PAESSLER
THE NETWORK MONITORING COMPANY

WHITE PAPER

Is Your Security Really Secure?

White Paper

PRTG NETWORK MONITOR

Author: Thomas Timmermann, Senior Manager Technical Marketing, Paessler AG

Published: February 2016

Contents

Introduction 2
The Biggest Security Threats to Your IT 3
Tasks of a Monitoring Solution 3
Evaluation Checklist 4
- Comprehensive Monitoring Features Plus API 4
- “All Inclusive” 4
- “Unusual Behavior” 4
- Data Storage 4
- Publication of Data 4
- Usability 4
- Price and Licensing 5
- Test 5

Introduction

Many hot trends in IT follow the trajectory of a firework on the Fourth of July: A loud bang, burst of light and it’s over. Security is not one of those trends. Since the early days of networking, IT security has been a critical issue, and that remains true now more than ever. In 2015, a survey conducted by Paessler revealed that 58% of all surveyed IT administrators named security as one of their key tasks and constant challenges. In the past, a firewall and a virus scanner were sufficient to protect the network of an SME, but today, a number of interconnected solutions are needed to counteract the ever-evolving threats. All these IT security tools can only provide comprehensive security if their function is ensured and if the overview about all measures is being guaranteed. This requires a comprehensive security strategy that identifies potential hazards, sets up appropriate tools as a preventive protection, and controls and maps all this within one central solution.

The Biggest Security Threats to Your IT

Viruses and Trojans are no less dangerous today, just because they have been around since the dawn of the Internet. Again and again, new malware creates headlines and the ever progressing integration of everything and everybody constantly opens up new doors. Therefore, antivirus, firewall and intrusion detection systems are still justified. Bring Your Own Device (BYOD) and Internet of Things (IoT) create new opportunities for malware intrusion by expanding the threat vector. Previously, a simple ban on private disks, CDs or USB flash drives was sufficient, but today there are too many devices connected to the network. A general ban is neither practical nor sensible in most companies, because many employees use smartphones, tablets or laptops both privately and professionally. Even IoT creates new gateways, integrating numerous devices into the network which do not belong to IT and which come with a risk that is often difficult to assess. IT has to meet the risks involved in advance and find the right compromise between new opportunities and greater flexibility on the one hand and the necessary security on the other.

Not only malicious attackers threaten your data: failures or misconfigured devices and applications can also cause data loss. It is not about building lines of defense, but rather setting up a monitoring and early warning system which constantly monitors all critical components and immediately takes action on an error or, ideally, can already see the first signs of impending problems and warns you before the situation becomes critical. But IT is threatened by more than systemic risks. Physical disasters such as fires, floods, heat or theft should not be disregarded in a comprehensive safety concept. The best antivirus software can't protect you from a flood in the data center or an air conditioning failure in the server room.

For virtually every threat there is the right "antidote". Virus scanners and firewalls protect against malware, backup tools assure data, environmental sensors control humidity and temperature, and surveillance cameras have unwanted intruders in view. As long as all these systems operate reliably, your IT is relatively safe. But how do you make sure that everything works? And most of all: How do you keep track of the number of systems that are essential for the security of your IT? For a comprehensive security concept you need a monitoring solution as a kind of meta-security tool for the monitoring and control of individual measures.

Tasks of a Monitoring Solution

Are the virus definitions up to date? Are backups valid? Is the firewall online? Security only works when the security tools are working. The meta-security solution must be able to monitor traditional security tools input and to ensure its correct functioning. What happens when a virus is not detected or a Trojan bypasses the firewall? A suitable monitoring solution detects unusual behavior, such as the proliferation of traffic, the fast full running of memory or atypical email traffic, and will notify you accordingly.

Monitoring solutions continuously monitor performance and function of all components of your IT infrastructure, no matter whether it comes to hardware, software or data streams, in order to help prevent data loss and ensure optimum working conditions for your colleagues. On a higher level a monitoring solution is also able to monitor physical sensors as well as video cameras, thus ensuring that all systems operate and if necessary to notify respectively alert you when defined thresholds have been hit.

The essential aspect of a comprehensive security concept is clarity. Only if you are able to quickly and easily view all your security tools in real time, without having to call up each solution individually, you have a fighting chance to keep track of the entire security situation. The monitoring solution needs to be able to integrate all the tools used and to map them without great effort in a central overview. Not every monitoring tool is able to fulfill all these tasks. Some do not offer the necessary functions, while others are too expensive, too complex or too costly. Below is an overview of the criteria that you should consider when evaluating a comprehensive monitoring solution.

Evaluation Checklist

COMPREHENSIVE MONITORING FEATURES PLUS API

No monitoring solution can monitor your entire IT out-of-the-box, modern infrastructures are far too complex and heterogeneous. It is important that the right solution possesses all the necessary functions to monitor the entire IT infrastructure, including as many as possible of the common protocols, such as SNMP, Ping, FTP, http, NetFlow, sFlow, jFlow, WMI or packet sniffing. In conjunction with a well-documented API, almost all devices and applications can be connected – as well as other security tools, sensors, surveillance cameras, etc. And when all this can be done easily with the help of templates and examples, then you've almost found the appropriate solution.

"ALL INCLUSIVE"

Many monitoring systems are offered as a kit and require paid add-ons for almost any function, often at a significant cost. The right monitoring solution will offer as many options as possible in the most basic version. When doing price comparisons between monitoring tools, be sure to include the cost of add-on modules.

"UNUSUAL BEHAVIOR"

Of course you must be able to define individual limits for notifications and alarms in your monitoring solution. In addition, the software should also be smart enough to recognize unusual behavior even if the defined limits are not reached. For example, if a virus begins producing increased data traffic in your network, an intelligent solution can detect the atypical increase and inform you accordingly, so that you can take timely measures.

DATA STORAGE

Most monitoring solutions use SQL databases for storing monitoring data, but it is not the best fit. SQL databases are not designed for storing monitoring data (many small records that enter chronologically at short intervals, no write access is required), and monitoring data can't be stored in them in the RAW format due to the structure of a SQL server, but only as compressed averages. This can be especially problematic for a monitoring solution used as a security tool, if long-term research is required to identify vulnerabilities.

PUBLICATION OF DATA

Monitoring data can be published in various ways:

- As a live display (Dashboards and Maps) – Make sure that the solution doesn't only offer a Windows GUI, but a web interface, and if possible, apps for the most popular mobile systems. The dashboards and maps should be easily customizable and allow the presentation of the data in a clear and attractive manner: nicely prepared graphs are perceived with more enjoyment than old-fashioned and unsightly tables and lists.
- As HTML or PDF reports – These reports can be realized with standard tools or third-party tools, on-the-fly or scheduled at specified times. Reports usually offer the option to display the data for a defined period. This makes it possible to map and evaluate historical data.

Ideally, the solution provides built-in reporting, as well as ways to easily create customized dashboards and maps. It's very interesting being able to generate custom HTML maps on which all elements of the security concept can be clearly displayed. Possibly with a floor plan as background, on which the physical sensors, surveillance cameras, etc. can be positioned.

USABILITY

Even if a new monitoring solution is implemented and installed as a meta-security tool in a project, it still needs to be usable. If the solution is too complex in daily use, it will probably not work out as designed. Unused security software is not only a pointless investment, it also constitutes a security risk because it creates the illusion of security. Therefore, the ease of use of the software in the evaluation should be on top of the list. Sometimes it even makes sense to dispense with one or another additional feature, if for acceptance and use of the solution is ensured.

PRICE AND LICENSING

Of course, price and licensing play an important role when buying a monitoring solution. First and foremost, it's about transparency. Are all rates available? Is the licensing comprehensible? If modules and add-ons are available, which ones do you need from the outset or in the foreseeable future? There are often hidden cost traps in the form of modules or due to non-comprehensible licensing models so that you need an upgrade to a higher license after a short time.

TEST

Install and test the software! Don't rely on feature lists, consultants, or even the manufacturer's marketing. A meta-security solution is a key element in a comprehensive safety concept. Only if the software „feels good" it will find the necessary acceptance in order to be able to fulfill its role. And if already the trial proves to be difficult to obtain or cumbersome to install, then serious problems impend for the full version.

ABOUT PAESSLER AG

Paessler AG's award winning PRTG Network Monitor is a powerful, affordable and easy-to-use Unified Monitoring solution. It is a highly flexible and generic software for monitoring IT infrastructure, already in use at enterprises and organizations of all sizes and industries. Over 150,000 IT administrators in more than 170 countries rely on PRTG and gain peace of mind, confidence and convenience. Founded in 1997 and based in Nuremberg, Germany, Paessler AG remains a privately held company that is recognized as both a member of the Cisco Solution Partner Program and a VMware Technology Alliance Partner.

Freeware and Free Trial versions of all products can be downloaded from www.paessler.com/prtg/download.

Paessler AG · www.paessler.com · info@paessler.com