KENNA Security

Risk-Based SLAs

Achieve and maintain an acceptable level of risk for your business

The longer you're a Kenna.VM user, the more likely you are to reach a steady-state with your risk score. Kenna Security has taken its unique research and data to help customers to reach and maintain an acceptable level of risk with a new feature that sets service-level agreements based on risk.

Risk Tolerance Groups

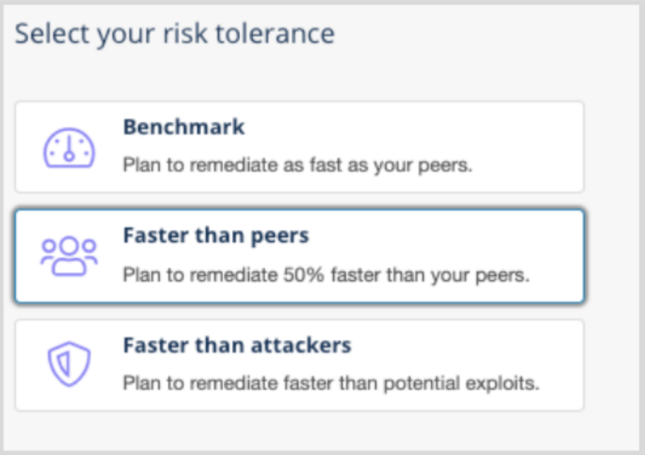
To have the most success with risk-based SLAs, it's critical to select the risk tolerance that you feel is appropriate for your organization—that is, a higher risk tolerance means you are willing to accept more risk. Kenna.VM segments risk tolerances into three groups: Benchmark, Faster than peers, and Faster than attackers.

BENCHMARK

This is the highest risk tolerance level and is best suited to organizations new to SLAs or without a mature vulnerability management program. Timeframes are recommended with the objective of enabling you to remediate vulnerabilities as fast as your peers.

FASTER THAN PEERS

This group sets a mid-level risk tolerance. Timeframes are recommended with the objective of enabling you to remediate vulnerabilities faster than 50% of your peers.



Select your risk tolerance

Benchmark
Plan to remediate as fast as your peers.

Faster than peers
Plan to remediate 50% faster than your peers.

Faster than attackers
Plan to remediate faster than potential exploits.

Figure 1: Risk tolerance options in Kenna.VM

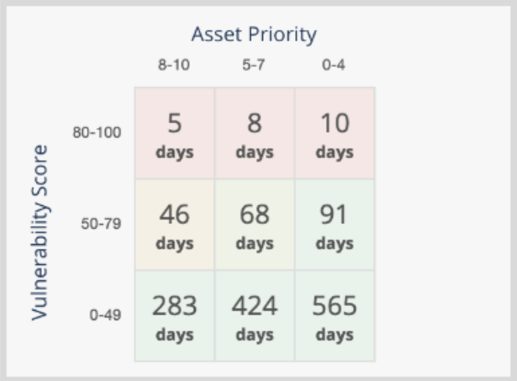
FASTER THAN ATTACKERS

This is the lowest possible risk tolerance level and is best suited to organizations that are very mature in their vulnerability management program. Timeframes are recommended with the objective of enabling you to remediate vulnerabilities faster than attackers.

SLA Timelines

When you set up your SLAs, you will see a grid with a range of timeframes, as depicted in Figure 2. These timeframes are segmented by three factors:

- The risk tolerance of the client
- The asset priority upon which the SLA is being set
- The vulnerability risk score (high, medium, or low)



	Asset Priority		
Vulnerability Score	8-10	5-7	0-4
80-100	5 days	8 days	10 days
50-79	46 days	68 days	91 days
0-49	283 days	424 days	565 days

Figure 2: An example of SLA recommendations in Kenna.VM

The Data Behind Risk-Based SLAs

Kenna Security draws from nearly a decade of research and data, including more than 15 threat and exploit intelligence feeds, more than 7 billion managed vulnerabilities, and more than one billion security events processed monthly.

To understand Kenna.VM's SLA recommendations, let's look at exactly which pieces of data factor into the creation of different timelines. There are two datasets that underlie our SLA recommendations:

Mean Time to Remediation

Mean Time to Remediation (MTTR) is a metric that signals how fast organizations using Kenna.VM are remediating vulnerabilities (i.e. the average rates at which vulnerabilities are closed). For example, at the "Benchmark" level, a recommendation of 50 days means your peers are remediating a vulnerability within an average of 50 days. Timelines in both the "Benchmark" and "Faster Than Peers" risk tolerance levels are generated by looking at MTTR data.

Mean Time to Exploitation

Using our vast database of threat and exploit intelligence, Kenna Security is able to identify how fast attackers are exploiting vulnerabilities. This allows us to calculate the Mean Time to Exploitation (MTTE). Timelines in the "Faster Than Attackers" category are based on MTTE data. When Kenna.VM recommends to your customer to remediate a vulnerability within 7 days, it means that attackers will exploit that vulnerability, on median, within 7 days. These timeframes are very aggressive, and some may be difficult to meet, but keep in mind that attackers often exploit vulnerabilities before we even know about them.

Build Towards Faster Remediation

Kenna.VM's risk-based SLAs are designed to help encourage and facilitate faster remediation. Kenna Security research, *Prioritization to Prediction, Volume 4: Measuring What Matters*, analyzed how organizations are implementing SLAs and came to understand the "motivating power of deadlines." Our analysis showed that defined SLAs helped to reduce the volume of surviving (or not remediated) high-risk vulnerabilities by 15%.

By using real-world threat intelligence and peer usage data, SLAs in Kenna.VM are more meaningful than ever. Even if all deadlines are not met with complete success, a risk-based approach to SLAs is the most effective way to ensure that your organization is moving towards a meaningful, proactive risk posture. Keep in mind that there is only a small subset of vulnerabilities for which Kenna.VM will recommend aggressive timeframes. For the overwhelming majority of vulnerabilities, you will have more time—more time than you likely thought you did, thanks to Kenna.VM's prioritization. With SLAs, you can continue to focus your resources on the vulnerabilities that matter the most.

Find out more about the robust threat intelligence of Kenna.VM at **www.kennasecurity.com**

K☰NNA Security