Technical Support Policy

Date:	November 30, 2018
Version:	2.0

In November 2018, ForeScout acquired SecurityMatters. References to SecurityMatters below will mean ForeScout.

1 Software releases

In general, SecurityMatters releases updates and upgrades in accordance with its published release cycle. A new version includes improvements and new functionalities. It may also include updates such as patches or security patches. New product versions and updates are distributed via the SecurityMatters Portal. These can be installed with remote assistance or, if agreed with reseller, on-site assistance of the support team (see Appendix Support Systems and Documentation).

2 Technical Support Levels

The product technical support follows a multi-level support model of three levels:

1. Level 1 handles the majority of basic questions.
2. Level 2 supports customer during deployment and maintenance activities, such as installations and upgrades, and can troubleshoot product misbheaviors.
3. Level 3 is a specialized group of subject matter experts that perform complex event analysis on misbheaviors of the product able to provide quick workaround and hot fixes if necessary.

The support levels are described in more detail below.

Additional support levels and procedures can be agreed in writing as part of a service level agreement to suit customer requirements.

2.1 SecurityMatters Support Services

2.2 Level 1

The goal of Level 1 support is to assist with common issues and answer general questions related to the Software. The Level 1 support team shall be available via email during service hours or as agreed otherwise with the customer.

Level 1 support representatives shall have a general and broad understanding of the product. Level 1 support staff are not required to understand the inner workings of the product or how to interpret the monitoring information.

Level 1 support representatives shall gather information from the customer to determine the customer's issue. The information could be installation type (e.g. physical, virtual, bundled), system components affected (e.g. Command Center), Error messages, log files, screenshots and possibility data (e.g. PCAP files), as well as, the action the customer tried to achieve or the steps that were taken. Once the issue has been identified, the support representative shall examine the possible solutions available. Solutions can be found in the Documentation and the SecurityMatters Knowledge Base. The Knowledge Base provides answers to reoccurring questions and issues. Some issues may be straightforward to solve, while others may require more interaction with the customer.

If no solution can be found, the Level 1 support representatives shall escalate the issue to Level 2 support representatives. Before escalating, Level 1 representatives must have gathered all relevant deployment information and they shall document the (unsuccessful) steps taken as well as what has already been

accomplished.

Examples of potential problems addressed by Level 1:

- User got locked out of the SilentDefense Command Center
- User cannot find how to change the time zone settings
- Questions regarding the deployment of a virtual machine of SilentDefense (e.g. common problems when deploying on different hypervisors)
- Questions about which protocols are recognized or parsed
- Questions about how to configure widgets/syslog forwarding/LDAP integration/etc.

2.2.1. Level 2

Level 2 support tackles more complex issues that may not always have a straightforward, documented solution available. Level 2 support representatives shall be able to actively troubleshoot the product with customer.

When an issue is escalated to Level 2 support, a Level 2 support specialist shall first study the actions taken at Level 1 support. If the cause of the customer's issue is unclear, the Level 2 support specialist shall start the troubleshooting process, by running tests, diagnostics and considering the monitored environment to understand the problem. When a documented solution is available, the Level 2 support representative shall offer the solution to the customer and may guide the customer through the process (for example, via remote web conference with screen sharing and take-control functions). The Level 2 specialist shall use best efforts to come up with a solution or workaround.. If the issue is an open Error, the support specialist shall report it to a Level 3 expert.

Examples of potential problems addressed by Level 2:

- Verifying a system Error
- Give suggestions on sensor placement points
- Diagnosis of hardware issues
- Basic suggestions on profile tuning
- Assistance during event analysis
- Support during installations and upgrades

2.2.2. Level 3

Level 3 support concerns in-depth troubleshooting related to errors and product mishbeaviors. Errors are also analyzed by Level 3 support to determine the impact and urgency.

Examples of potential problems addressed by Level 3 support:

- A software Error that needs to be fixed
- Customer finds strange network behavior and asks for analysis. This could involve PCAP analysis and Software event analysis

Outcomes of the Level 3 support are workaround instructions and procedure or hot fixes.

3 Support Terms

3.1 Fixing of Errors

After receipt of a request for Level 2 or 3 support, SecurityMatters shall do the best of its ability attempt to fix any Errors in the Software and/or make corrections in any later Updates or releases of the product in accordance

with and subject to this Technical Support Policy and the terms of the main body of the Agreement.

3.2 Pre-requisites

Customer shall lend any reasonable cooperation required by SecurityMatters for the purpose of performing the support, including but not limited to (i) the temporary suspension of use of the Software if SecurityMatters deems this to be necessary and (ii) allowing SecurityMatters access to the customer's site(s) or (online) to the System, e.g. to test patches (see also the Appendix Support Systems and Documentation).

If customer fails to lend the cooperation requested, SecurityMatters may suspend or limit the support. If SecurityMatters is providing support on the basis of information to be provided by customer, this information shall be prepared in accordance with the conditions to be imposed by SecurityMatters and provided at the risk and expense of customer.

Customer guarantees that all materials, information, software, procedures and instructions that it and/or the customers make available to SecurityMatters for the purpose of providing SecurityMatters Support Services is accurate and complete and that all data carriers issued to SecurityMatters meet SecurityMatters' specifications.

3.3 Reinstatement of Support Services

If customer has not paid a Maintenance Fee for a Product in any year(s), SecurityMatters will perform the support services in any subsequent year only upon payment of a reinstatement fee. The reinstatement fee over each year for which payment was not made, is 150% of the last Maintenance Fee that was paid by customer. The reinstatement fee shall be prorated from the date support services are ordered back to the date such support lapsed.

In addition to the reinstatement fee described above, the regular Maintenance Fee is due for the support period in question.

3.4 Service hours

Requests for support may be done anytime by means of electronic submission during Service Hours. Service Hours are from 9:00am – 3:00am (CET/CEST) on working days of SecurityMatters, according to the laws of the Netherlands, unless otherwise agreed upon.

3.5 Response times

SecurityMatters shall make every effort to ensure that the support is provided with due care and in accordance with this Technical Support Policy and any other arrangements and procedures agreed in writing with customer. SecurityMatters shall respond to a request of support as soon as possible, provided that SecurityMatters shall only respond on requests during Service Hours.

SecurityMatters shall be entitled to provide the Software with temporary solutions, or with software bypasses or problem-avoiding restrictions.

Priority	Meaning	Description	Response Time	Resolution time
urgent	Blocking Error	Error has a far-reaching and immediate effect on the normal use of the product. No alternative solution with similar options and performance is available.	4 hours	2 calendar days
High	Misbheavior	Error has a significant effect on the normal use of the product. An alternative solution is available (with some limitations).	8 hours	5 calendar days
Normal	Misbheavior	Error has a limited effect on the normal use of the Software.	2 working days	15 calendar days
Low	Misbheavior	Error has no negative effect on the normal use of the Software.	3 working days	20 calendar days

Response Time is intended to be the elapsed time beginning when Customer creates a service request until SecurityMatters first responds during Service Hours. Resolution Time is intended to be the elapsed time beginning when a support request is submitted by Customer until when the issue is resolved.

3.6 End of life support

SecurityMatters shall never be obliged to provide support services to any version that customer obtained from SecurityMatters more than 2 (two) years ago. However security patches to mitigate or fix product vulnerabilities are distributed only for last version and the version before the last one.

3.7 Use of third parties

SecurityMatters is entitled to use third parties to fulfil its obligations, provided it remains solely responsible and liable towards the Customer for any breach of the agreements with customer committed by such third parties in accordance with the provisions of the agreements.

3.8 Exclusions

Support services shall not include the fixing of Errors arising from or related to:

a) usage errors or the improper use of the product, including errors that occur during the data input process or in the data itself;
b) changes to the product other than those carried out by or on behalf of SecurityMatters;
c) use of the product contrary to the applicable conditions or contrary to the instructions in the Documentation;
d) changes to or errors, defects or shortcomings in the hardware or Software that is not included within the scope of the SecurityMatters Support Services to be carried out by SecurityMatters pursuant to this Agreement;
e) failure by Reseller or the customer to have SecurityMatters Support Services carried out on the Software in a timely manner;
f) the use of an older version of the Software that is no longer maintained by SecurityMatters;
g) the recovery of scrambled or lost data;
h) other causes that are not attributable to SecurityMatters.

If SecurityMatters carries out any services in connection with the above mentioned provisions, SecurityMatters shall be entitled to invoice these services in accordance with its standard rates. This shall not affect the other fees payable by the customer in respect of support of the Software.

SecurityMatters shall under no circumstances be obliged to recover data that has been scrambled or lost as a result of breakdowns and/ or sany Services.

Appendix – Support systems & documentation

Email

The support teams of SecurityMatters can be reached with the dedicated email address *support@secmatters.com* with usage questions, feedback and Error reports. The support team analyzes each request and opens a ticket in the internal ticketing system if necessary. In most cases the support team can directly respond with a solution or will offer a remote assistance call. For other cases, additional information, such as SilentDefense logs, screenshots or PCAPs may be requested.

Web portal

The SecurityMatters Portal is used to provide standard product documentation, software packages, product updates and security patches.

Remote access

By default, SecurityMatters has no remote access to the product. For the performance of the support, the support team may require temporary access to the Software or System. Remote access can be granted via a web conference tool, such as Webex or GoToMeeting. A web conference allows Reseller or the customer to watch and interact with the support team. For on-site assistance SecurityMatters requires networking access to the Systems. In some cases physical access may be required.