

Rapid7 Customer Support services provide rapid resolution of issues. We include telephone and email support, 24 hour vulnerability service level agreement, 24 hour incident response time, and a reliable testing guarantee.

We are dedicated to delivering superior support for our products. Whether you are testing NeXpose or Metasploit, or have been using them for some time, you are backed by our years of experience and commitment to customer satisfaction. Our team of highly skilled and responsive experts in network security understands the criticality of your issues and is available to help.

Telephone Support

Our standard support provides access to support resources from 9 a.m. to 8 p.m. EST to ensure you can scan and fix your network vulnerabilities before your systems are compromised. Need help now? Call 866-390-8113 to reach a support representative.

See 'Submitting A Support Case' below for more information about our support guidelines.

Types of Support

	NeXpose	Metasploit Pro	NeXpose Express	MetaSploit Express	NeXpose Community	Metasploit Community
<i>Rapid7 Community</i>	✓	✓	✓	✓	✓	✓
<i>Rapid7 Self-Help / Knowledgebase</i>	✓	✓	✓	✓	✓	✓
<i>eSupport</i>	✓	✓	✓	✓		
<i>Software Releases, Updates, Fixes</i>	✓	✓	✓	✓		
<i>Telephone Support (Mon-Fri, 8am - 8pm ET)</i>	✓	✓				
<i>Severity 1 Support</i>	✓	✓				

Product Updates

Rapid7 releases NeXpose updates twice a month and Metasploit updates every week. These updates contain the latest vulnerability tests, exploits, product updates and new device and system support. They are applied through the products' auto-update feature to ensure you are running the latest versions in your environment.

NeXpose Reliable Testing Guarantee

Rapid7 believes that false positives, in other words mistakenly reporting vulnerabilities where there are none, are bugs in the product. Our guarantee to our customers is that we handle the reporting of a false positive as a bug and it gets the same priorities in our development process as other software bugs. Product fixes are delivered through our auto-update capability and are available to you as soon as they are tested within the product. Whether you are running software, an appliance or our managed service, these updates are available to you quickly.

In the rare instance that NeXpose does issue a false positive, Rapid7 will follow our zero false positive policy process. [Notify Rapid7 support](#) immediately to report the incident and begin the resolution process. The Rapid7 technical support team will work with you to investigate the incident and escalate it to development for resolution. After extensive testing in the Rapid7 QA lab, the update will be released to all NeXpose customers with a valid subscription service.

NeXpose 24-hour Vulnerability Service Level Agreement

Rapid7 is committed to providing timely updates to NeXpose customers with the most current vulnerability definitions. Microsoft releases patches on the second Tuesday of each month and occasionally releases additional out of cycle advisories. Within 24-hours of release by Microsoft, Rapid7 will release updates to all NeXpose customers reflecting checks for all vulnerabilities identified in Microsoft's advisories.

Comprehensive Vulnerability Database

The key to the NeXpose system is Rapid7's extensive built-in database with more than 61,000 vulnerability checks for over 15,600 vulnerability definitions.. This database cross-links the thousands of external databases that provide patches, downloads, references and additional information about the security weaknesses in systems including CERT, SANS, CVE, and the Microsoft Knowledge Base. NeXpose automatically updates this database every six hours by downloading new vulnerability definitions as XML definition templates. [Search the NeXpose Vulnerability Database](#) and find out the depth of NeXpose's scanning capabilities.

Whether you need assistance in the installation of our product, a recommendation about how to configure NeXpose for your enterprise network or guidance on how you can use NeXpose to comply with federal regulations such as Sarbanes-Oxley reporting requirements or HIPAA, we can offer you the services required to achieve success.

Largest public database of quality-assured exploits

Thanks to its unique cooperation between Rapid7 and the large Metasploit community supported by more than 110,000 active users, Metasploit maintains the world's largest public database of quality assured exploits and payloads, making your penetration tests both realistic and safe to simulate attacks on your infrastructure. Unlike alternative solutions, which often list local exploits that are of limited use to penetration testers, all Metasploit exploits are remote so they can be executed over the network. All exploits and payloads are quality assured before they are included in the the commercial editions of Metasploit to ensure that they work correctly and do not contain malware. All of the exploits and payloads run in memory only and never install any software on the systems you are testing.

[Contact us](#) to get more information on Rapid7 support.

SUBMITTING A SUPPORT CASE

Severity Level

When submitting a case, you will be asked for the Severity Level. The Support Engineer will evaluate the case with you and together you may determine to change the severity of the case based on the business impact. The following definitions are used to ensure your case's integrity:

LEVEL	DESCRIPTION
Severity-1 <i>"Mission Critical"</i>	A severity one (1) issue is an issue in production indicating any of the below: <ul style="list-style-type: none"> • Rapid7 product is severely impacted or completely down • Business-critical applications are unable to function • A software defect leaving the system open to attack
Severity-2 <i>"High"</i>	A severity two (2) issue is an issue that: <ul style="list-style-type: none"> • Rapid7 product is functioning with limited capability • System instability present with periodic interruptions
Severity-3 <i>"Medium"</i>	A severity three (3) issue is an issue in that: <ul style="list-style-type: none"> • Rapid7 product has errors and is still fully functional • Clarification of product or documentation is necessary • General usage question • Recommendation for future product enhancement

Roles and Responsibilities

ROLE	WILL DO
Customer	<ul style="list-style-type: none"> • Train users to appropriate degree on Rapid7 products • Maintain test environments • Communicate business impacts of any technical issues appropriately • Collect diagnostics and other information in submitting cases • Engage technical and management resources appropriately • Provide equal resource availability
Rapid7 SE	<ul style="list-style-type: none"> • Understand the business impact of the customer's issue • Provide technical expertise • Troubleshoot and resolve the client's issue • Provide status updates to clients through the resolution process
Rapid7 Support Manager	<ul style="list-style-type: none"> • Communicate product updates and important news • Ensure highest degree of technical "know-how" in support • Keep apprised of high priority customer issues
Rapid7 Account Manager	<ul style="list-style-type: none"> • Understand customer requirements • Recommend solutions with Rapid7 technology that meet requirements

Case Response Times

When creating a support case, expect initial contact during normal business hours within the following targeted response times by a Support Engineer. Ongoing response times shall be governed by the following default times unless other communication statuses are set.

LEVEL	TARGET INITIAL RESPONSE TIME	ON-GOING RESPONSE TIME
Severity-1 <i>"Mission Critical"</i>	< 2 Hours	4 Business Hours
Severity-2 <i>"High"</i>	< 4 Business Hours	3 Business Days
Severity-3 <i>"Medium"</i>	< 12 Business Hours	5 Business Days