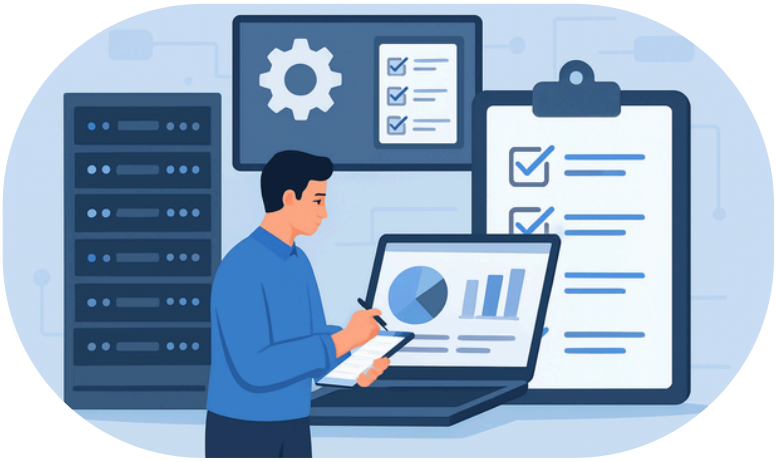
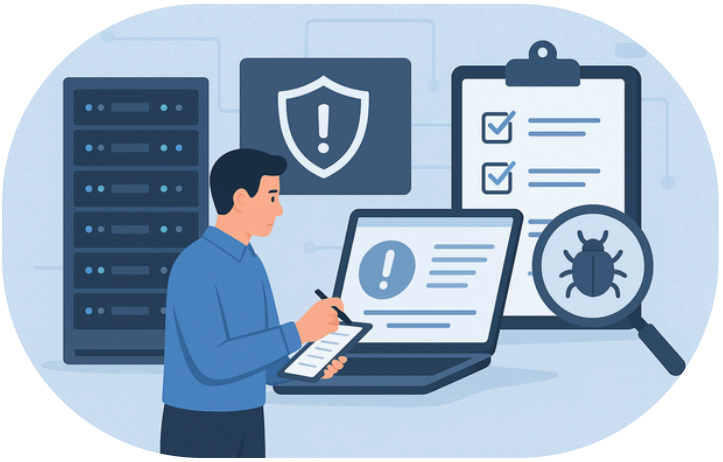
FUTURECALLS
Your Progress, Our Passion.

CAVA: A Holistic Approach to Firewall & Server Security





What is CAVA?

Configuration Assessment and Vulnerability Assessment (CAVA) is a dual-layered security evaluation methodology that combines

- Configuration Assessment (CA): A manual, checklist-driven review of firewall and server configurations against industry best security practices, proprietary hardening baselines, and ISO/IEC 27001:2022 controls.

- Vulnerability Assessment (VA): Automated scanning using tools to detect known vulnerabilities, outdated protocols, and misconfigured services.

Thus, CAVA ensures that both known vulnerabilities and hidden misconfigurations are identified, prioritized, and remediated.

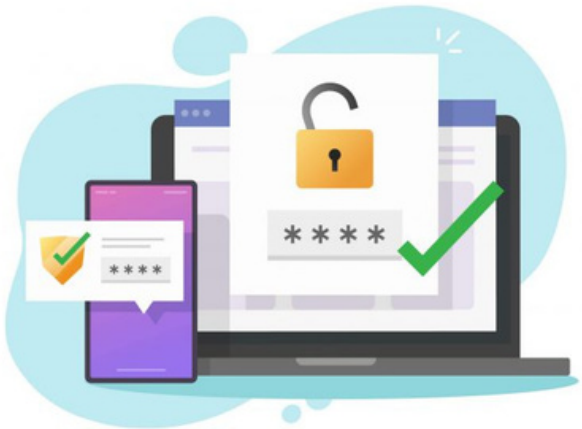
Why CAVA essential for Firewalls and Servers?

Firewalls and servers are the **first line of defence** in cybersecurity strategy.
Relying solely on VA can leave critical gaps:

- VA tools cannot identify flaws and GAPs in security configurations. VA tools can identify predefined generic checklists only.

- CA identifies these gaps, ensuring hardened configurations, secure remote access, compliance with global standards. However, CA will not generally identify hidden vulnerabilities with operating systems, components, firmware, device drivers,etc

CAVA provides a 360° security posture by combining automated scans with expert manual reviews.



Why VA Alone Isn’t Enough

While VA is essential, it is not comprehensive

- Does not detect insecure configurations (e.g., HTTPS enabled on WAN without MFA)
- Does not flag policy-level gaps (e.g., LAN to WAN rules without IPS or AV)
- Fails to assess operational hygiene (e.g., SNMP misconfigurations, NTP sync issues)
- Ignores firmware age and patch status, which are critical for zero-day protection.

CAVA fills these gaps, offering actionable insights and prioritized remediation plans.

FutureCalls unique CAVA - Customer Success Stories

Financial Services Group (Mutual Funds & Investment Advisory)

FutureCalls’ expert security team identified the following critical vulnerabilities using a comprehensive CAVA

- Outdated firmware exposed firewalls to known vulnerabilities.
- Weak administrative password policies and lack of multi-factor authentication (MFA) for WAN access
- LAN to WAN policies were missing critical security services like IPS, Antivirus, and Web Filtering.
- Misconfigured SNMP settings and exposed admin consoles increase the risk of unauthorized access and data leakage.

HTTPS access is enabled on WAN interfaces without MFA.

- **Remediations Completed**
- **The client implemented remediations as suggested by FutureCalls security team. FutureCalls team helped the client to implement the corrective actions**

- The group upgraded firewall firmware and established process for timely firmware upgrades .
- Enforced strong password policies.
- HTTPS access on WAN was disabled; remote access was routed through secure VPN tunnels.
- IPS, AV, and Web Filtering were enabled across all LAN to WAN rules.
- SNMP was reconfigured with secure community strings and restricted IP access.
- Endpoint Management System (EMS) was integrated with VPN to enforce device compliance

Energy Sector Client

- **Challenge**: Vulnerable to SYN flood and Slowloris attacks; multiple open ports exposed to the internet.
- **CAVA Findings:** No DDoS protection, improper WAN access controls, and weak SSL configurations.
- **Outcome:** Enabled SYN flood protection, closed unused ports, and deployed external DDoS mitigation—resulting in uninterrupted uptime and enhanced resilience.

Ready to Secure Your Infrastructure?

FutureCalls Technology, an ISO 9001:2015 & ISO/IEC 27001:2022 certified firm, brings 23+ years of expertise in IT and InfoSec. Our CAVA services deliver:

✅ Expert-led assessments
✅ Proprietary hardening checklists
✅ Post-remediation validation
✅ Compliance alignment with ISO/IEC 27001:2022, GDPR, HIPAA, and more

📞 Contact us today to schedule your CAVA assessment and transform your cybersecurity posture.

Email to : support@futurecalls.com Contact : 91+8148959848

www.futurecalls.com