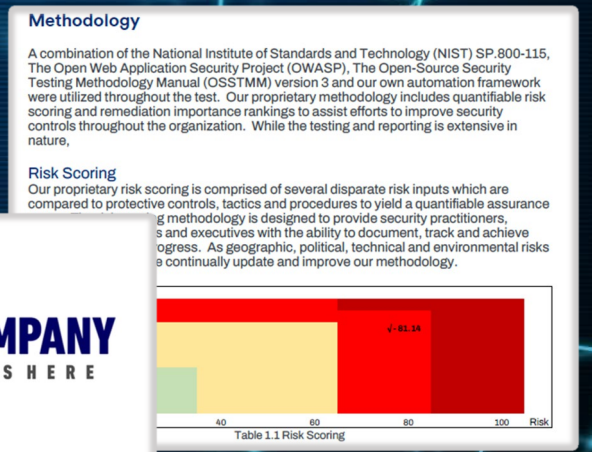
Security Services for Managed Service Providers

White-Labeled Penetration Testing

- Engagement tailored to the client
- Specific timeframe and deliverables
- On-premise, cloud and hybrid
- Preferred pricing

Penetration Testing as a Service (PTaaS)

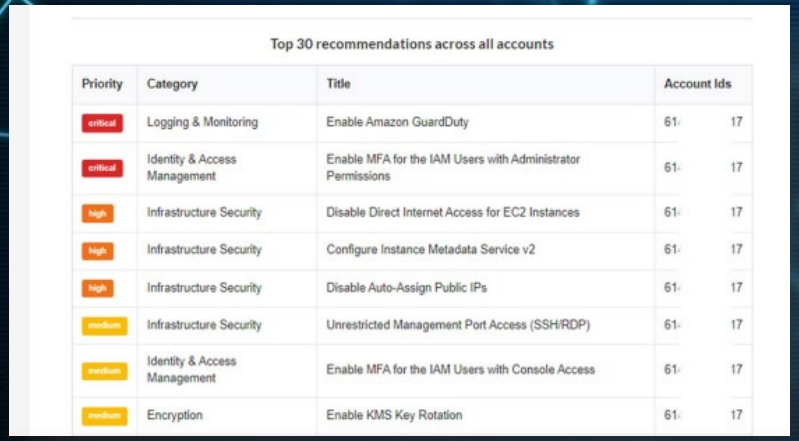
- Automated external vulnerability scanning and penetration testing
- Open ports, exposures, misconfigurations, 60,000+ vulnerabilities
- Customizable dashboards with real-time views & reporting
- Ongoing support/coverage for Zero Days



Security Services for Managed Service Providers

Cloud Security and Compliance

- Automated assessment for cloud infrastructure, systems and services
- Customized checks and dashboards
- Automated/scheduled compliance reporting

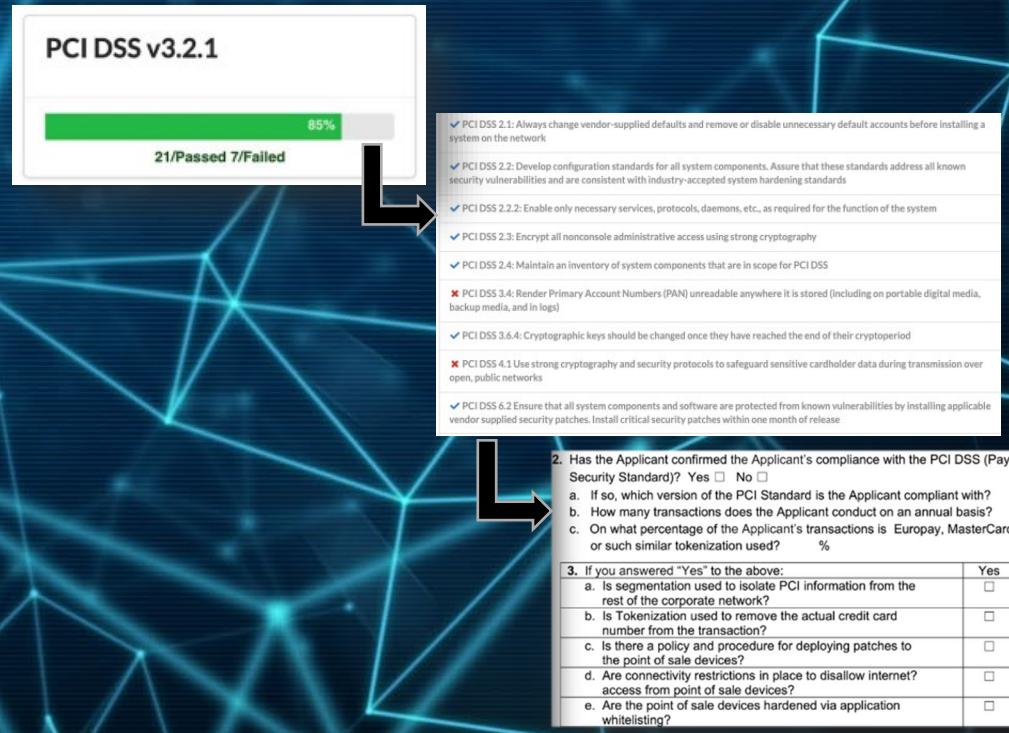


Top 30 recommendations across all accounts

Priority	Category	Title	Account Ids
critical	Logging & Monitoring	Enable Amazon GuardDuty	61 17
critical	Identity & Access Management	Enable MFA for the IAM Users with Administrator Permissions	61 17
high	Infrastructure Security	Disable Direct Internet Access for EC2 Instances	61 17
high	Infrastructure Security	Configure Instance Metadata Service v2	61 17
high	Infrastructure Security	Disable Auto-Assign Public IPs	61 17
medium	Infrastructure Security	Unrestricted Management Port Access (SSH/RDP)	61 17
medium	Identity & Access Management	Enable MFA for the IAM Users with Console Access	61 17
medium	Encryption	Enable KMS Key Rotation	61 17

Cyber Insurance Readiness Assessment

- Compliance and configuration mapped directly to Cyber Insurance forms
- Automated discovery and form completion
- Accompanied reporting and attestation for the cyber insurance carrier



PCI DSS v3.2.1

85%

21/Passed 7/Failed

✔ PCI DSS 2.1: Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network

✔ PCI DSS 2.2: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards

✔ PCI DSS 2.2.2: Enable only necessary services, protocols, daemons, etc., as required for the function of the system

✔ PCI DSS 2.3: Encrypt all nonconsole administrative access using strong cryptography

✔ PCI DSS 2.4: Maintain an inventory of system components that are in scope for PCI DSS

✖ PCI DSS 3.4: Render Primary Account Numbers (PAN) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)

✔ PCI DSS 3.6.4: Cryptographic keys should be changed once they have reached the end of their cryptoperiod

✖ PCI DSS 4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks

✔ PCI DSS 6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release

2. Has the Applicant confirmed the Applicant's compliance with the PCI DSS (Payment Card Industry Data Security Standard)? Yes ☐ No ☐
   a. If so, which version of the PCI Standard is the Applicant compliant with?
   b. How many transactions does the Applicant conduct on an annual basis?
   c. On what percentage of the Applicant's transactions is Europay, MasterCard, Visa (EMV Chip and Pin) or such similar tokenization used? %

3. If you answered "Yes" to the above:	Yes	No
a. Is segmentation used to isolate PCI information from the rest of the corporate network?	☐	☐
b. Is Tokenization used to remove the actual credit card number from the transaction?	☐	☐
c. Is there a policy and procedure for deploying patches to the point of sale devices?	☐	☐
d. Are connectivity restrictions in place to disallow internet? access from point of sale devices?	☐	☐
e. Are the point of sale devices hardened via application whitelisting?	☐	☐

Contact Us for More Information
Schedule a Live Demo:

info@tenfoldsecurity.com
https://tenfoldsecurity.com/request-info/contact/
https://assessment.tenfoldsecurity.com

TENFOLD SECURITY
A SECURITY STRATEGY MUST BE LAYERED TENFOLD