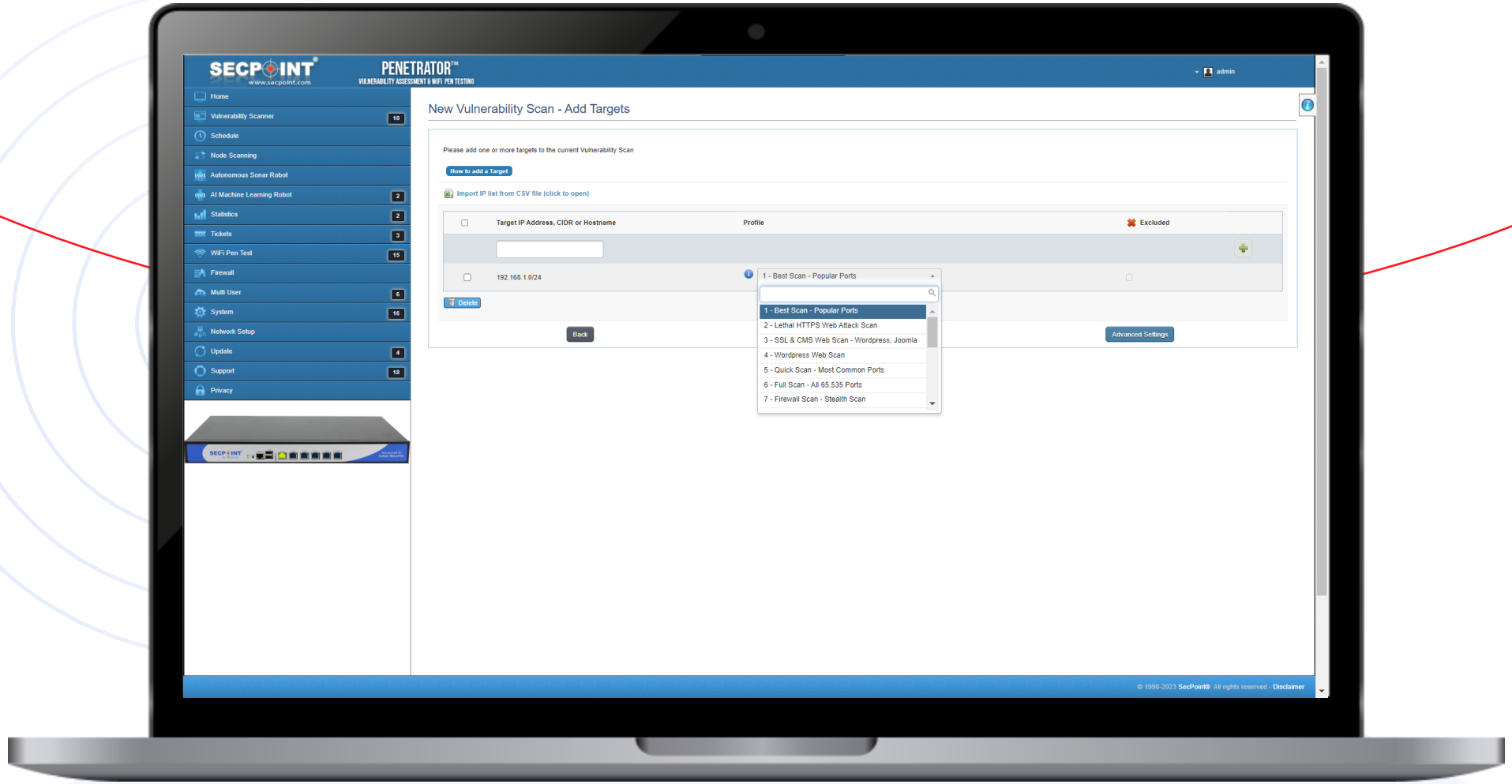
SECPOINT
www.secpoint.com

Vulnerability Scanner & WiFi Pen Testing

https://Penetrator.SecPoint.com/spscan/new_scan.php

SECPOINT®
www.secpoint.com

Vulnerability Scanner



https://Penetrator.SecPoint.com/spscan/new_scan.php

SECPOINT®
www.secpoint.com

Vulnerability Scanner

You can choose between 30 different vulnerability scanning profiles.

Profile can help you to perform quick and fast scans that will give a brief overview of vulnerabilities. You can also perform the recommended Normal Scan or more intensive Full Firewall Scan which are safe to run in production environments. If you need to test the strength of your firewall and systems the Aggressive Scan profile can help with that. We also have several compliance scanning profiles that can be deployed.

If you are not sure which scanning profile is best in your network security environment just feel free to contact us to get support

- **Profile 1** - Best Scan - Popular Ports
- **Profile 2** – Lethal HTTPS Web Attack Scan
- **Profile 3** – SSL & CMS Web Scan – Wordpress – Joomla
- **Profile 4** – Wordpress Web Scan
- **Profile 5** – Quick Scan - Most Common Ports
- **Profile 6** – Full Scan - All 65.535 Ports
- **Profile 7** – Firewall Scan - Stealth Scan
- **Profile 8** – Aggressive Scan - Exploits & DoS Attacks
- **Profile 9** – SSL Security Checks
- **Profile 10** – VoIP devices
- **Profile 11** – Cloud Infrastructure and Services Security
- **Profile 12** – OWASP 10 2021 Compliance
- **Profile 13** – PCI-DSS Preparation for Web Application
- **Profile 14** – HIPAA Policy Compliance
- **Profile 15** – SCADA ICS PLC IoT
- **Profile 16** – CWE 2011 Compliance
- **Profile 17** – ISO 27001 Compliance
- **Profile 18** – NIST 800-53/FISMA Compliance
- **Profile 19** – CIS Controls v8.0 Compliance
- **Profile 20** – CMMC Level 1 Compliance

SECPOINT®
www.secpoint.com

Vulnerability Scanner

You can choose between 33 different vulnerability scanning profiles.

Profile can help you to perform quick and fast scans that will give a brief overview of vulnerabilities. You can also perform the recommended Normal Scan or more intensive Full Firewall Scan which are safe to run in production environments. If you need to test the strength of your firewall and systems the Aggressive Scan profile can help with that. We also have several compliance scanning profiles that can be deployed.

If you are not sure which scanning profile is best in your network security environment just feel free to contact us to get support

- **Profile 21** – DORA Compliance
- **Profile 22** – GLBA Integrity Compliance
- **Profile 23** – FFIEC Compliance
- **Profile 24** – CyberScope Compliance
- **Profile 25** – NERC Compliance
- **Profile 26** – SCAP Compliance
- **Profile 27** – SOX Compliance
- **Profile 28** – CERT Compliance
- **Profile 29** – COBIT/ITIL Compliance
- **Profile 30** – DISA STIGs Compliance
- **Profile 31** – FDCC Compliance
- **Profile 32** – NSA Compliance
- **Profile 33** – NIS2 Compliance

SECPOINT®
www.secpoint.com

Vulnerability Scanner

Profile 1 - Best Scan - Popular Ports

- Will do a non harmful scan with recommended ports.
- Scans 8000 among the most common ports.
- Performs 133.000+ checks.
- Web application vulnerability scanner WAS.
- Automatic Service Identification.
- SQL Injection - XSS Cross Site Scripting - Remote Code Execution.
- Web Crawler - Joomla Security Scan - Google Safe Browsing.
- 50+ Blacklist Checks. Wordpress Security Scan.
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, *Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.
- The normal scan will scan for all areas only limited to most common ports.

Profile 2 – Lethal Web Attack

- SQL Injection (SQLi).
- Blind SQL Injection (Blind SQLi).
- Cross Site Scripting (XSS).
- Attack String Reflection (Reflected XSS).
- Command Code Execution (RCE).
- Web Crawler.
- Remote File Inclusion.
- Directory Traversal.
- Scans Web portals.
- CMS, Web pages.
- Web Interfaces.
- Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Vulnerability Scanner

Profile 3 – SSL & CMS Web Scan

- Will do a non harmful scan with recommended ports.
- Ports such as 80,443,3128,8000,8080,8843,9443,9997,9998.
- Web application vulnerability scanner WAS.
- Lethal Attack Crawler.
- SQL Injection (SQLi).
- Blind SQL Injection (Blind SQLi).
- Cross Site Scripting (XSS).
- Reflected Cross Site Scripting (Reflected XSS).
- Checks for popular SSL Vulnerabilities such as: Heartbleed – Ticketbleed – BREACH.
- Scans Windows, Mac OS X, Linux, *Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.
- The normal scan will scan for all areas only limited to most common ports.

Profile 4 – Wordpress Web Scan

- Scans web ports such as Port 80, 443.
- Quick Wordpress Scan.
- Lethal Attack Crawler.
- SQL Injection (SQLi).
- Blind SQL Injection (Blind SQLi).
- Cross Site Scripting (XSS).
- Cross Site Scripting Attack String Reflection (Reflected XSS).
- Remote Code Execution (RCE).
- Remote File Inclusion.
- Directory Traversal.
- Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Vulnerability Scanner

Profile 5 – Quick Scan – Most Common Ports

- Scan Profile Quick Scan Top common popular ports for fast scan.
- Same as best scan but faster scanning.
- Lethal Attack Crawler.
- SQL Injection (SQLi).
- Blind SQL Injection (Blind SQLi).
- Cross Site Scripting (XSS).
- Reflected Cross Site Scripting (Reflected XSS).
- Remote Code Execution (RCE).
- Remote File Inclusion.
- Directory Traversal.
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- Duration can be several minutesdepending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Profile 6 – Full Scan – All 65.535 Ports

- Will do a non harmful scan with 65.535 ports.
- Scans the whole range of 65535 Ports.
- Performs 120.000+ checks.
- Web application vulnerability scanner.
- WAS Automatic Service Identification.
- SQL Injection(SQLi) Blind SQL Injection (Blind SQLi).
- Cross Site Scripting (XSS) Reflected (Reflected XSS).
- Remote Command Execution (RCE) Web Crawler.
- Google Hack DB Joomla Security Scan.
- Google Safe Browsing 50+ Blacklist Checks.
- Wordpress Security Scan.
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Vulnerability Scanner

Profile 7 - Firewall Scan - Stealth Scan

- Will do a non harmful scan with 65535 ports.
- Scan Profile Full Firewall Scan The Full scan will force the ports to be
- scanned even if port scanning blocking is in place.
- Scans the whole range of **Common Firewall Ports.**
- Performs 133.000+ checks.
- Especially designed for firewalls, because tries to scan nodes even if they appear offline.
- Web application vulnerability scanner WAS.
- Automatic Service Identification.
- SQL Injection.
- XSS Cross Site Scripting.
- Command Execution.
- Web Crawler.
- Google Hack DB.
- Joomla Security Scan. Google Safe Browsing.
- 50+ Blacklist Checks. Wordpress Security Scan.
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Profile 8 - Aggressive Scan - Full Scan, Exploits & DoS Attacks

- Will do a Full Port Scan, Overflow Attacks + DoS Attacks
- Scan Profile Aggressive Scan The Aggressive Profile will launch Denial of
- Service DoS attacks & Exploit attacks.
- This is only recommended on pre production systems since it can cause systems to crash.
- Scans the whole range of 65.535 Ports.
- Includes **Overflow** and **Denial of Service (DoS) attacks. • Performs 60.000+ checks.**
- Web application vulnerability scanner WAS
- Automatic Service Identification
- SQL Injection
- XSS Cross Site Scripting
- Command Execution
- Web Crawler
- Google Hack DB
- Joomla Security Scan, Wordpress Security Scan
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- **Duration can be several hours depending on how many services are found during the scan.**

⚠ **During the scan. Aggressive profile is designed to be harmful against pre production systems.** ⚠

Vulnerability Scanner

Profile 9 - SSL Security Checks

- This profile scans for common SSL checks.
- Scans for missing security headers such as
- X-Frame-Options, X-Xss-Protection, X-Content-Type-Options, Referrer- Policy
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Profile 10 – VoIP Devices

- This scan will check if the audited target for vulnerable VoIP or exposing sensitive data.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Vulnerability Scanner

Profile 11 - Cloud Infrastructure and Services Security Scan

- This profile focuses on identifying misconfigurations, vulnerabilities, and non-compliance with best practices in cloud environments.
- This scan includes checks for exposed data storage, unsecured cloud services, and adherence to cloud platform security guidelines. This scan is vital for organizations leveraging cloud computing to ensure their infrastructure remains secure and resilient against potential threats.
- Will do a non harmful scan on the most common ports

Profile 12 – OWASP 10 2021 Compliance

- Scan Profile OWASP Top 10 Scan.
- **This profile will carry out checks in the OWASP TOP 10. For each of these profiles, when every target IP in a scan is audited with the same profile.**
- Will perform a OWASP 10 2021 compliant scan:

  A01-2021 – Broken Access Control

  A02-2021 – Cryptographic Failures

  A03-2021 – Injection

  A04-2021 – Insecure Design

  A05-2021 – Security Misconfiguration

  A06-2021 – Vulnerable and Outdated Components

  A07-2021 – Identification and Authentication Failures

  A08-2021 – Software and Data Integrity Failures

  A09-2021 – Security Logging and Monitoring Failures

  A10-2021 – Server-Side Request Forgery

  It is designed to be **non harmful and not flood the services** by simulating the human behavior.

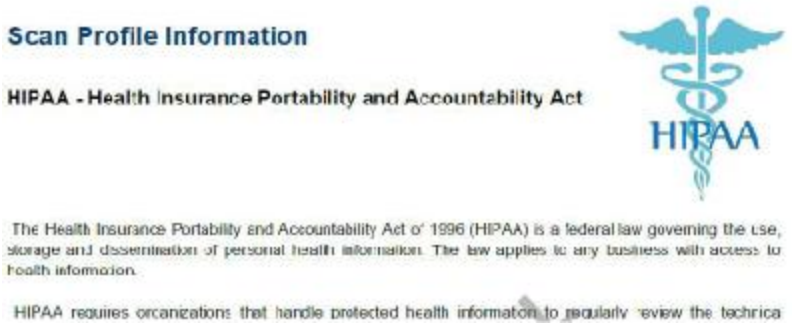
Vulnerability Scanner

Profile 13 - PCI-DSS Preparation for Web Applications

- Get ready for a PCI-DSS assessment. This profile will perform
- A Vulnerability Scan for web applications on the selected targets.
- PCI does not allow self assessments, but requires an external vulnerability scan from an Authorized Scanning Vendor (ASV).
- SecPoint® Penetrator™ can not be used to perform an Internet based scan as it would be done by an ASV.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Profile 14 – HIPAA Policy Compliance

- The HIPAA profile will perform a scan on the requested targets to assess compatibility with the HIPAA security regulations.
- This vulnerability scan should be considered as a part of the HIPAA Security Risk Analysis assessment (SRA).
- This scan will check if the audited target systems are exposed to risk or comply with the key HIPAA security regulations.
- It is designed to be non harmful and not flood the services by simulating the human behavior.



Vulnerability Scanner

Profile 15 - SCADA ICS PLC IoT

- Scan SCADA Industry Systems for vulnerabilities.
- SCADA ICS PLC
- Optimized Scan for Industry Scanning
- SCADA (Supervisory Control and Data Acquisition)
- ICS (Industrial Control Systems)
- PLC (Programmable Login Controllers)
- Including Popular Systems such as:
- Niagara / Foxboro / Moxza / Emerson
- GE General Electrics / Hitachi
- Mitsubishi / Panasonic / Rockwell
- Fisher / IEEE / Schneider / Beckhoff
- OSIsoft / OMRON / OPC / ABB
- Iconic / SNC / Sielco / Telvent
- RUGGEDCOM / Danfoss / Modbus
- Phoenix / Siemens / Tridium
- It is designed to be **non harmful and not flood the services** bysimulating the human behavior.

Profile 16 – CWE 2011 Compliance

- This scan willl check if the audited target is compliant with the 2011 SWE/SANS Top 25 Most Dangerous Software Erors List.
- It is designed to be **non harmful and not flood the services** by simulating the human behavior.

Vulnerability Scanner

Profile 17 - ISO 27001 Compliance

- 1. Information Security Policies: Check for compliance with organizational information security policies. This involves scanning for unauthorised changes to policies, procedures, and configurations that protect data.
- 2. Organization of Information Security: Scan for proper management of information security within organizational processes and structures, ensuring responsibilities are clearly defined.
- 3. Human Resource Security: Before employment, during, and after termination, ensure that access controls and rights are updated to reflect changes, minimizing the risk of unauthorized access.
- 4. Asset Management: Identify systems where sensitive data is stored, processed, or transmitted without adequate protection measures, ensuring all assets are accounted for and securely managed.
- 5. Access Control: Scan for misconfigurations or weaknesses in systems that could allow unauthorized access to information, ensuring that access is restricted based on the principle of least privilege.
- 6. Cryptography: Check for the use of weak encryption algorithms and poor key management practices that could compromise the confidentiality and integrity of data.
- 7. Physical and Environmental Security: While physical security checks are mostly beyond the scope of vulnerability scanning, ensure that logical access controls for physical security systems are not compromised.
- 8. Operations Security: Identify vulnerabilities related to malware protection, backup procedures, logging and monitoring, and control of operational software.
- 9. Communications Security: Scan for weaknesses in network security mechanisms and the management of technical vulnerabilities that could affect data in transit.
- 10. System Acquisition, Development, and Maintenance: Check for vulnerabilities in systems throughout their lifecycle, ensuring they are protected against data loss, malware, and unauthorized access.
- 11. Supplier Relationships: Assess the security of interfaces and data processing with suppliers, ensuring supplier services are monitored and audited for compliance with security requirements.
- 12. Information Security Incident Management: Identify inadequacies in incident detection and response processes, including the effectiveness of monitoring systems to detect and manage breaches.
- 13. Information Security Aspects of Business Continuity Management: Scan for vulnerabilities that could impact business continuity and data recovery capabilities.
- 14. Compliance: Ensure compliance with legal and contractual requirements regarding intellectual property rights, protection of records, privacy, and regulation of cryptographic controls.

Profile 18 – NIST 800-53/FISMA Compliance

- 1. Access Control (AC): Scan for improper enforcement of access controls and policies, ensuring that unauthorized users cannot access or modify information.
- 2. Audit and Accountability (AU): Check for the adequacy of logging and audit mechanisms. Ensure that actions performed on the systems can be uniquely traced to individuals and that unauthorized access attempts are logged.
- 3. Awareness and Training (AT): While not directly scannable, ensure that systems are configured to enforce security awareness, with checks for security notices upon login and reminders.
- 4. Configuration Management (CM): Identify unauthorized changes to software, hardware, and firmware configurations, and ensure systems are hardened against vulnerabilities.
- 5. Contingency Planning (CP): Scan for vulnerabilities in backup and recovery processes that could affect the system resilience to outages or data loss incidents.
- 6. Identification and Authentication (IA): Check for weaknesses in identity verification processes of the system, ensuring that authentication mechanisms are strong, effective, and properly implemented.
- 7. Incident Response (IR): Identify gaps in the incident response capability, including the absence of automatic alerting mechanisms for potential security incidents.
- 8. Maintenance (MA): Scan for vulnerabilities related to the maintenance of information systems, ensuring that maintenance tools and sessions do not introduce new vulnerabilities.
- 9. Media Protection (MP): Check for vulnerabilities related to the protection of digital and non-digital media containing sensitive information, focusing on data leakage and unauthorized access.
- 10. Physical and Environmental Protection (PE): While mostly physical in nature, ensure that systems related to physical access controls (e.g., door access systems) are not vulnerable to tampering or bypass.
- 11. Planning (PL): Indirectly scannable, check that security plans are reflected in system configurations and policies, including the enforcement of security practices.
- 12. Risk Assessment (RA): Identify systems and processes not regularly assessed for vulnerabilities, ensuring continuous risk evaluation and response.

Vulnerability Scanner

Profile 19 – CIS Controls v8.0 Compliance

- 1. Inventory and Control of Enterprise Assets: Scan to ensure all hardware assets connected to the organization network are identified and managed, preventing unauthorized access and vulnerabilities on unknown devices.
- 2. Inventory and Control of Software Assets: Identify unauthorized software installations and ensure only authorized software is present on systems, reducing the attack surface.
- 3. Data Protection: Check for vulnerabilities that could lead to data breaches, ensuring sensitive data is encrypted, properly handled, and protected against unauthorized access.
- 4. Secure Configuration of Enterprise Assets and Software: Identify misconfigurations in operating systems, applications, and network devices that could be exploited by attackers. Ensure systems are securely configured according to the latest benchmarks.
- 5. Account Management: Scan for issues related to account management practices, such as the use of default usernames/passwords, excessive user privileges, and stale user accounts, ensuring adherence to principles of least privilege.
- 6. Access Control Management: Ensure proper implementation of access controls, verifying that users are granted access based on necessity and that controls are in place to prevent unauthorized access.
- 7. Continuous Vulnerability Management: Identify new vulnerabilities and verify that systems, software, and firmware are regularly scanned and updated to protect against known vulnerabilities.
- 8. Audit Log Management: Check for proper configuration and retention of logs to ensure activities are recorded for detecting and investigating potential security incidents.
- 9. Email and Web Browser Protections: Identify vulnerabilities in email systems and web browsers that could be exploited through phishing or malicious downloads, ensuring configurations minimize the risk of malware.
- 10. Malware Defenses: Scan for the absence of malware protection systems or configurations that could allow malware to infiltrate or spread within an organization network.
- 11. Data Recovery: While not directly scannable, ensure backup solutions are in place and secure, protecting against data loss and facilitating recovery in the event of a cyber incident.
- 12. Network Infrastructure Management: Identify vulnerabilities in network devices and infrastructure, ensuring they are securely configured and managed to protect against unauthorized access and attacks.
- 13. Security Configuration of Network Devices: Scan for misconfigurations in firewalls, routers, and switches that could be exploited to bypass security measures.

Profile 20 – CMMC Level 1 Compliance Scan

AC.1.001	Limit access to FCI to authorized users	Human
AC.1.002	Limit operations to least privilege	Human
AC.1.003	Control external system connections	Scannable
AC.1.004	Protect publicly posted information	Human
IA.1.076	Track system users and devices	Scannable
IA.1.077	Verify identity before granting access	Human
MP.1.118	Sanitize or destroy media before disposal	Human
PE.1.131	Restrict physical access to systems	Human
PE.1.132	Escort and monitor visitors	Human
PE.1.133	Maintain physical access logs	Human
PE.1.134	Control physical access devices	Human
SC.1.175	Protect communications at boundaries	Scannable
SC.1.176	Isolate subnetworks for FCI	Scannable
SI.1.210	Identify and correct system flaws	Scannable
SI.1.211	Use malware protection on systems	Scannable
SI.1.212	Keep malware protections updated	Scannable
SI.1.213	Perform periodic and real-time scans	Scannable

Vulnerability Scanner

Profile 21 – DORA Compliance Scan

- Ensures compliance with the EU Digital Operational Resilience Act (DORA) for financial entities and ICT service providers.
- This profile focuses on identifying vulnerabilities, misconfigurations, and ICT risks to align with DORA's requirements for operational resilience and risk management.
- Vulnerability Scanner Checks:
- System Vulnerabilities: Scan for weaknesses in ICT systems that could be exploited by attackers.
- Access Control Validation: Identify misconfigured or overly permissive access controls.
- Incident Reporting Readiness: Detect gaps in log collection, retention, and incident response configurations.
- Third-Party Risks: Scan for vulnerabilities in integrations with ICT service providers.
- Patch Management: Identify outdated or missing patches that could lead to exploits.
- Network Monitoring Gaps: Assess network configurations for potential monitoring blind spots.
- Human Actions (Consultant Required):
- Policy Development: Craft incident response, risk management, and operational resilience policies tailored to the organization.
- Third-Party Risk Assessments: Conduct in-depth reviews of vendor contracts, security measures, and operational dependencies.
- Governance Reviews: Ensure that DORA compliance efforts align with the organization's business strategy and regulatory obligations.
- Simulated Tests: Perform hands-on resilience tests, such as tabletop exercises or cyberattack simulations.
- Regulatory Reporting: Assist in preparing reports required by DORA regulatory authorities.

Profile 22 – GLBA Integrity Compliance

- 1. Access Controls: Scan for improper access control configurations that could allow unauthorized access to customer financial information, ensuring that access is restricted to authorized personnel only based on the principle of least privilege.
- 2. Data Encryption: Identify areas where financial data is transmitted or stored without adequate encryption, ensuring data is protected both in transit and at rest to prevent unauthorized access or disclosure.
- 3. Change Management: Check for vulnerabilities related to inadequate change management procedures, ensuring all changes to information systems are logged, reviewed, and authorized to maintain data integrity.
- 4. Network Security: Identify weaknesses in network security configurations that could allow unauthorized access or data breaches, ensuring firewalls, intrusion detection systems, and other security measures are properly configured and up to date.
- 5. Vulnerability Management: Detect outdated systems, software, and applications that could contain vulnerabilities, verifying that regular vulnerability scanning and patch management processes are in place to address potential security issues.
- 6. Incident Response and Monitoring: Assess the effectiveness of incident response plans and monitoring systems for detecting and responding to security incidents that could impact the integrity of customer financial information.
- 7. Secure Software Development and Acquisition: Scan for vulnerabilities in applications handling customer financial information, ensuring they are developed securely or assessed for security before integration into IT environments.
- 8. Third-party Service Provider Oversight: Evaluate security measures and controls of third-party service providers with access to customer financial information, ensuring they comply with GLBA requirements to protect data integrity.
- 9. Disposal of Customer Information: While not directly scannable, ensure policies and procedures are in place for the secure disposal of customer financial information, preventing unauthorized access to data no longer in use.
- 10. User Authentication: Check for weak authentication mechanisms that could allow unauthorized access to systems containing customer financial information, ensuring strong authentication methods are employed.
- 11. Data Integrity Measures: Identify the absence of data integrity controls, such as checksums or digital signatures, which are necessary to ensure that financial information has not been altered or tampered with.
- 12. Audit Trails: Verify that systems maintain audit trails for accessing and modifying customer financial information, ensuring accountability and the ability to detect unauthorized changes.

Vulnerability Scanner

Profile 23 – FFIEC Compliance

- Ensures compliance with the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, covering critical areas for financial institutions.
- **Scope:** Comprehensive scan covering all critical systems and applications within the organization.
- **Key Checks:**
- - Access Controls: Verify proper access controls to ensure only authorized personnel have access to sensitive financial data.
- - Authentication Mechanisms: Assess the strength and implementation of authentication methods.
- - Data Encryption: Ensure encryption of sensitive financial data both in transit and at rest.
- - Patch Management: Identify outdated systems and missing security patches.

Profile 24 – CyberScope Compliance

- Ensures compliance with CyberScope reporting requirements for federal agencies.
- This profile focuses on identifying misconfigurations, vulnerabilities, and non-compliance with best practices in federal information systems to meet CyberScope compliance requirements.
- Key Checks:
- - Configuration Management: Assess the configurations of systems and applications for compliance.
- - Vulnerability Scanning: Perform regular vulnerability scans and ensure timely remediation.
- - Access Control: Check for proper implementation of access controls and user authentication.
- - Continuous Monitoring: Ensure continuous monitoring of systems and networks.
- - Patch Management: Identify and remediate missing patches and outdated software..

Vulnerability Scanner

Profile 25 – NERC Compliance

- Targets compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.
- This profile focuses on systems and assets critical to the operation of the bulk electric system.
- Key Checks:
- - Access Control: Verify strict access controls to critical cyber assets.
- - Systems Security Management: Check for secure configuration and management of critical systems.
- - Information Protection: Ensure sensitive information is protected against unauthorized access.
- - Configuration Change Management: Assess the processes for managing changes to critical systems.

Profile 26 – SCAP Compliance

- Ensures compliance with the Security Content Automation Protocol (SCAP) for automating vulnerability management and compliance.
- This profile focuses on comprehensive scan of all systems and applications for SCAP compliance.
- Key Checks:
- - Vulnerability Scanning: Perform SCAP-compliant vulnerability scans.
- - Patch Management: Identify and remediate missing security patches.
- - Configuration Management: Assess configurations against SCAP benchmarks.
- - Continuous Monitoring: Ensure continuous monitoring for vulnerabilities and compliance.
- - Reporting: Generate SCAP-compliant reports for auditing and compliance purposes.
- - Security Automation: Ensure automation of security checks and remediation processes.

Vulnerability Scanner

Profile 27 – SOX Compliance

- Ensures compliance with the Sarbanes-Oxley Act (SOX) for protecting financial data integrity and accuracy.
- This profile focuses on systems and processes related to financial reporting.
- Key Checks:
- - Access Controls: Verify proper access controls to financial reporting systems.
- - Data Integrity: Check for mechanisms to ensure the integrity and accuracy of financial data.
- - Change Management: Assess processes for managing changes to financial systems and data.
- - User Authentication: Evaluate the strength and implementation of user authentication mechanisms.
- - Vendor Management: Assess the security measures and controls of third-party service providers handling financial data.

Profile 28 – CERT Compliance

- Ensures compliance with the Computer Emergency Response Team (CERT) standards for handling and mitigating security incidents.
- This profile focuses on comprehensive scan covering all critical systems and applications.
- Key Checks:
- - Incident Detection: Ensure proper mechanisms are in place for detecting security incidents.
- - Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation.
- - Configuration Management: Assess the configurations of systems and applications for compliance.
- - Access Control: Verify strict access controls and user authentication mechanisms.

Vulnerability Scanner

Profile 29 – COBIT/ITIL Compliance

- Ensures compliance with the Control Objectives for Information and Related Technologies (COBIT) and Information Technology Infrastructure Library (ITIL) standards for IT governance and management.
- This profile focuses on IT governance, risk management, and service management processes.
- Key Checks:
- - Access Controls: Verify proper access controls to critical IT systems.
- - Configuration Management: Ensure secure configurations of IT systems and applications.
- - Compliance Monitoring: Ensure continuous monitoring of compliance with COBIT and ITIL standards.

Profile 30 – DISA STIGs Compliance Scan

- Ensures compliance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) for securing Department of Defense (DoD) systems.
- This profile focuses on comprehensive scan of systems and applications for compliance with DISA STIGs.
- Key Checks:
- - Access Controls: Verify strict access controls to DoD systems.
- - Configuration Management: Assess configurations against DISA STIGs benchmarks.
- - Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation.
- - Patch Management: Identify and remediate missing security patches.
- - Compliance Reporting: Generate reports to demonstrate compliance with DISA STIGs.

Vulnerability Scanner

Profile 31 – FDCC Compliance Scan

- Ensures compliance with the Federal Desktop Core Configuration (FDCC) standards for securing federal desktops and laptops.
- This profile focuses on desktop and laptop configurations within federal agencies.
- Key Checks:
- - Configuration Management: Assess configurations of desktops and laptops against FDCC benchmarks.
- - Access Controls: Verify proper access controls to federal desktops and laptops.
- - Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation.
- - Patch Management: Identify and remediate missing security patches.
- - Compliance Reporting: Generate reports to demonstrate compliance with FDCC standards.

Profile 32 – NSA Compliance Scan

- Ensures compliance with National Security Agency (NSA) guidelines for securing national security systems.
- This profile focuses on comprehensive scan of systems and applications for compliance with NSA guidelines.
- Key Checks:
- - Access Controls: Verify strict access controls to national security systems.
- - Configuration Management: Assess configurations against NSA guidelines.
- - Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation.
- - Patch Management: Identify and remediate missing security patches.
- - Data Encryption: Ensure encryption of sensitive national security data.
- - Compliance Reporting: Generate reports to demonstrate compliance with NSA guidelines.

Vulnerability Scanner

Profile 33 – NIS2 Compliance Scan

- Ensures compliance with the Network and Information Security (NIS2) Directive for enhanced cybersecurity across essential and important sectors in the EU.
- Focuses on technical safeguards for systems supporting critical infrastructure.
- Risk Management: Scan for misconfigurations, vulnerabilities, and outdated systems.
- Incident Response: Verify IDS/IPS alerts and logging of security events.
- Network Security: Review firewall rules, open ports, and network exposure.
- Access Control: Identify weak credentials & verify use of MFA.
- Encryption: Check SSL/TLS configurations & detect unencrypted data.
- Patch Management: Detect missing security updates & outdated software.
- Supplier Risk: Scan third-party systems for insecure configs.
- Monitoring: Ensure proper logging and monitoring is in place.
- System Hardening: Detect default settings, weak encryption, & excess services.

Vulnerability Scanner Report Languages

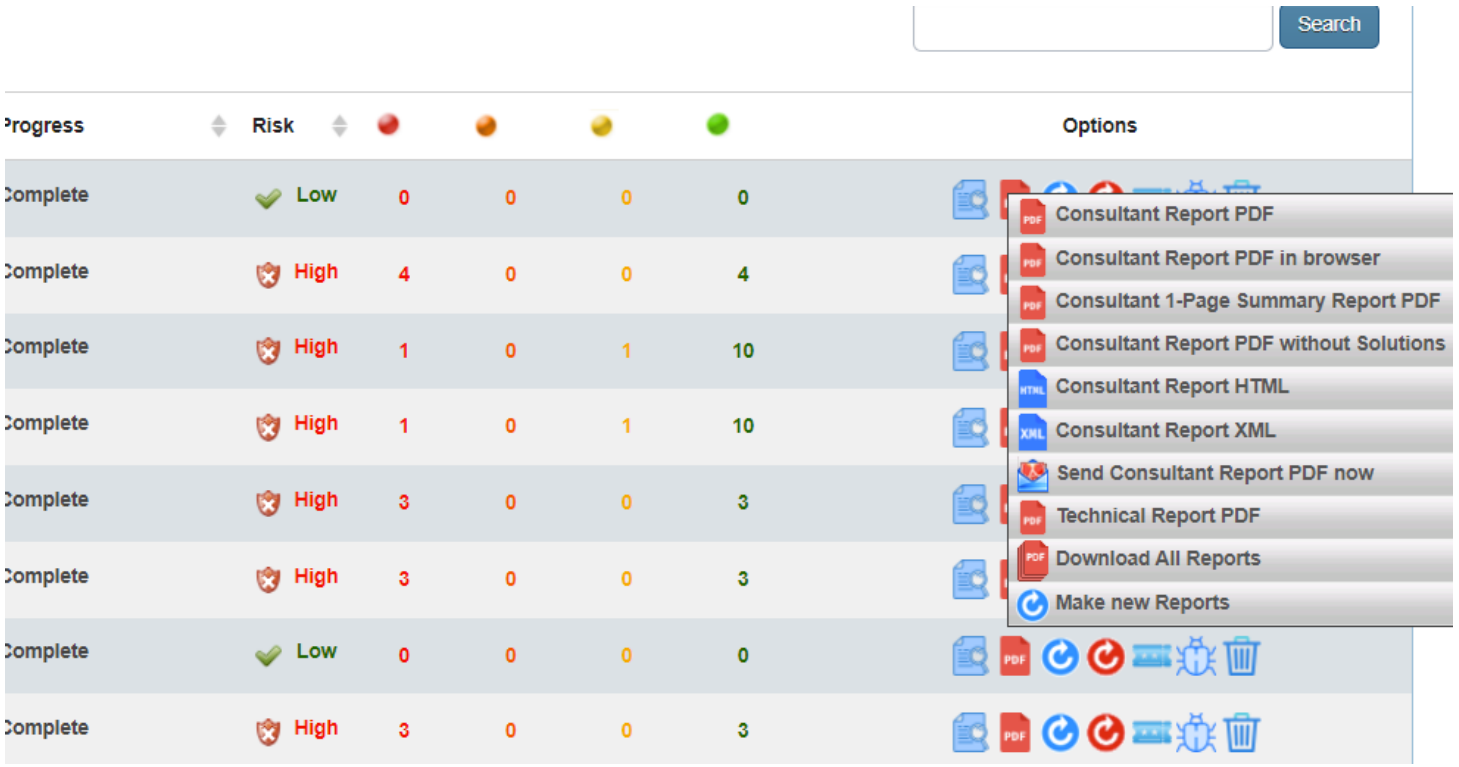
Multilingual Reports

- 1. Arabic (العربية)
- 2. Chinese Simplified (简体中文)
- 3. Croatian (Hrvatska)
- 4. Danish (Dansk)
- 5. Dutch (Nederlands)
- 6. English
- 7. French (Français)
- 8. Georgian (ქართული)
- 9. German (Deutsch)
- 10. Greek (Ελληνικά)
- 11. Hindi (हिंदी)
- 12. Indonesian (Bahasa Indonesia)
- 13. Italian (Italiano)
- 14. Japanese (日本語)

Available in 26 Languages

- 15. Korean (한국의)
- 16. Macedonian (македонски јазик)
- 17. Norwegian (Norsk)
- 18. Polish (Polski)
- 19. Portuguese (Português)
- 20. Romanian (Română)
- 21. Russian (Русский)
- 22. Spanish (Español)
- 23. Swedish (Svenska)
- 24. Thai (ไทย)
- 25. Turkish (Türkçe)
- 26. Ukrainian (Українська)

Vulnerability Scanner & WiFi Pen Testing



reports are available in PDF HTML and comes as consultant, technical, executive, versions

https://Penetrator.SecPoint.com/spscan/new_scan.php

SECPOINT
www.secpoint.com

Vulnerability Scanner & WiFi Pen Testing

SAMPLE VULNERABILITY SCANNING Summary Report

http://www.SecPoint.com/manual/Penetrator_Example_Audit_Summary.pdf

SECPOINT® www.secpoint.com

Scan Summary Report

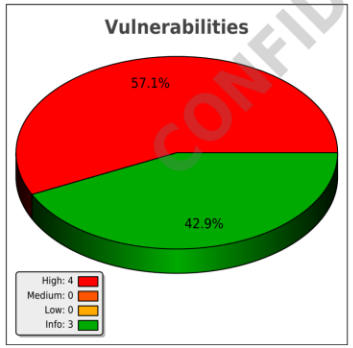
Confidential

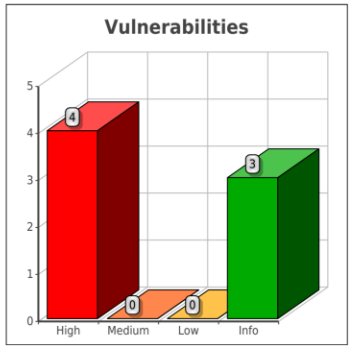
Scan Name		**Audited on**	[redacted]
Scan Profile	Best Scan		
Scan Engine	[redacted]	**Firmware Version**	[redacted]
Audited Targets			

Overall Risk Level: High (Critical Level). Your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data.
It is recommended that you take immediate action to improve the security level.

Compliance result: The Scan is Not Compliant

Vulnerabilities: 7 potential vulnerabilities identified, with the following risk levels:
High: 4
Medium: 0
Low: 0
Information: 3



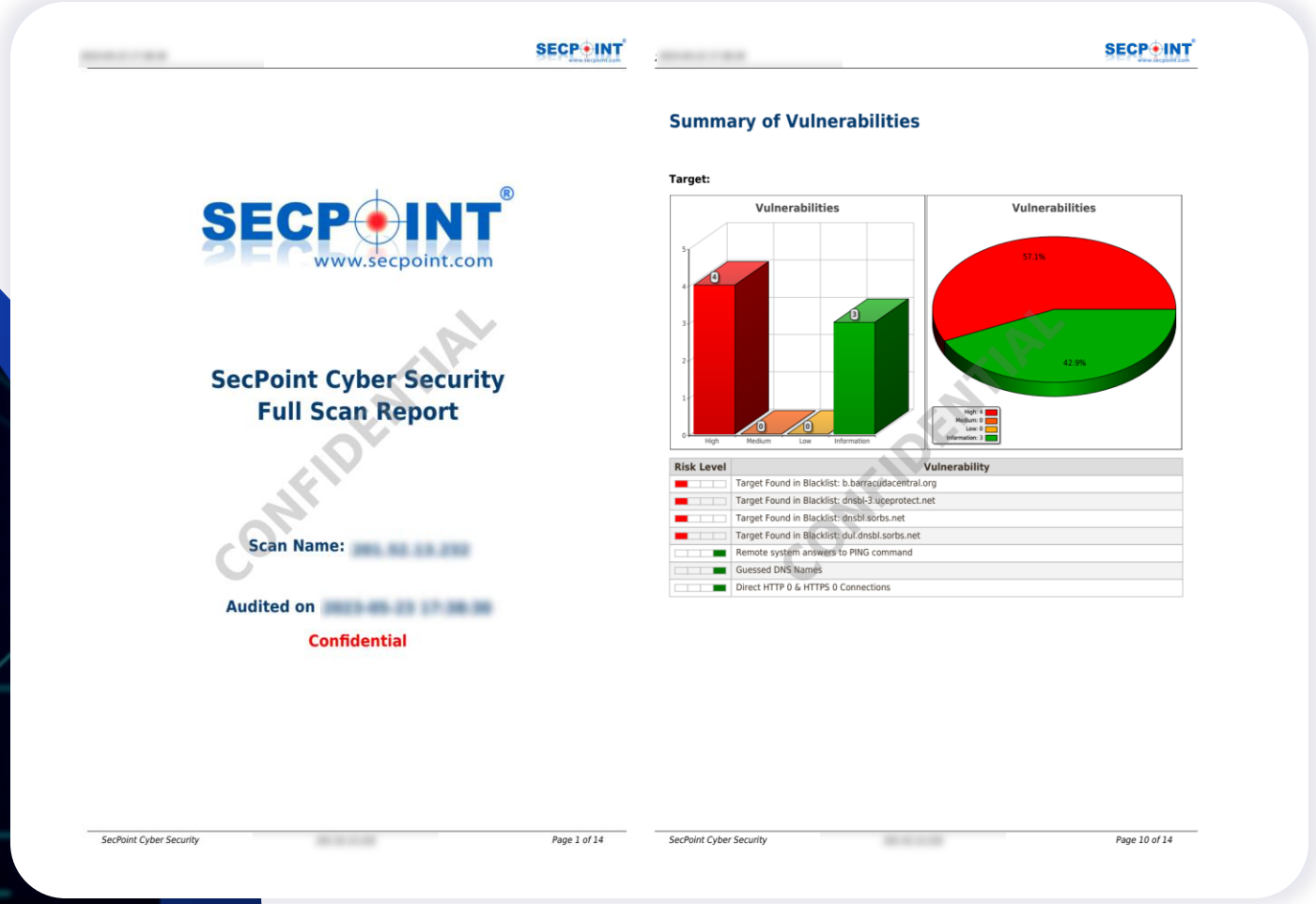


If you wish to view a detailed report of your scan or change your scan details, you can login to your SecPoint® Penetrator

Vulnerability Scanner & WiFi Pen Testing

SAMPLE VULNERABILITY SCANNING FULL Report

http://www.SecPoint.com/manual/Penetrator_Example_Audit.pdf



SECPOINT
www.secpoint.com

SecPoint Cyber Security
Full Scan Report

Scan Name:

Audited on

Confidential

SecPoint Cyber Security — Page 1 of 14

SECPOINT

Summary of Vulnerabilities

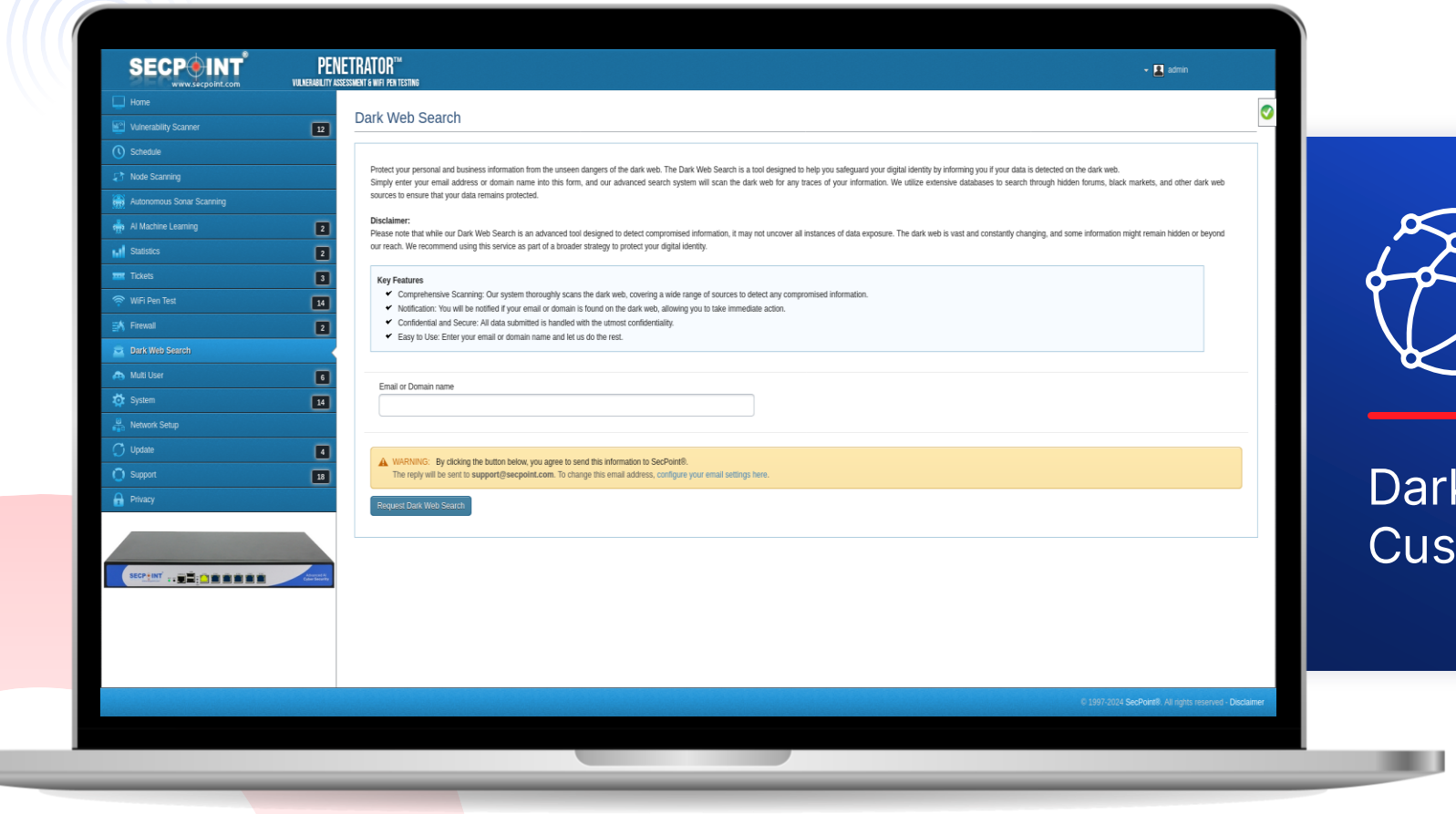
Target:

Risk Level	Vulnerability
	Target Found in Blacklist: b.barracudacentral.org
	Target Found in Blacklist: dnsbl-3.uceprotect.net
	Target Found in Blacklist: dnsbl.sorbs.net
	Target Found in Blacklist: dul.dnsbl.sorbs.net
	Remote system answers to PING command
	Guessed DNS Names
	Direct HTTP 0 & HTTPS 0 Connections

SecPoint Cyber Security — Page 10 of 14

SECPOINT
www.secpoint.com

Vulnerability Scanner & WiFi Pen Testing



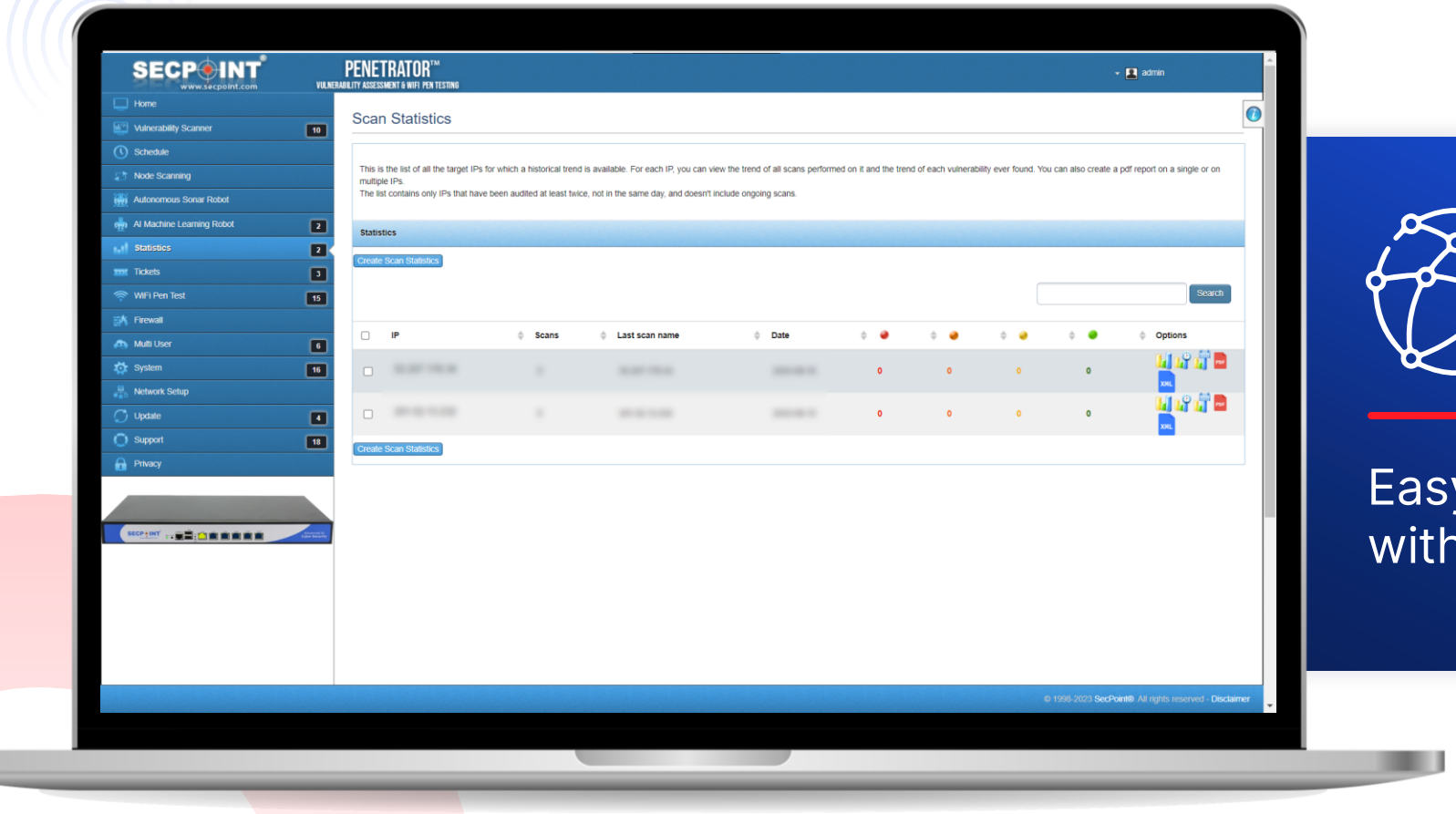
Dark Web Search 4.0 – Discover Customer Leaks

https://Penetrator.SecPoint.com/spscan/darkwebmon.php

CLICK!

SECPOINT®
www.secpoint.com

Vulnerability Scanner & WiFi Pen Testing



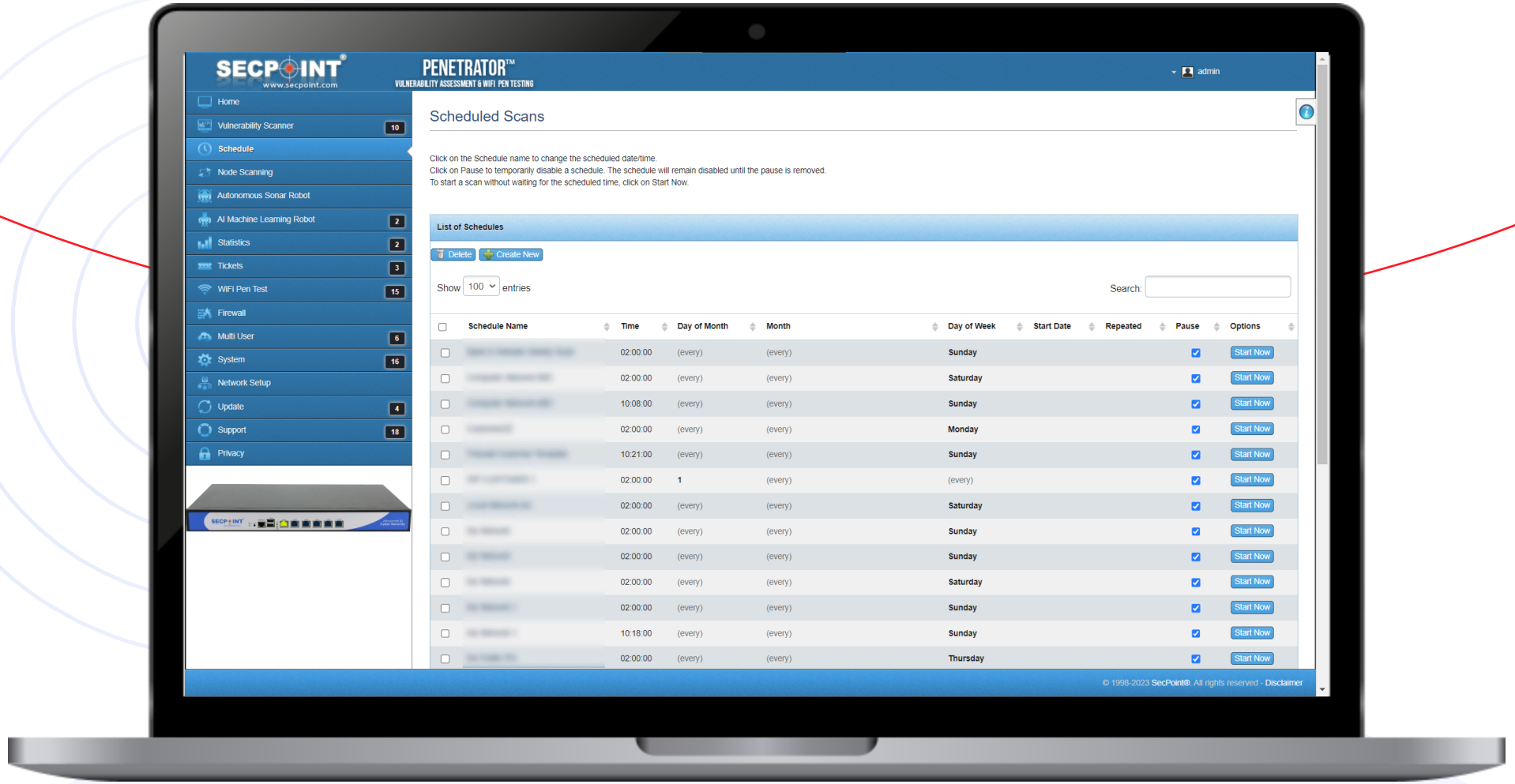
Easy to manage false positives with global false positive system

https://Penetrator.SecPoint.com/spscan/false_positives_scan.php

CLICK!

SECPOINT®
www.secpoint.com

Schedule

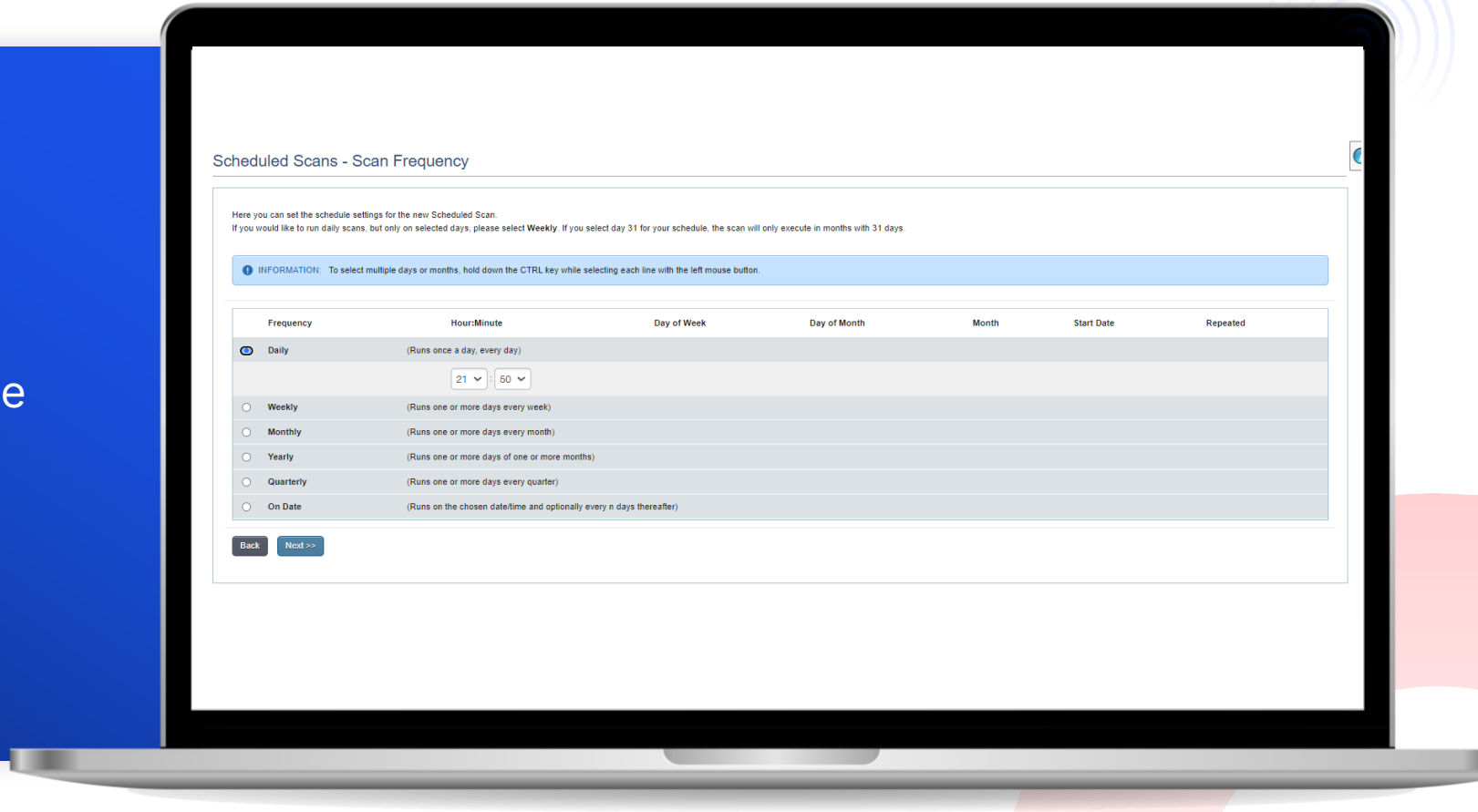


https://Penetrator.SecPoint.com/spscan/view_schedule.php

Schedule

Easy to setup scheduled scanning they can choose based on compliance

- Daily
- Weekly
- Monthly
- Yearly
- Quarterly
- on specific dates

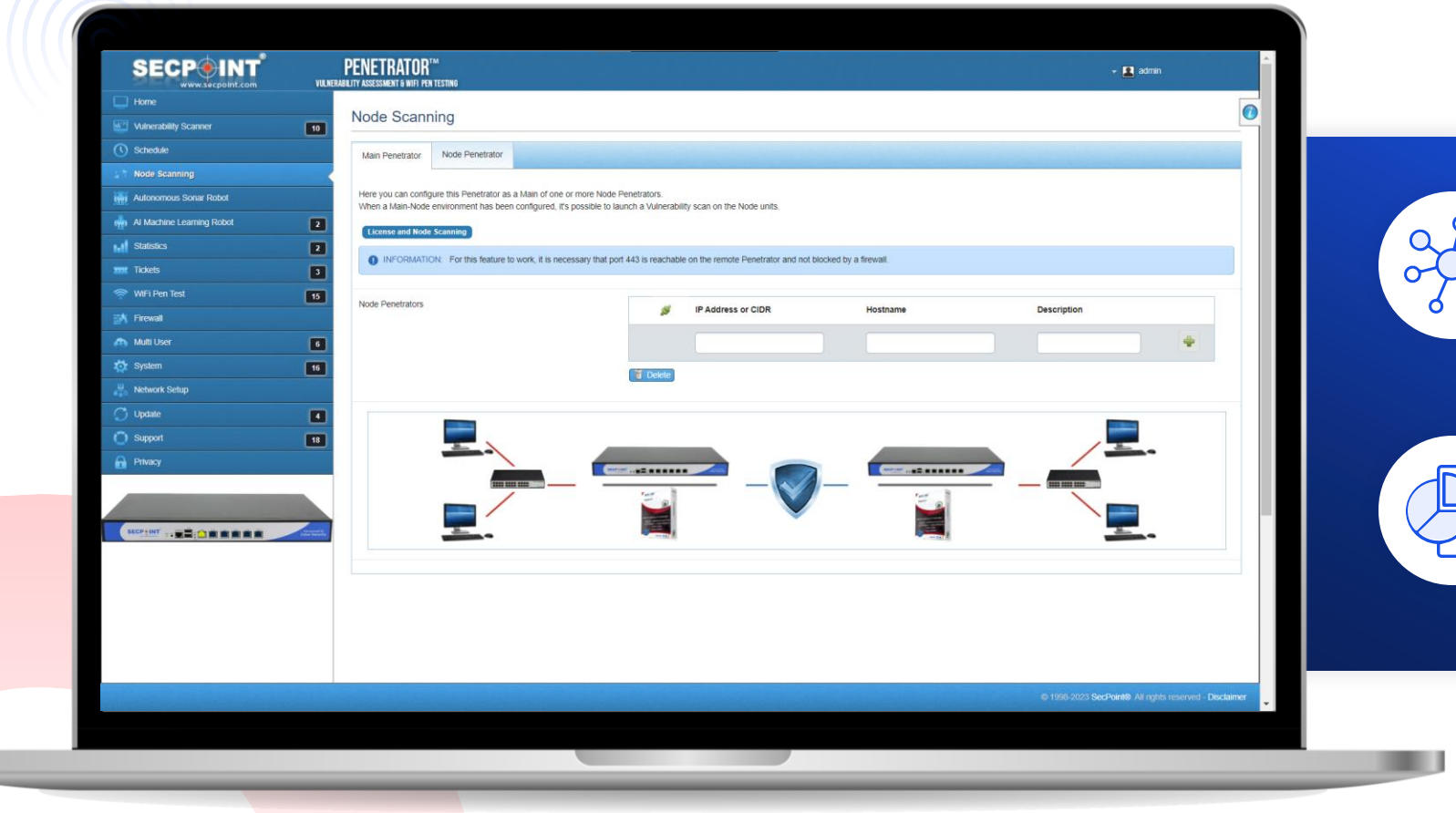


https://Penetrator.SecPoint.com/spscan/view_schedule.php

CLICK!

SECPOINT®
www.secpoint.com

Node Scanning



Allows to connect multiple software or appliances together in a distributed manner and do the scanning centralized.

Then all data and reporting will be centralized and allows for easy control from the admin

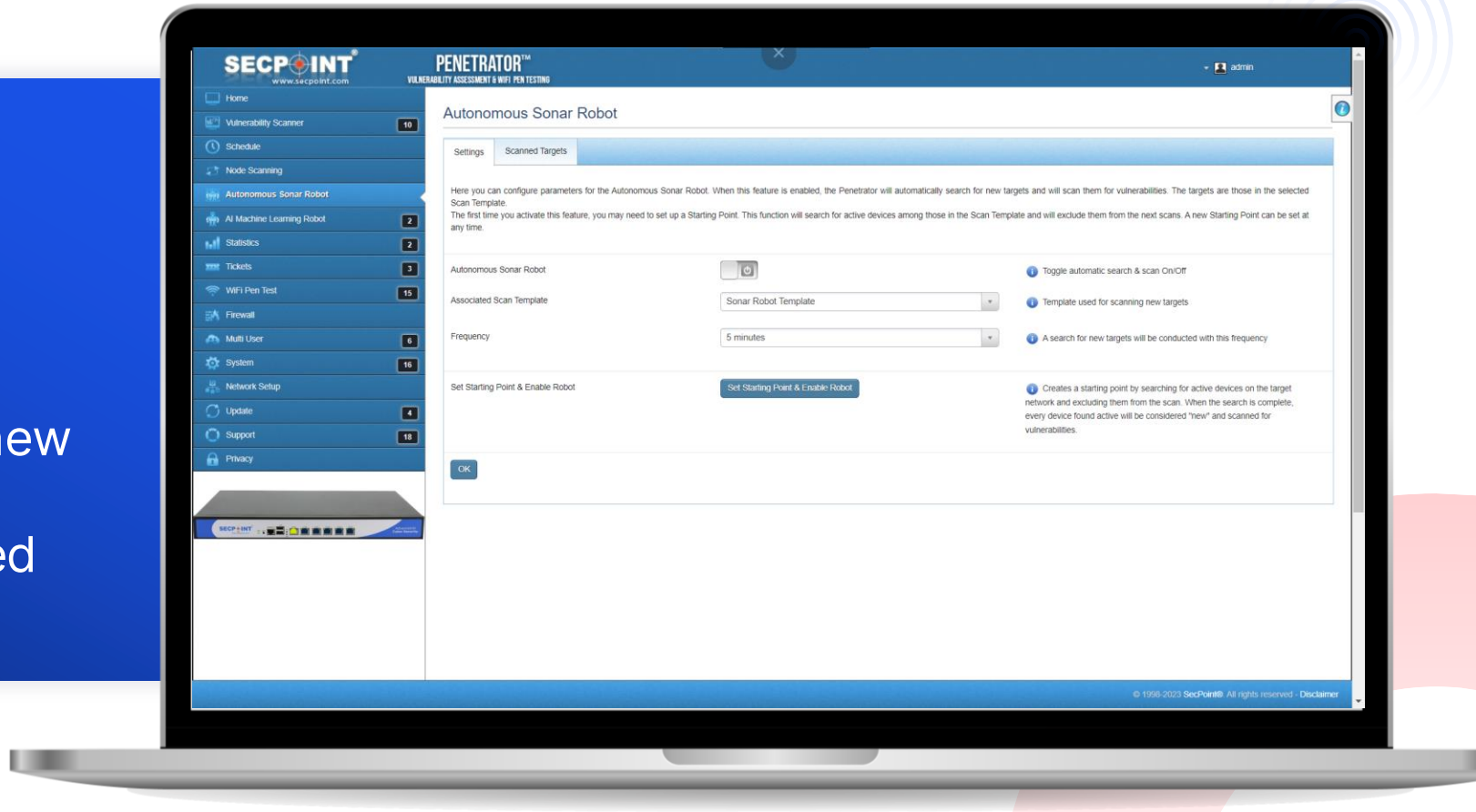
https://Penetrator.SecPoint.com/spscan/admin/distribution.php

CLICK!

SECPOINT
www.secpoint.com

Autonomous Sonar Robot

This allows Penetrator sweep network and automatically scan new devices and notify admin if new vulnerable devices gets connected

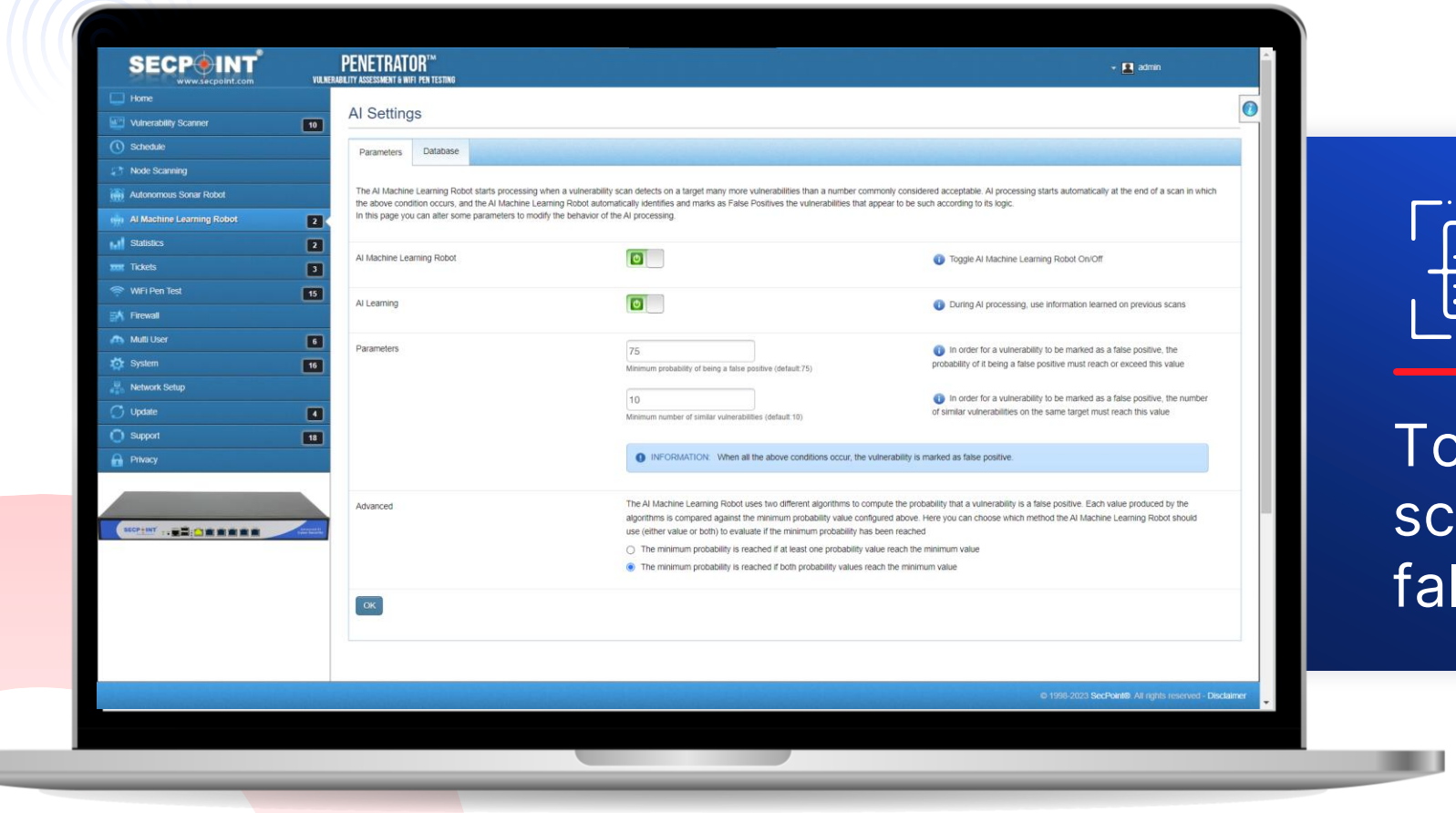


https://Penetrator.SecPoint.com/spscan/admin/sonar.php

CLICK!

SECPOINT®
www.secpoint.com

AI Machine learning



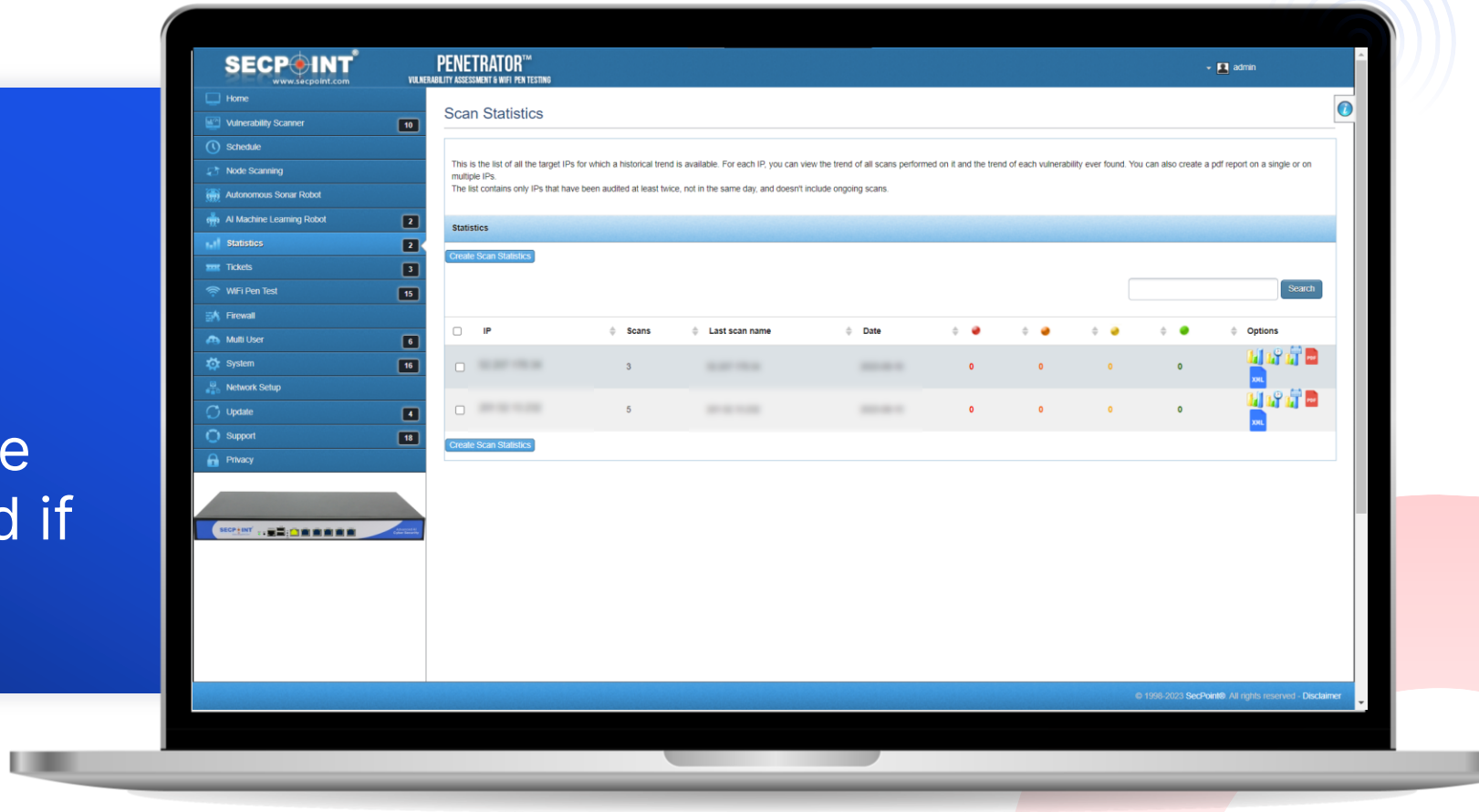
To allow for perfection of scans to automatic remove false positives

https://Penetrator.SecPoint.com/spscan/aisetup.php CLICK!

SECPOINT
www.secpoint.com

Statistics

The user can see over a time line vulnerabilities found and if new being discovered

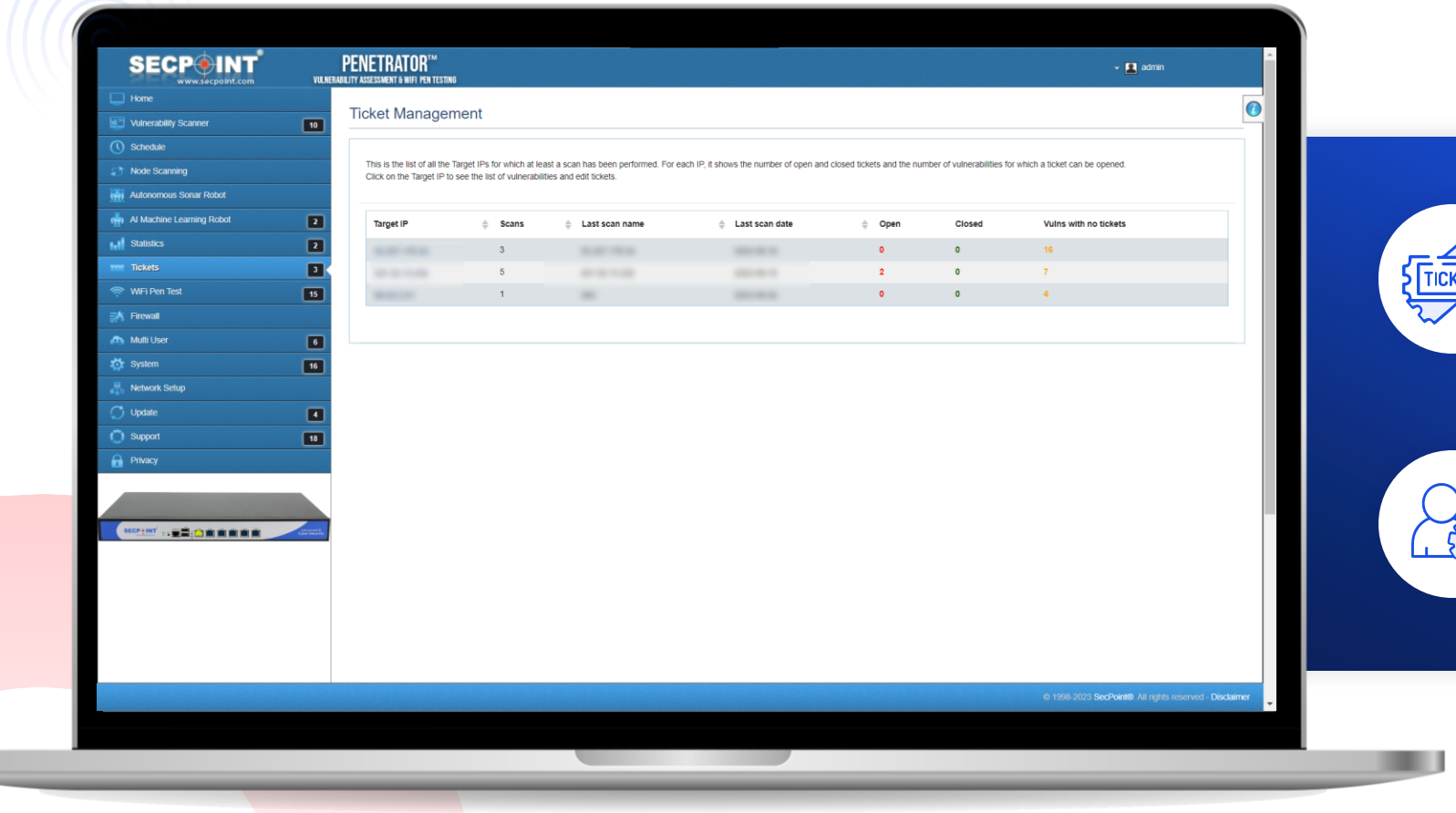


https://Penetrator.SecPoint.com/spscan/admin/sonar.php

CLICK!

SECPOINT
www.secpoint.com

Ticket system



The user set tickets for found vulnerabilities and assign their personell to fix them.

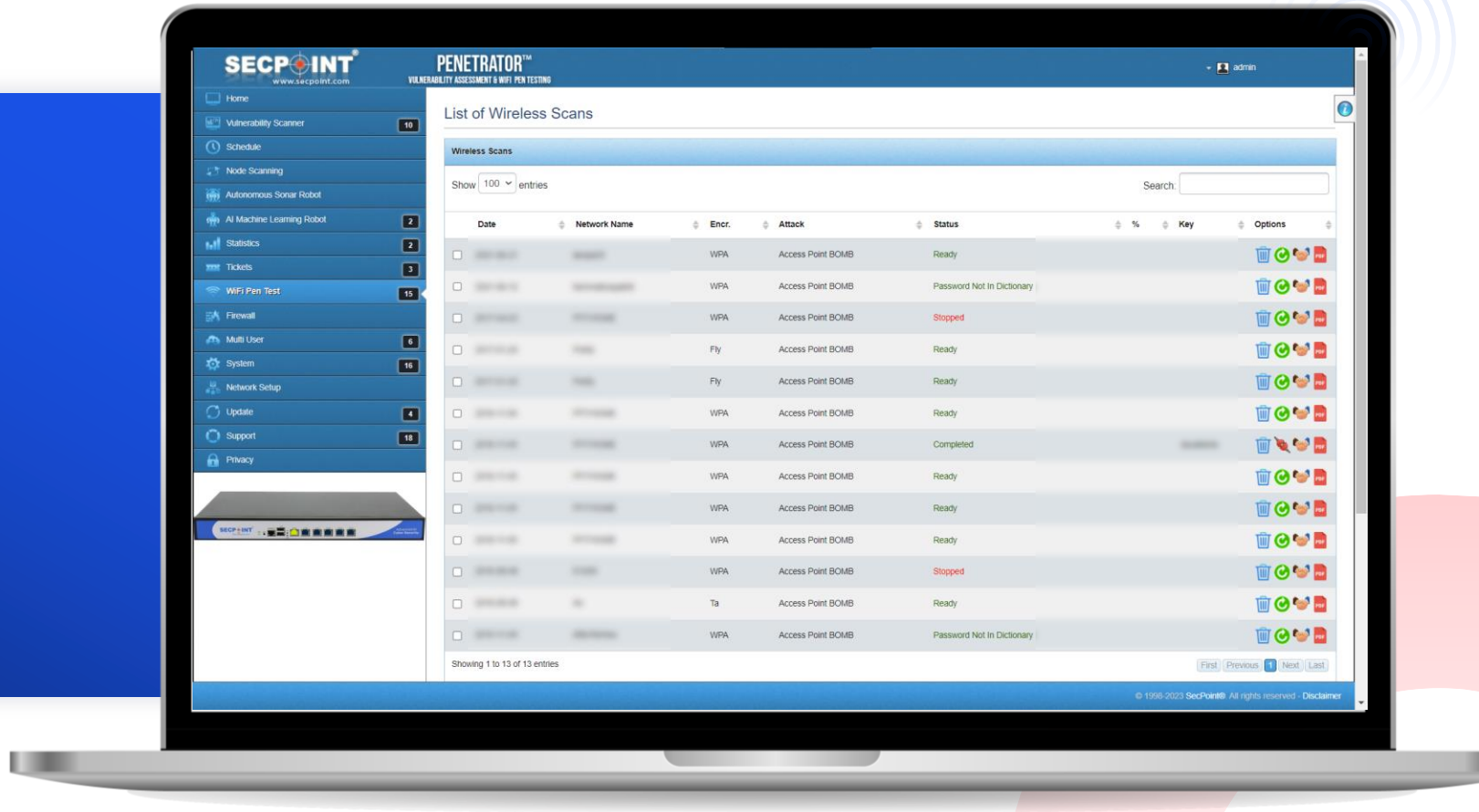
Then the admin can set deadlines on tickets and follow up vulnerabilities gets fixed

https://Penetrator.SecPoint.com/spscan/ticket.php?query=open_tickets

SECPOINT®
www.secpoint.com

WiFi Penetration Testing

The user can perform WIFI Pen testing and get professional reportingLaunch up to 7 different WIFI pen testing techniques

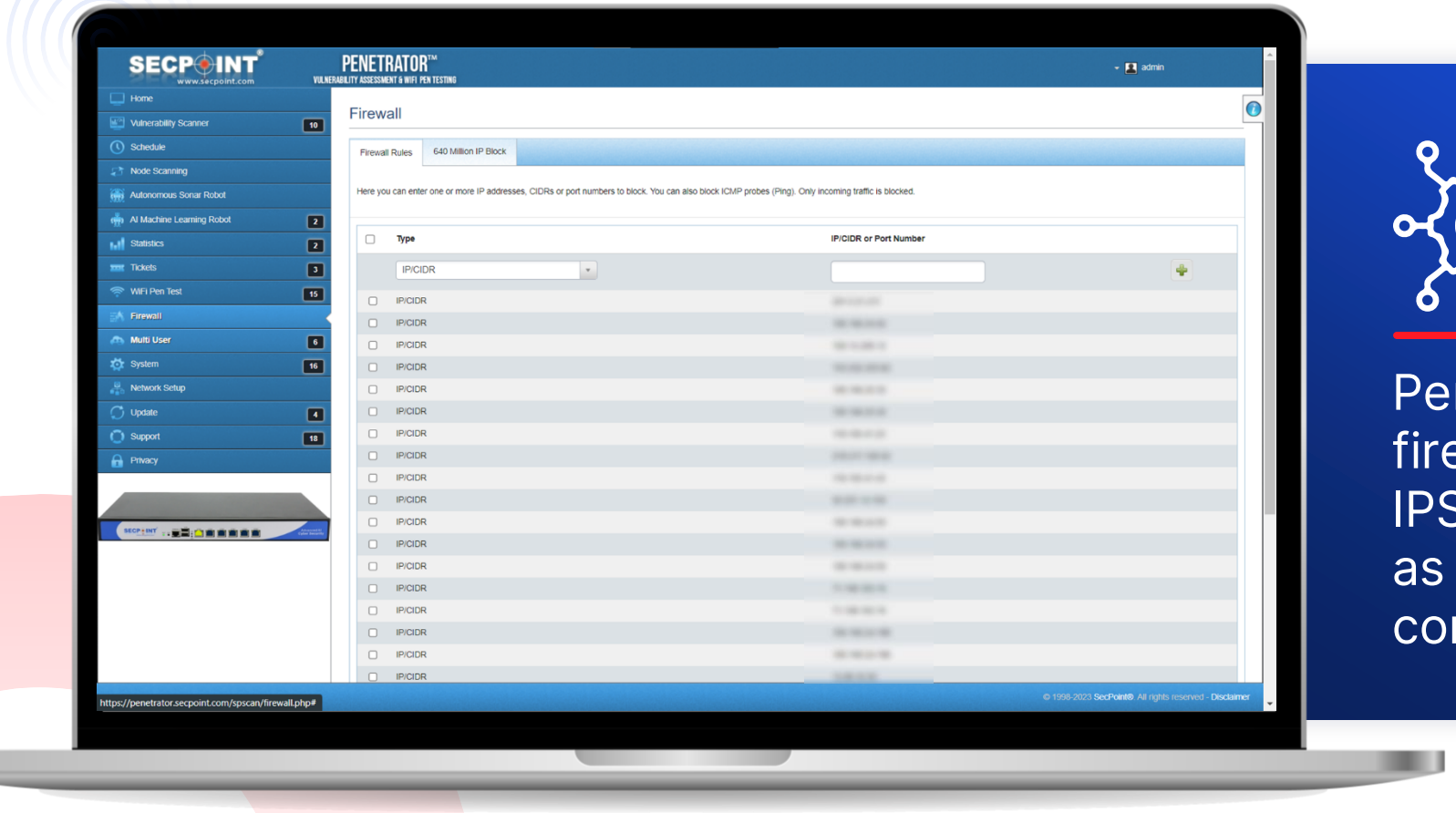


https://Penetrator.SecPoint.com/spscan/wireless.php

CLICK!

SECPOINT®
www.secpoint.com

Firewall



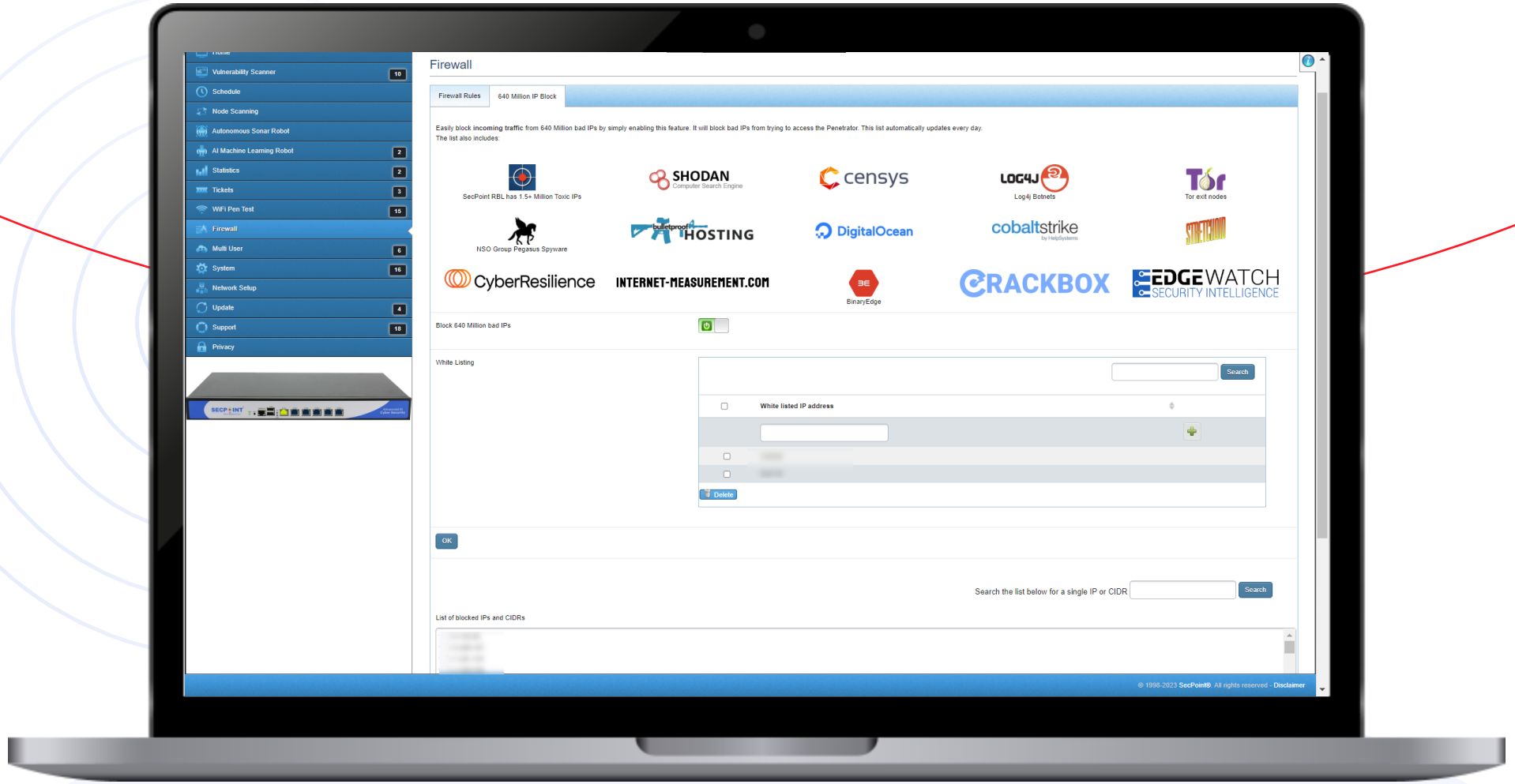
Penetrator™ has strong onboard firewall system to block attacks, toxic IPS to connect, specific attacks such as brute force , SQL injection, command execution and more

https://Penetrator.SecPoint.com/spscan/firewall.php

CLICK!

SECPOINT
www.secpoint.com

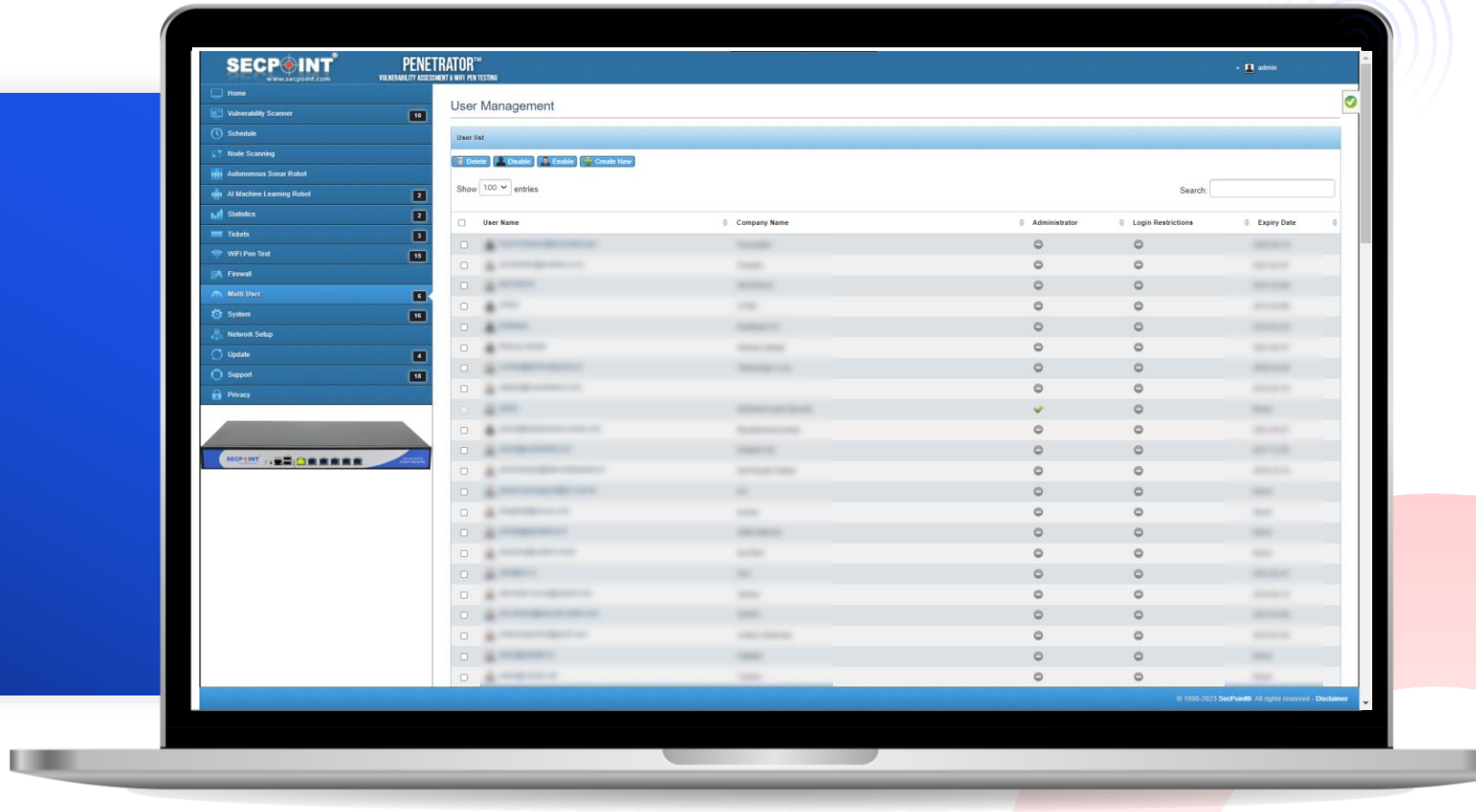
Firewall



SECPOINT®
www.secpoint.com

Multi User

Support and allows for MSP Managed service provider functionality

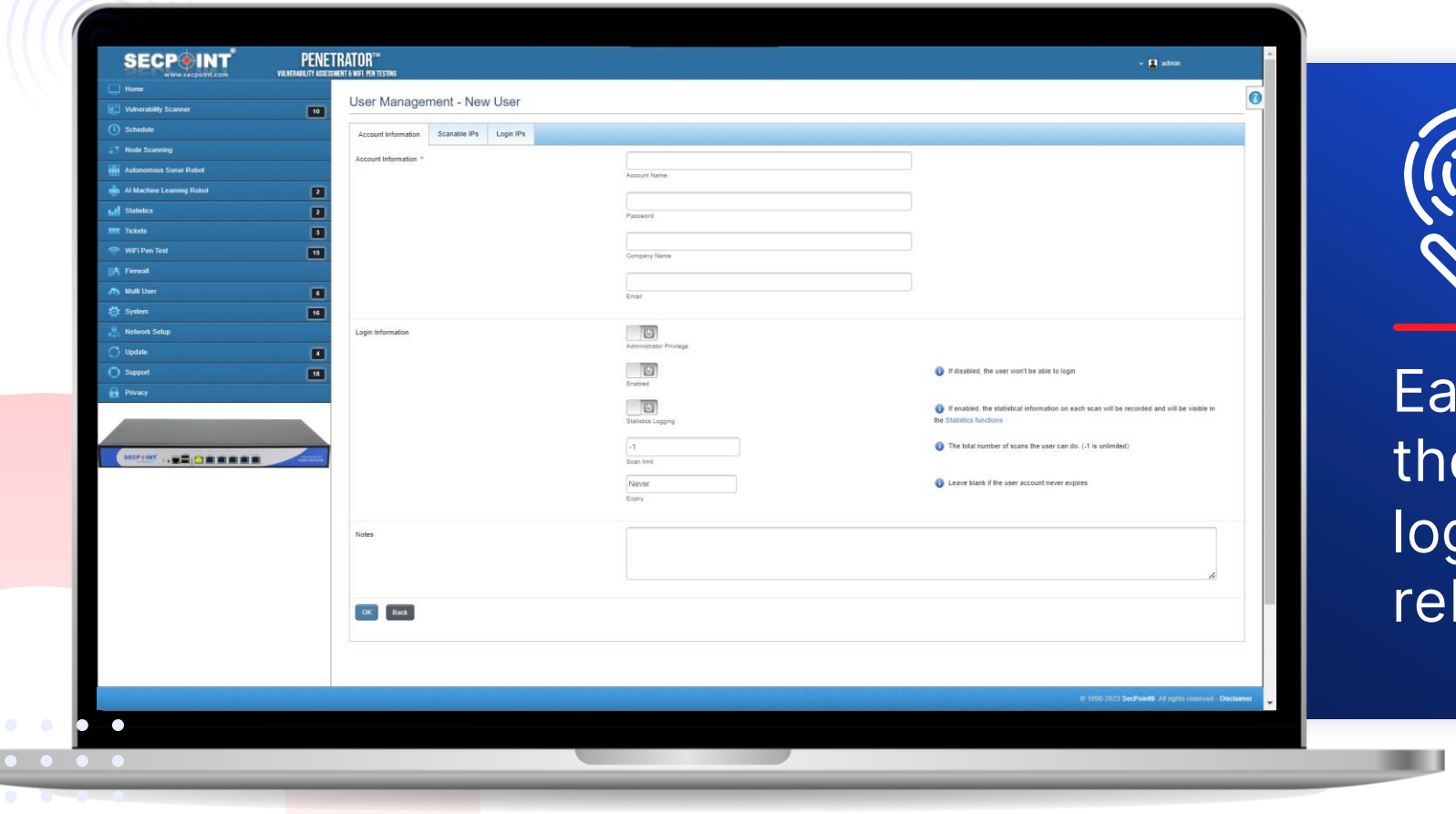


https://Penetrator.SecPoint.com/spscan/admin/user.php

CLICK!

SECPOINT
www.secpoint.com

Multi User

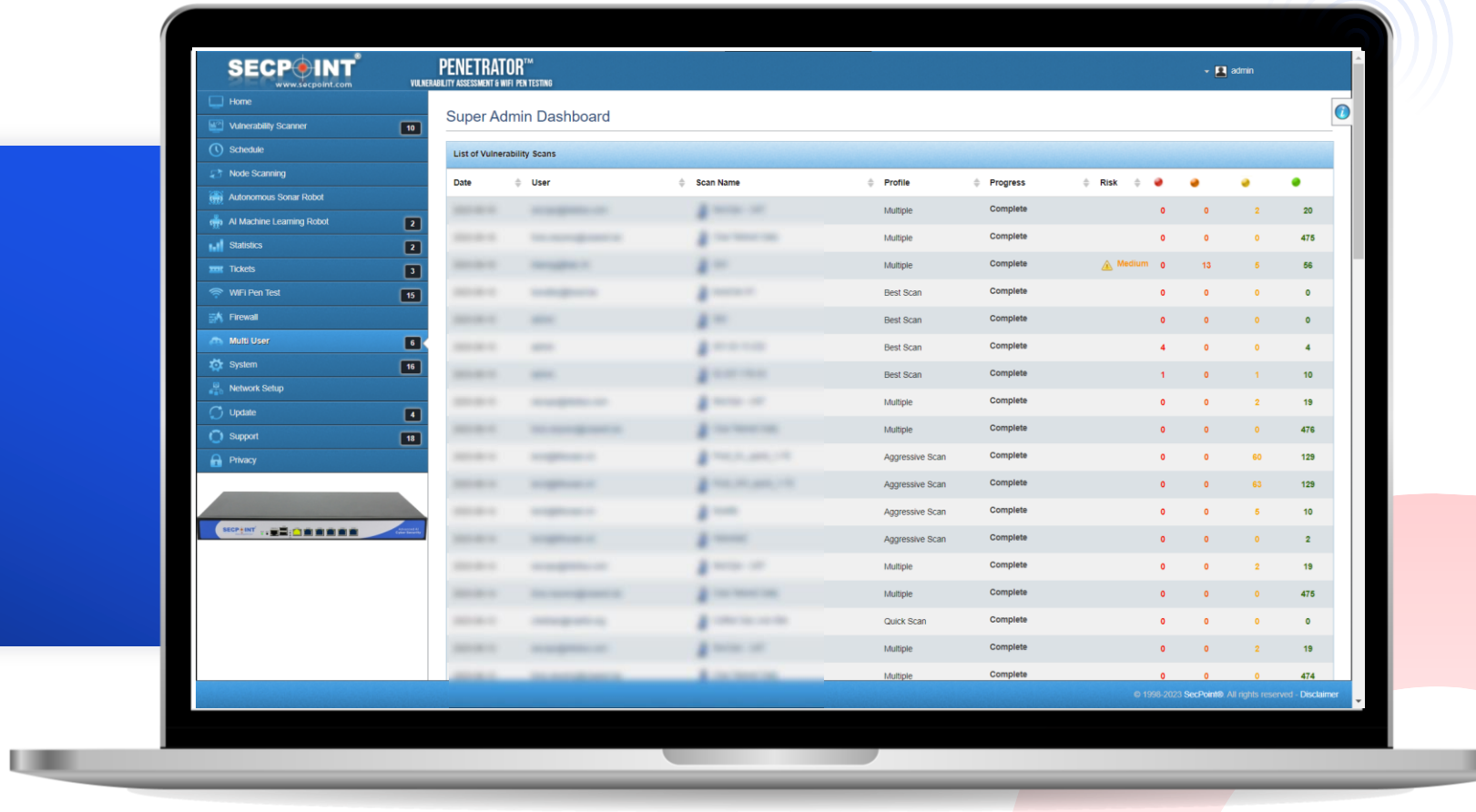


Easy create multiple users on the system and control their login and at interface brand rebrand to operate as a MSP

SECPOINT
www.secpoint.com

Multi User

The super admin allows for easy overview



https://Penetrator.SecPoint.com/spscan/admin/superadmin.php

CLICK!

SECPOINT®
www.secpoint.com

Multi User

MSP interface

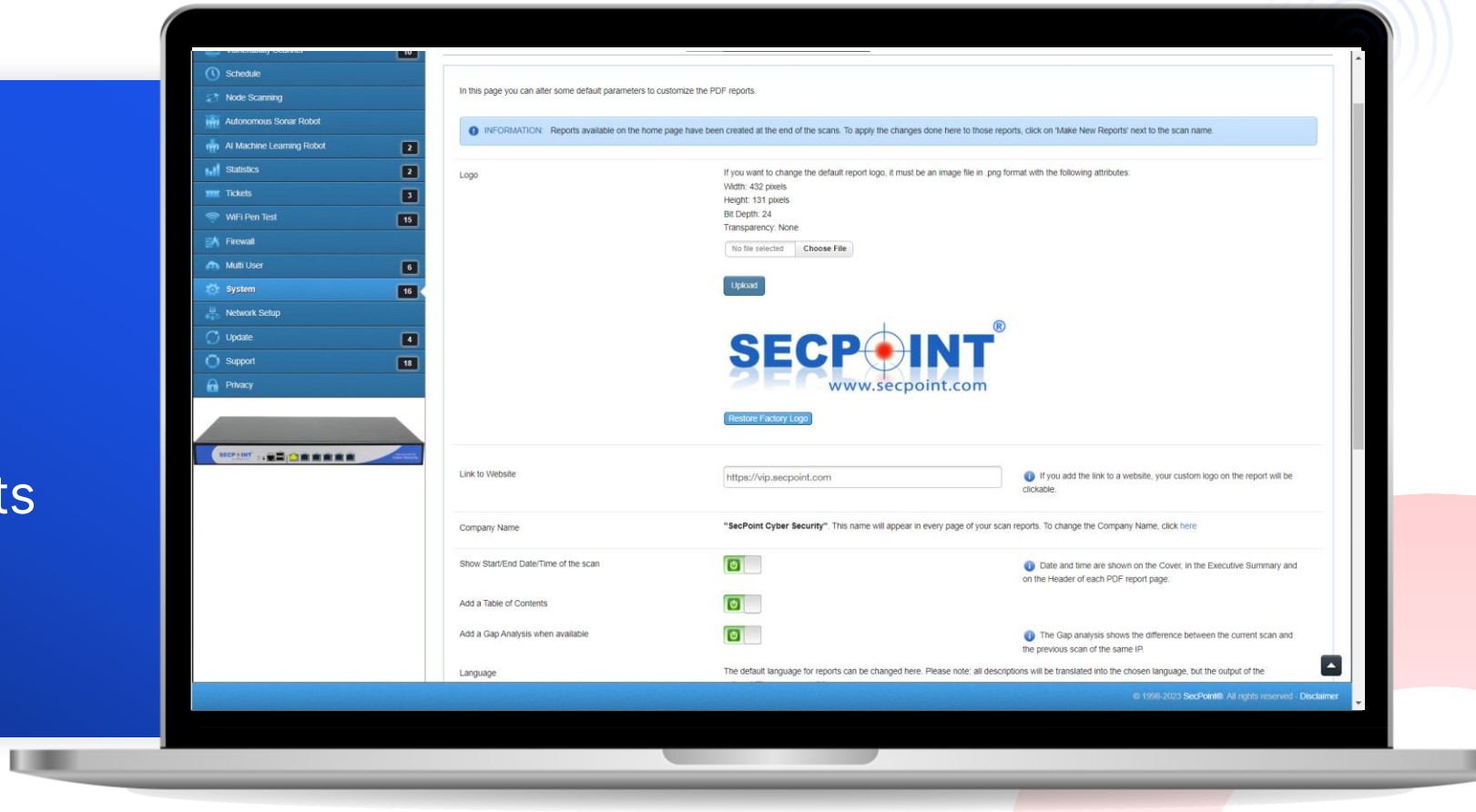
https://Penetrator.SecPoint.com/spscan/admin/branding.php

CLICK!

SECPOINT®
www.secpoint.com

Whitelabeling

It is possible on the Penetrator™ to rebrand reports with company name, logo, watermark and specific text



https://Penetrator.SecPoint.com/spscan/admin/change_logo.php

CLICK!

SECPOINT
www.secpoint.com

Whitelabeling

Available for both the software and the appliance versions

Allow users, resellers, integrators, consultants to customize the vulnerability scanning and WIFI penetration testing reporting on the system to fit their requirements or offer it as a service to their customers

Users can customize the logo in the report

User can set a custom watermark to appear on all pages. Company name can be customized

Supporting up to 26 languages

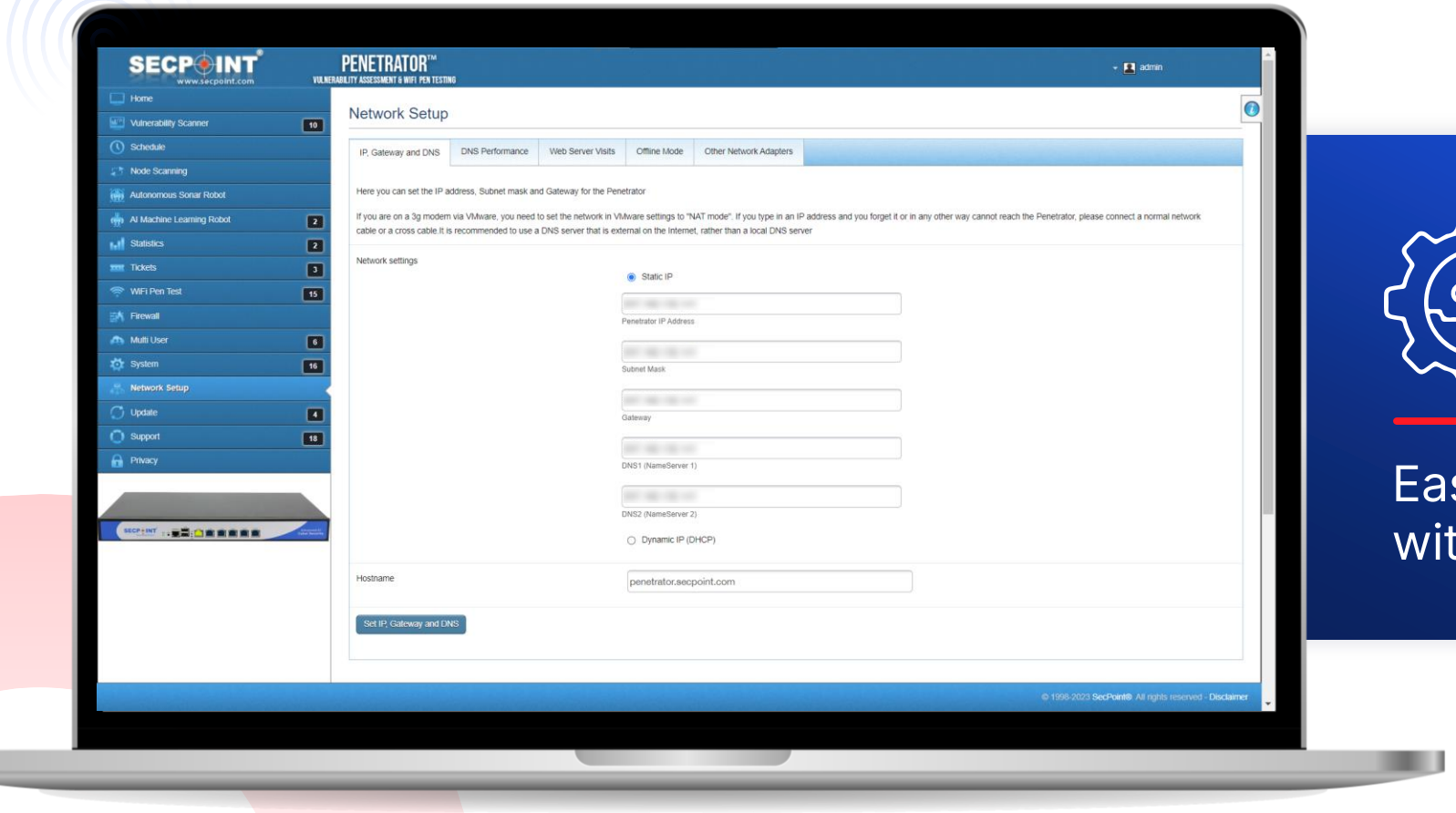
Use as a managed server MSP

Login logo and top logo in the interface can be customize to align with branding requirements

Support multiple user accounts with their own policies

Multi-Factor Authentication (MFA) supported for admin and individual users

Network Setup



Easy network setup DHCP/static IP with multiple network adapters

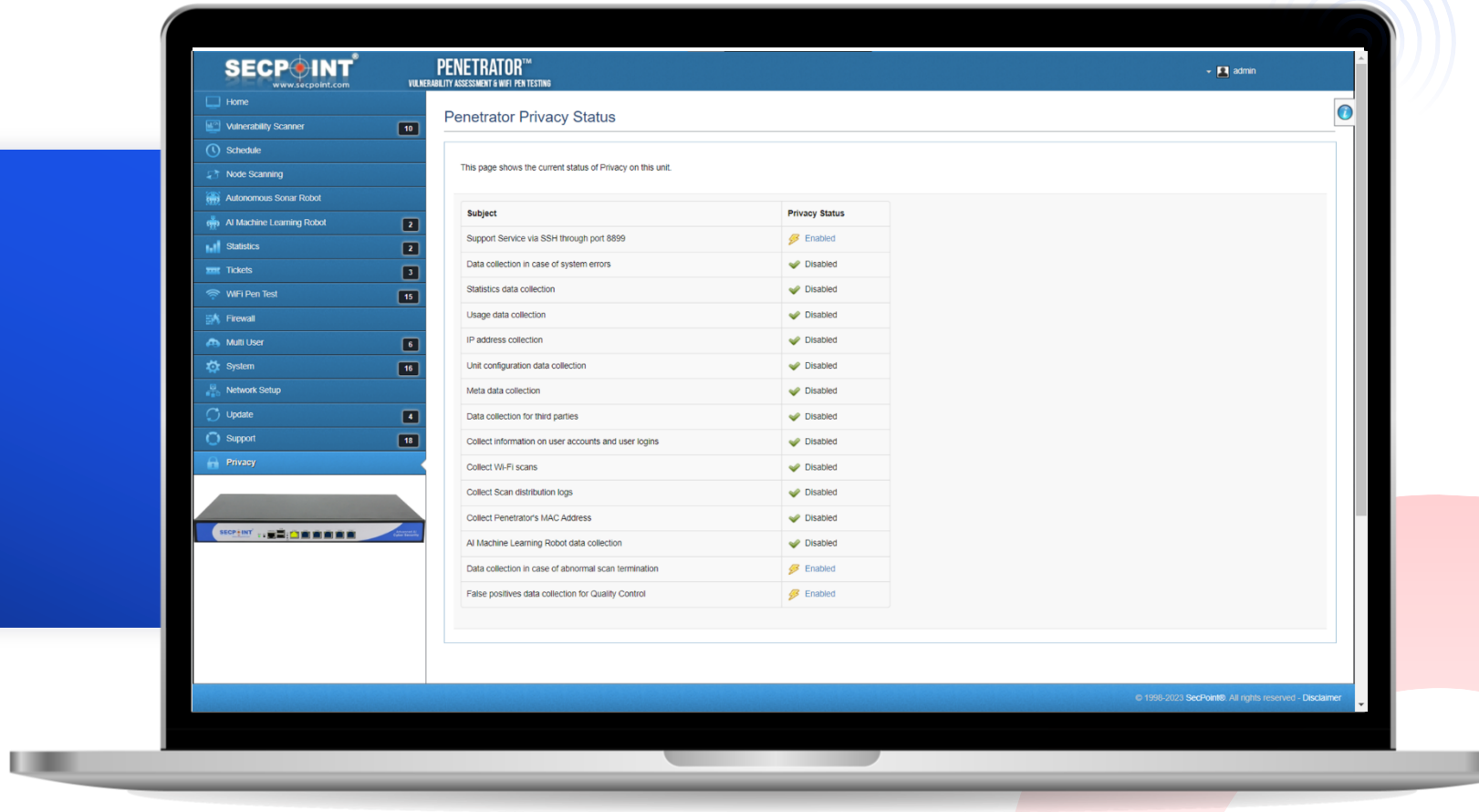
https://Penetrator.SecPoint.com/spscan/admin/network.php

CLICK!

SECPOINT
www.secpoint.com

Full Privacy Menu

Get full control about which data is being collected



https://Penetrator.SecPoint.com/spscan/admin/privacy.php

CLICK!

SECPOINT®
www.secpoint.com

Best product support

24 hour live chat

Ticket system

Support in

- Signal
- Telegram
- WhatsApp
- Skype

SECPOINT®
www.secpoint.com

Safe Trusted Ordering

Trustpilot

TrustScore **4.9** | **121** reviews

trust ECOMMERCE EUROPE

e-mærket

CYBERSECURITY™ MADE IN EUROPE

CO_2 neutral website ▶

SECPOINT® www.secpoint.com

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision