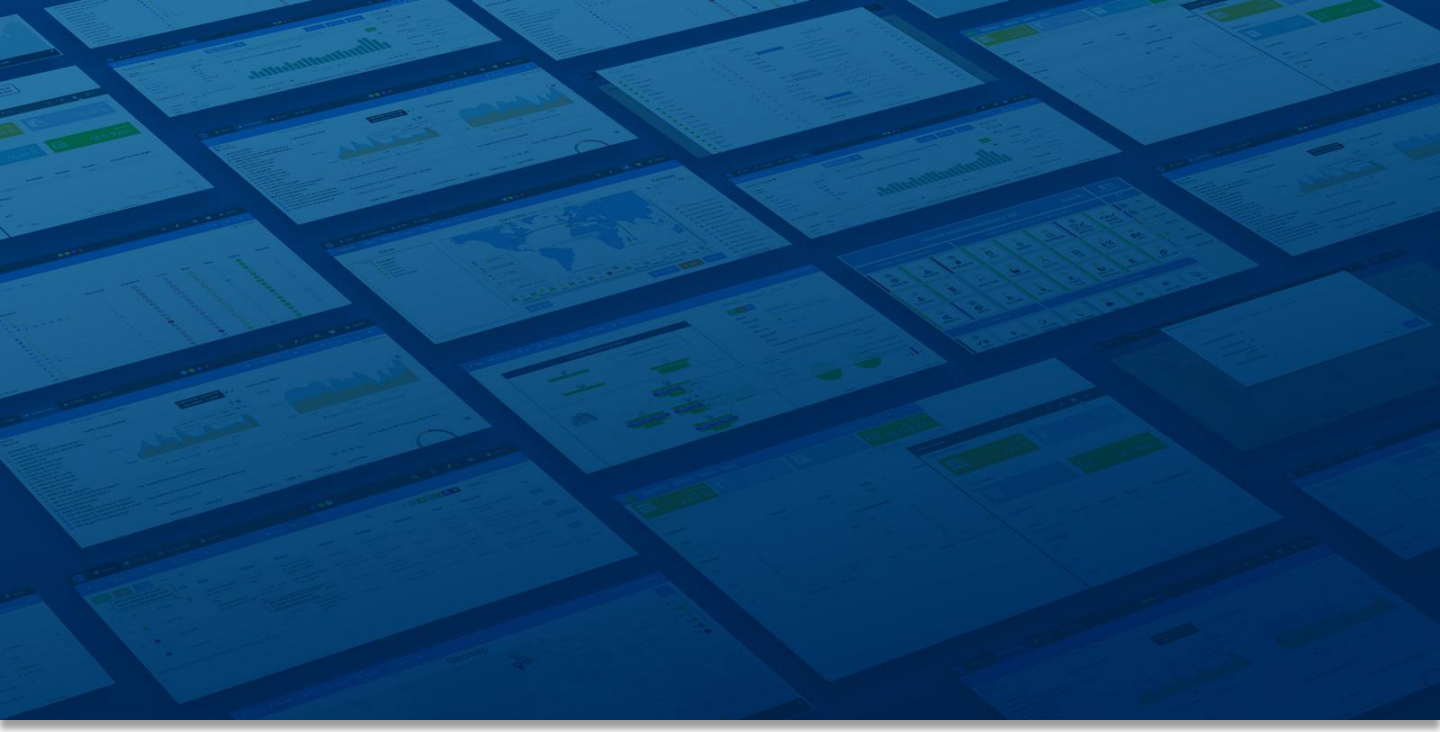


SOLUTION SIEM SERVICEPILOT

FULL-STACK LOG MANAGEMENT

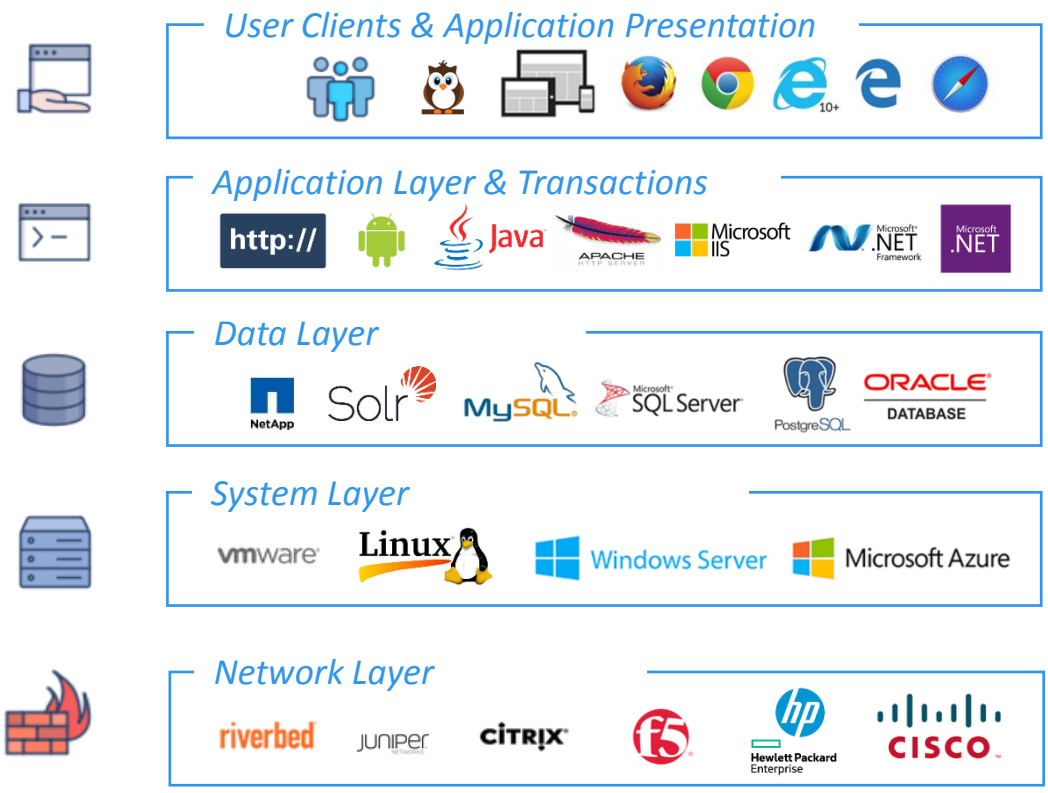
AVAILABILITY, PERFORMANCE
& LOG MANAGEMENT

servicepilot

A SOFTWARE SOLUTION FOR FULL-STACK LOG MANAGEMENT

ServicePilot is a complete Log Management solution and meets the needs of Centralized Event Management. ServicePilot centralizes both Logs, syslogs, traps, CDR,... as well as performance indicators from polling and/or application scripts for all your IT. This information is indexed, formatted and classified to simplify the configuration of analysis requests, the correlation of IS events and the generation of reports and alerts. ServicePilot has the necessary functionalities to detect, analyze and control security incidents.

COLLECTION OF EVENTS AND PERFORMANCE INDICATORS FOR ALL YOUR TECHNOLOGY SILOS



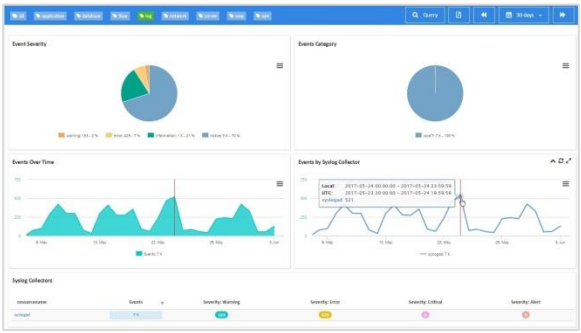
Some scenarios that can be easily realized with simple Queries:

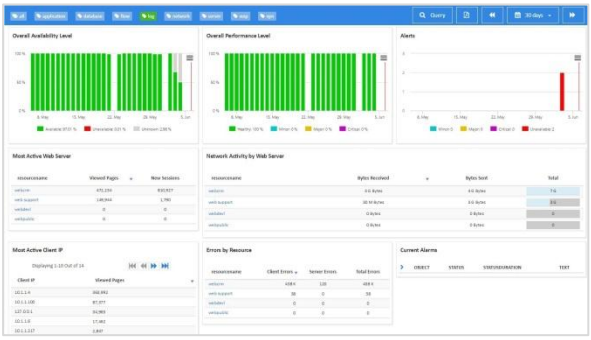
- Search for security keywords, alerts,... in a string of characters
- Analyze VPN connections
- Analyze the activity of robots that connect to your site by severity, IP source, location and type of event
- Analysis of "cdr" to identify fraud to prohibited destinations
- Analysis of configuration changes by users
- Analysis of user behaviour and access to different equipment
- Analysis of application response times as a function of CPU loads
- Analysis of TOS fields in a Netflow collection
- Analysis....

BY CREATING WIDGETS AND SETTING ALERT THRESHOLDS VIA THE WEB

CENTRALIZATION OF DATA

ServicePilot SOURCES allows you to quickly integrate your data from different IT resources and in different formats (flat files, Logs, Syslogs, traps, Windows Events...), correlate them and extract the valuable information you need to manage your IT and reduce risks.



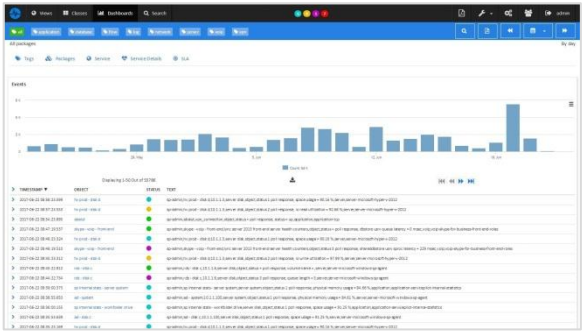


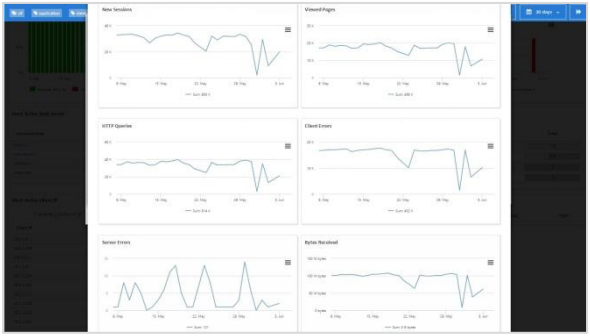
SYSTEM LOGS ANALYSIS

With its unique agent, ServicePilot not only supervises your server, it will also collect all events that may be correlated with performance problems to anticipate service degradation and possible security problems.

CONTEXT RESTRICTING

ServicePilot provides you with a contextual view of each event generated by your applications and server with a single click. By observing your server and network equipment data in the context of application performance, you have better visibility into user experiences, causes and impacts.

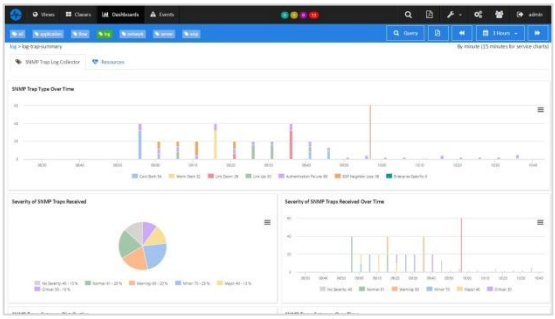


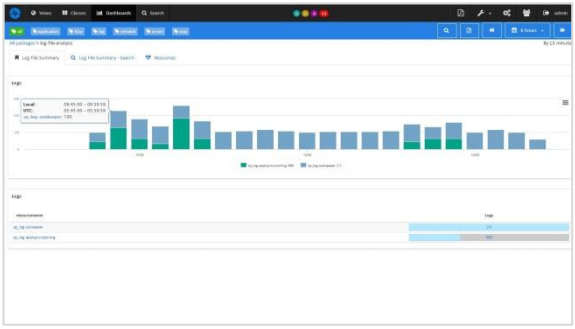


W3C LOGS ANALYSES OR IIS

ServicePilot allows to analyze web server log files. The ServicePilot agent collects data in W3C or IIS format that will be formatted in dashboards to analyze the activity of your Web servers, the number of pages viewed, network traffic generated, client and server errors,....

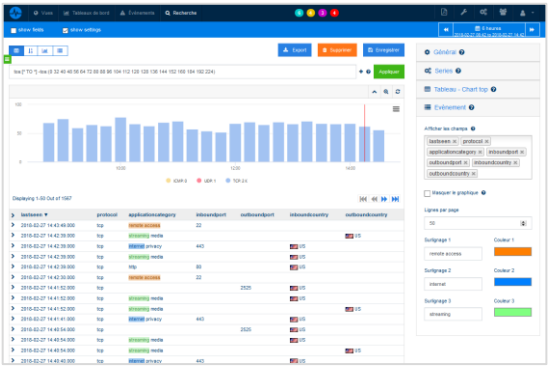
ANALYSIS OF SNMP TRAPS AND SYSLOGS
ServicePilot is able to receive and interpret SNMP Traps or Syslogs that are likely to be emitted by the equipment. These events are organized according to different criteria of priority, criticality, status and duration.





DEFINITION OF "SMART RULLES"
ServicePilot allows the definition of Smart Rule. These filtering rules can then be used to partition certain perimeters and not to group alerts from different perimeters within the same event tray.

RESEARCH AND CORRELATION
ServicePilot allows you to filter and correlate your logs to better identify security threats and abnormal behavior that could lead to a problem or attack. Keyword highlighting rules allow you to quickly answer any questions you may have.



AUTOMATIC PDF REPORTS
Permanent monitoring of the event logs of your servers, network equipment, firewalls and proxies allows you to intervene with a very high level of reactivity. On-the-fly or scheduled and automatic PDF reporting allows you to take action on any security issues.

THE ADVANTAGES OF CENTRALISED LOG MANAGEMENT

IS SECURITY
Analyzing all your log sources with the same solution allows you to identify and locate multiple threats.

COMPLIANCE
To create a unified view of your business and application KPIs from a single platform.

THREAT MAPPING
A simple analysis of event logs allows you to identify threats from within the company.

RESEARCH AND FILTERING
To obtain visibility into the impact of security events on infrastructure and applications.

7 REASONS TO CHOOSE SERVICEPILOT FOR FULL-STACK MONITORING

EASE OF DEPLOYMENT	Provisioning files, drawing tool, built-in packages for 150 technologies, universal agent collection, automatic discovery of resources
ADMINISTRATION SIMPLICITY	Windows installation, updates in minutes, no dependencies to manage
COLLECTOR DIVERSITY	SNMP, Traps, AXL, CDR VoIP, RTCP, RTCP-XR, FTP, Netflow, Logs, Syslogs, SQL, SMI, Telnet SSH, scripts,…
TRANSACTION ANALYSIS	Collecting user response times for JAVA,. NET, or HTTP application users
MONITORING INTERFACES	Unified mapping of all IT elements, end-to-end business views, IT service weather forecast...
ADVANCED PDF REPORTING	Preconfigured reports for each technology Capacity planning, trend analysis
NOSQL DATABASE	Storage of data in a NoSQL database, wizards to simplify the creation of widgets, dashboards or ad-hoc searches...

WEBSITE
https://www.servicepilot.com

PHONE
+33 2 40 60 13 30

EMAIL
info@servicepilot.com