

MITIGATE

Mitigate

To reduce the severity or probability of significant network intrusion, damage or espionage by known and unknown security vulnerabilities.

Why Mitigate?

Almost daily, vendors announce new security vulnerabilities. The goals of these security risks are to interrupt the speed of normal business processes, destroy or steal information. Simply put, stopping infiltration of these security risks is virtually impossible. However there are both preemptive and post emptive techniques which can be taken to lessen the severity. The result = Mitigation.

How We Do It

Mitigation is an excellent post emptive technique used by Pari Networks. While monitoring the configuration changes of your network, one of primary goals is to detect new changes and unusual behavior. Once we detect new changes or unusual behavior, the following steps of mitigation/remediation are taken:

1. Alert applicable personnel of potential problems
2. Automatic Security Assessment on changes (AUDIT)

3. Quarantine identified network devices for further analysis
4. Implement temporary policy
5. Access centralized global policy monitor for most recent security vulnerability announcements.
6. Update temporary policy with new vendor policy
7. Review and update profiles as required.

Pari Networks Components Used

Policy

Conducts policy and audit execution, fix generation and application.

Reports

Generates policy and audit report generation, system log reports.

Audit

Conducts capability and network status audits.

About Us

Pari Networks provides effective and easy to use security risk management solution. We have a patent pending approach for combining network operations, regulatory/corporate compliance, security assessments and remediation actions. This enables simplified administration of networks ensuring secure and regulated business operations for our partners and customers.