Vulnerability Assessment & Audit - Close the Patching Gap

A Strategic Briefing for CISOs, CTOs, IT Managers, and Compliance Leaders. Learn how risk-based vulnerability management closes patching gaps and strengthens security.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

VAPT

Vulnerability Assessment & Audit

briskinfosec.com

Building a Stronger Security Posture
Through Risk-Based Vulnerability Management

CREST Approved
India's Only CREST Accredited Partner

CERT-IN Empanelled
Government of India Recognized

ISO 27001:2022
Certified Information Security Management

VA/PT Specialists
Dedicated Vuinerability & Penetration Testing

5600+	640+	25+	95+	8+
Projects Delivered	Customers	Countries	Security Experts	Years of Excellence

Understanding Vulnerability Management — The Risks Organizations Often Overlook

These are not warnings. They are the shared operating conditions every security team is working within right now.

28,000+ CVEs Published Per Year
Growing over 20% each period. Your technology stack accumulates new exploitable weaknesses every day.

60 Days Avg Time to Patch Critical CVEs
Adversaries weaponize newly disclosed critical CVEs within hours of publication. That gap is where the majority of breaches occur.

60%+ Breaches from Known Vulnerabilities
Over 60% of enterprise breaches trace back to a vulnerability that had a patch available.

$4.88M Average Breach Cost
IBM Security. For healthcare the figure rises to $7.42M to $8.77M.

Key Insight: The pattern across all sectors is consistent: teams are not failing to scan. They are failing to close the gap between when a vulnerability is known and when it is fixed. **This is what risk-based vulnerability management was designed to address.** Most security leaders are now asking: do we have the right prioritization framework in place?

Five Conversations We Have With IT Security Teams Every Week

These are not misconceptions to correct. They are reasonable assumptions that need updated context.

WHAT YOU THINK	VS	THE REALITY
"We run a vulnerability scanner monthly, so we are covered." A logical starting point, and it makes sense given how scanning tools are marketed.	→	**Point-in-time scanning creates a snapshot that is outdated within 24 hours.** New CVEs are disclosed daily. Continuous monitoring is the only approach that maintains an accurate picture of actual risk exposure at any given moment.
"A CVSS 10.0 vulnerability is always our top priority." CVSS is the universal scoring standard, so it seems natural to rank by CVSS score.	→	**CVSS measures theoretical severity. EPSS measures probability of exploitation in the next 30 days.** A CVSS 7.5 with an active exploit kit is more dangerous than a CVSS 10.0 with no public exploit. Risk-based prioritisation changes what gets fixed first.
"We patch everything critical within our SLA window." Most teams have strong patch visibility for managed endpoints, and that is a solid foundation.	→	**Shadow IT, cloud resources, third-party software, and OT systems frequently fall outside standard patching programs.** These unmanaged assets consistently carry the highest exploitability.
"Quarterly scans satisfy our compliance requirements." PCI DSS and other frameworks do reference quarterly scanning, and compliance is a legitimate driver.	→	**Compliance scans confirm a baseline. Securtly requires continuous visibility.** A quarterly scan passes an audit but leaves a 90-day window where new CVEs go undetected. Compliance and security are different goals.
"Our cloud provider handles vulnerability management for cloud assets." The shared responsibility model sounds like it should cover this.	→	**Cloud providers patch the underlying infrastructure.** Application-level, configuration-level, and identity-level vulnerability management sits entirely with the customer. Misconfigurations are the leading cause of cloud breaches.

The Business Impact of These Gaps

Every assumption gap has a measurable business consequence.

INCREASED BREACH RISK

60%+

Breaches trace back to known vulnerabilities with available patches.

HIGHER FINANCIAL IMPACT

$4.88M

Average cost of a data breach from known, unpatched CVEs.

LONGER RECOVERY TIME

258 Days

Average breach lifecycle without continuous vulnerability monitoring.

COMPLIANCE EXPOSURE

90-Day

Blind spot between quarterly scans where new CVEs go undetected.

WASTED SECURITY RESOURCES

30–50%

Of security team time spent chosing false positives and low-risk findings.

The Cost of Inaction — Prevention Costs Far Less

Annual continuous vulnerability management cost for a mid-size organization: a fraction of a single breach event averaging $4.88M.

$4.88M
Average Breach Cost

From known unpatched CVE (IBM Security), Proactive organizations spend 40% less on breach remediation than reactive peers.

258 Days
Avg Breach Lifecycle

Without continuous monitoring (IBM).

20–40%
Insurance Premium Reduction

Cyber insurance premium reduction with documented VA program.

100 Days
Lifecycle Compression

Breach lifecycle compression with AI-driven vulnerability management.

The Landscape Your Peers Are Navigating

Published benchmarks shaping how security leaders prioritize vulnerability investment.

WHAT YOU THINK	THE REALITY	BUSINESS IMPACT	SUPPORTING FACT
We scan quarterly, so we are compliant.	90-day blind window for new CVEs.	Exploits lond between scans, increasing breach risk.	60%+ breaches involve known, unpatched vulnerabilities.
We prioritize by CVSS score.	High-volume noise, wrong fixes first.	Teams waste cycles on low-risk issues, real risk remains.	EPS5-ranked CVEs 3x more likely to be exploited.
Cloud provider manages our cloud security.	Misconfigurations go undetected.	Misconfigurations are the leading cause of cloud breaches.	Misconfigurations are the leading cause of cloud breaches.
We patch everything critical in our SLA.	Shadow IT and OT assets remain exposed.	Unmanaged assets create easy entry points for attackers.	Mean time to patch: 60+ days industry average.

Key Takeaway

The gap between vulnerability discovery and remediation is the real risk.

1. Attackers act in hours. Most organizations take weeks.
2. Continuous visibility + risk-based prioritization close the gap.
3. The cost of prevention is always lower than the cost of breach.

What We Assess Across Your Environment — Why Prioritization Frameworks Matter

Three scoring systems working together produce better remediation decisions than any single score alone.

CVSS 3.1

TECHNICAL SEVERITY: BASE, TEMPORAL, ENVIRONMENTAL SCORES

EPSS

EXPLOITATION PROBABILITY IN NEXT 30 DAYS — PREDICTIVE PRIORITIZATION

SSVC

DECISION-BASED ACTION PRIORITY: DEFER / SCHEDULED / OOB / IMMEDIATE

CVSS 4.0

UPDATED SUPPLEMENTAL METRICS: SAFETY, AUTOMATABLE, RECOVERY

Common Technical Gaps We Identify

Overly Permissive IAM

Excessive access rights granted to users, roles, and service accounts beyond operational need.

Public Storage Exposure

Cloud storage buckets and repositories misconfigured with public read or write access.

Open Security Groups

Inbound rules permitting unrestricted access to sensitive ports and services.

Unencrypted Data

Data at rest and in transit lacking encryption controls across storage and communication layers.

Disabled Logging

Audit trails and monitoring logs disabled or misconfigured, leaving no forensic visibility.

Exposed Secrets

API keys, credentials, and tokens embedded in code repositories or configuration files.

Our Six-Stage Vulnerability Assessment Lifecycle

A structured audit follows a defined lifecycle. Each stage builds on the previous one to produce actionable, evidence-based results.

1 Discovery

Full asset enumeration across network, cloud, web applications, APIs, containers, and foT. Shadow IT and unmanaged assets included.

Output: Verified asset inventory with coverage gaps identified.

2 Prioritization

CVSS + SPSS + SSVC scoring with asset criticality weighting and threat intelligence overlay,

Output: Risk-ranked vulnerability qpoce with clear action categories.

3 Validation

Manual expert review of automated findings, false positive elimination, and explaitability verification.

Output: Confirmed vulnerability list without noise, adjusted for your environment.

4 Remediation Guidance

Prioritized remediation roadmap with developer-ready fix instructions and ticketing integration.

Output: Team-specific remediation plan with SLAs. (Critical 7 days, High 55 days, Medium 90 days)

5 Re-Testing

Patch verification scanning, residual risk documentation, and accepted risk sign-off.

Output: Confirmed clesure evidence for each finding, oudit-roody and compliance-mapped.

6 Reporting

Exccutive dashboard, full technical report, compliance evidence pack, and bSAFE maturity score.

Output: Board-level risk posture sommary alongside detailed technical findings for teams.

This structured six-stage process ensures every finding is **verified, prioritized, and mapped to a clear remediation action** before delivery to your team.

Compliance Frameworks Addressed — Reducing Separate Audit Preparation Effort

Vulnerability audit findings map directly to these frameworks, reducing separate audit preparation effort.

PCI DSS 4.0

QUARTERLY SCANS + CRITICAL PATCH TIMELINE REQUIREMENTS

ISO 27001

VULNERABILITY MANAGEMENT CONTROL REQUIREMENTS (2022 UPDATE)

NIST CSF 2.0

IDENTIFY AND PROTECT FUNCTIONS WITH CONTINUOUS EVIDENCE

RBI / SEBI

INDIA: VULNERABILITY MANAGEMENT FOR BANKS, NBFCs, MARKET INFRASTRUCTURE

Current State vs. Future State

CURRENT STATE (POINT-IN-TIME / REACTIVE)

- Vulnerability discovery lag of up to 90 days between scons.
- CVSS-only prioritization creates high-volume remediation noise.
- Shadow IT and cloud assets fall outside scanning coverage.
- Patch backlog grows faster than teams can address it.
- Compliance scans pass audits but do not reflect real-time pasture.
- No continuous evidence trail for insurance or regulatory review.
- Board receives a snapshot report, not a live risk posture view.

FUTURE STATE (CONTINUOUS, RISK-BASED PROGRAM)

- New CVEs identified within hours of NVD publication.
- CVSS + EPSS + SSVC prioritization focuses team on highest-probability threats.
- Full asset inventory including cloud, containers, and shadow IT.
- Mean time to patch critical vulnerabilities reduced from **60+ to 14 days.**
- Continuous compliance evidence for PCI DSS, ISO 27001, HIPAA, RBI.
- **20–40%** cyber insurance premium reduction with documented program.
- Board receives a live risk dashboard with trend data and KPIs.

The organizations closing the patching gap fastest share one common characteristic: they moved from point-in-time scanning to a continuous, risk-based program.

This shift reduces breach risk, controls cost, and builds lasting audit and board-level confidence.

Choosing the Right Security Assessment Approach — What a Vulnerability Management Partner Should Bring

The right partner combines accredited assessment capability with an intelligence layer that reflects real-world attacker behavior.

CAPABILITY	TYPICAL SCANNING VENDOR	BRISKINFOSEC APPROACH
Accreditation	Tool-based, no independent audit accreditation	**CREST Approved (Indiy's ONLY) + CERT-In + ISO 27001:2022**
Prioritization	CVSS score ranking from automated tool	**CVSS + EPSS + SSVC + asset criticality + threat intelligence**
False Positive Rate	High – manual review burden on your team	**Expert analyst validation** removes noise before delivery
Threat Intelligence	Static CVE database updates	**THREATSPLOIT** Adversory Report: **83+** editions of active explaitation intelligence
Asset Coverage	Managed endpoints and known IP ranges	**Full discovery:** shadow IT, cloud, containers, APIs, OT scope
Continuous Monitoring	Scheduled scan intervals	**LURA portal:** real-time tracking, live feed, remediation quoue
Compliance Evidence	PDF report at scan completion	**Continuous** repository for PCI DSS, ISO 27001, HIPAA, RBI, SEBI, SOC 2

Three Paths to a Stronger Vulnerability Posture

Choose based on where you are today and where you need to be.

1 Vulnerability Baseline Assessment

Comprehensive point-in-time audit across network, web apps, cloud, and APIs.

- Full asset discovery
- Risk-based prioritization
- Actionable remediation roadmap
- Executive & technical reporting

2 Continuous Vulnerability Management

Automated continuous scanning with analyst prioritization and business-aligned reporting.

- Continuous discovery & monitoring
- Expert-validated risk quoue
- Monthly reporting & dashboards
- Compliance evidence generation

3 Enterprise Vulnerability Risk Program

Fall-spectram program to manage risk across complex, dynamic, and regulated environments.

- End-to-end vulnerability lifecycle
- Threat intelligence integration
- DevSecOps & pipeline integration
- Boord-level risk reporting & RPIs

Our Track Record. Your Due Diligence.

540+
Clients Across 20+ Countries

4,800+
Security Assessments Delivered

0%
Client Breach Rate Post-Engagement

99.8%
Compliance Achievement Rate Across 50+ Frameworks

What a Continuous Vulnerability Program Protects

Each figure represents a real cost that a risk-based vulnerability program directly reduces.

$4.88M
Average breach cost from known unpatched CVE (IBM).
Proactive organizations spend 40% less on breach remediation than reactive peers.

40%
Cyber insurance premium reduction
with a documented and continuously evidenced vulnerability management program.

100 Days
Breach lifecycle compression achievable through AI-driven vulnerability management, reducing attacker dweit time significantly.

15,847+
Vulnerabilities identified and remediated across Brickiofosec client engagements, $127M in estimated breach costs prevented.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

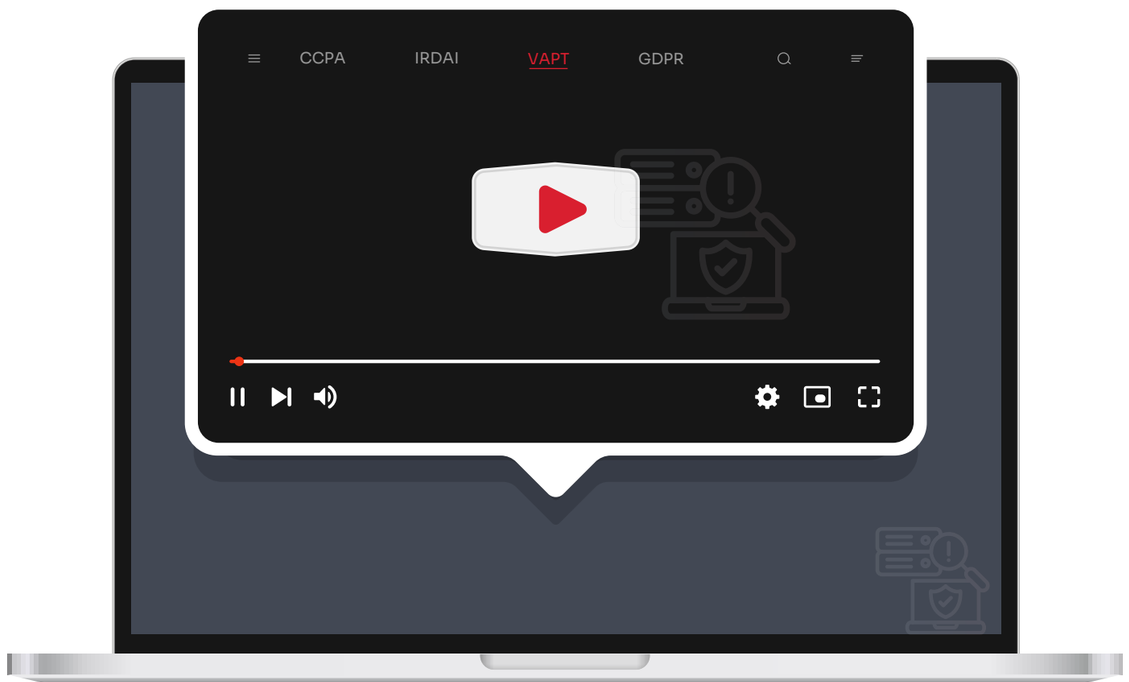
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence
India
UAE