MITIGATOR®

VULNERABILITY & THREAT MANAGER

TURNING CYBER RISK EXPOSURE INTO QUANTIFIABLE BUSINESS IMPACT

(305) 921-3881
Info@eSurelTy.com

VULNERABILITY & THREAT MANAGEMENT

The problem isn't finding vulnerabilities—it's knowing which ones matter and remediating them fast. The new version of Mitigator® delivers a fully modernized platform that transforms raw scan data into quantifiable risk intelligence—measuring cyber risk exposure in real dollar terms and arming security leaders with the metrics that drive decisions.

DRIVE MEASURABLE RISK REDUCTION WITH MITIGATOR

Mitigator is designed to help organizations move from qualitative to quantitative cyber risk measurement, providing clearer visibility into where exposure exists, how risk is trending, and what that exposure means in real dollars.

- **Faster Time to Remediate (TTR) –** Shortens exposure windows and blocks lateral movement before attackers exploit gaps.
- **Quantified Risk Exposure** – Calculates total organizational risk in real dollar terms, identifying where risk is most concentrated across assets, systems, and identities.
- **Continuous Visibility** – Unified dashboards and role-based views show risk by asset, severity, and business context—with a fully modernized, intuitive interface.
- **Prioritized Remediation** – CVSS, threat intelligence, exploitability, asset criticality, and a newly upgraded risk scoring engine guide which issues get fixed first.
- **Proof for Leadership & Auditors** – Evidence-based reports track MTTR, remediation velocity, and other KPIs boards care about, clearly demonstrating organizational maturity and progress.

TRANSFORM DATA INTO DECISIONS

Comprehensive Discovery

Identify all devices, services, and software (workstations, servers, IoT, cloud environments).

Smart Vulnerability Analysis

Detect CVEs, missing patches, misconfigurations, weak credentials, and encryption flaws.

Contextual Risk Adjustment

Account for compensating controls, segmentation, and asset sensitivity to produce more accurate reports.

Actionable Remediation

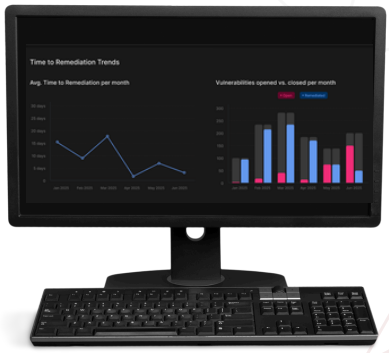
Step-by-step fix paths, on-demand pen testing of findings, and integration with ServiceNow/Jira/email.

Closed-Loop Tracking

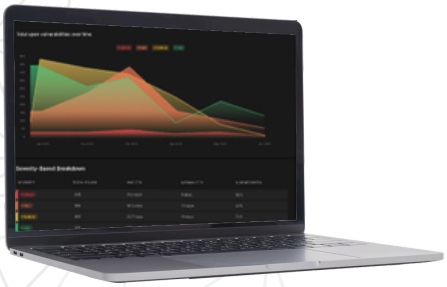
Real-time dashboards monitor remediation progress, while retest reports validate closure and provide defensible audit evidence.

CONTEXTUAL RISK INTELLIGENCE THAT PRIORITIZES RESPONSE

Mitigator isn't just a scanner—it's a decision platform that arms security leaders with metrics that matter.



- **Unified Dashboard** – Clear visibility across assets, severity, and trends.
- **Tailored Reporting** – Executive summaries for leadership; technical detail for engineers.
- **Metrics & Trends** – Track MTTR, remediation velocity, and compliance alignment (NIST, HIPAA, PCI-DSS, NERC CIP). These KPIs demonstrate to executives and auditors that vulnerabilities are remediated promptly, reinforcing governance, maturity, and sustained network security.
- **Seamless Ticketing Integration** – One-click exports to ServiceNow, Jira, or email workflows.
- **Proof of Remediation** – Retest confirmation ensures vulnerabilities are truly fixed—and progress is documented..



WHY THESE METRICS MATTER

Mean Time to Remediate (MTTR): Shows how quickly your team neutralizes vulnerabilities once discovered. Lower MTTR = reduced attack window.

Remediation Velocity: Tracks how consistently issues are resolved across business units, proving security progress over time.

Compliance Alignment: Demonstrates adherence to NIST, HIPAA, PCI-DSS, NERC CIP, and CIS with evidence-backed closure.

Together, these KPIs give your board and auditors proof of maturity—showing that vulnerabilities aren't just found, but fixed fast, keeping your environment resilient and audit-ready.

PLATFORM FEATURES

Discovery & Enumeration

Asset Discovery – Identify all reachable devices (workstations, servers, printers, network gear, security appliances, IoT, VMs, cloud endpoints).

Port & Service Enumeration – Detect open ports, running services, protocol versions, and fingerprint OS/firmware.

Smart Vulnerability Analysis

Vulnerability Identification – Map discovered services to known CVEs, missing patches, weak configurations, default credentials, and encryption issues

Risk Scoring – Evaluates and weights all identified risks for a more accurate representation of overall security posture.

Contextual Risk Adjustment - Account for compensating controls, segmentation, and asset sensitivity to produce accurate, environment-specific reports.

Actionable Remediation

Step-by-step fix paths – on-demand penetration testing of specific findings, and integration with ServiceNow / Jira / email.

Schedule Remediation - Publish findings with remediation instructions and assign remediation tasks to staff via the ticketing module.

Track Remediation Efforts – Monitor remediation progress within the portal.

Reporting & Analytics

Centralized Dashboard – View and analyze vulnerabilities by asset, criticality, and track trends.

Reporting - Generate both executive-level reports (for management/third parties) and technical reports with data export capabilities.

Metrics & Trend Analysis – Track risk scores, vulnerability age, remediation velocity, and compliance alignment (CIS, NIST CSF).

MITIGATOR
VULNERABILITY & THREAT MANAGER

ATTACK THREATS HEAD ON!

Are you ready to see how your current vulnerability program measures up?
Contact us to learn more about Mitigator.