

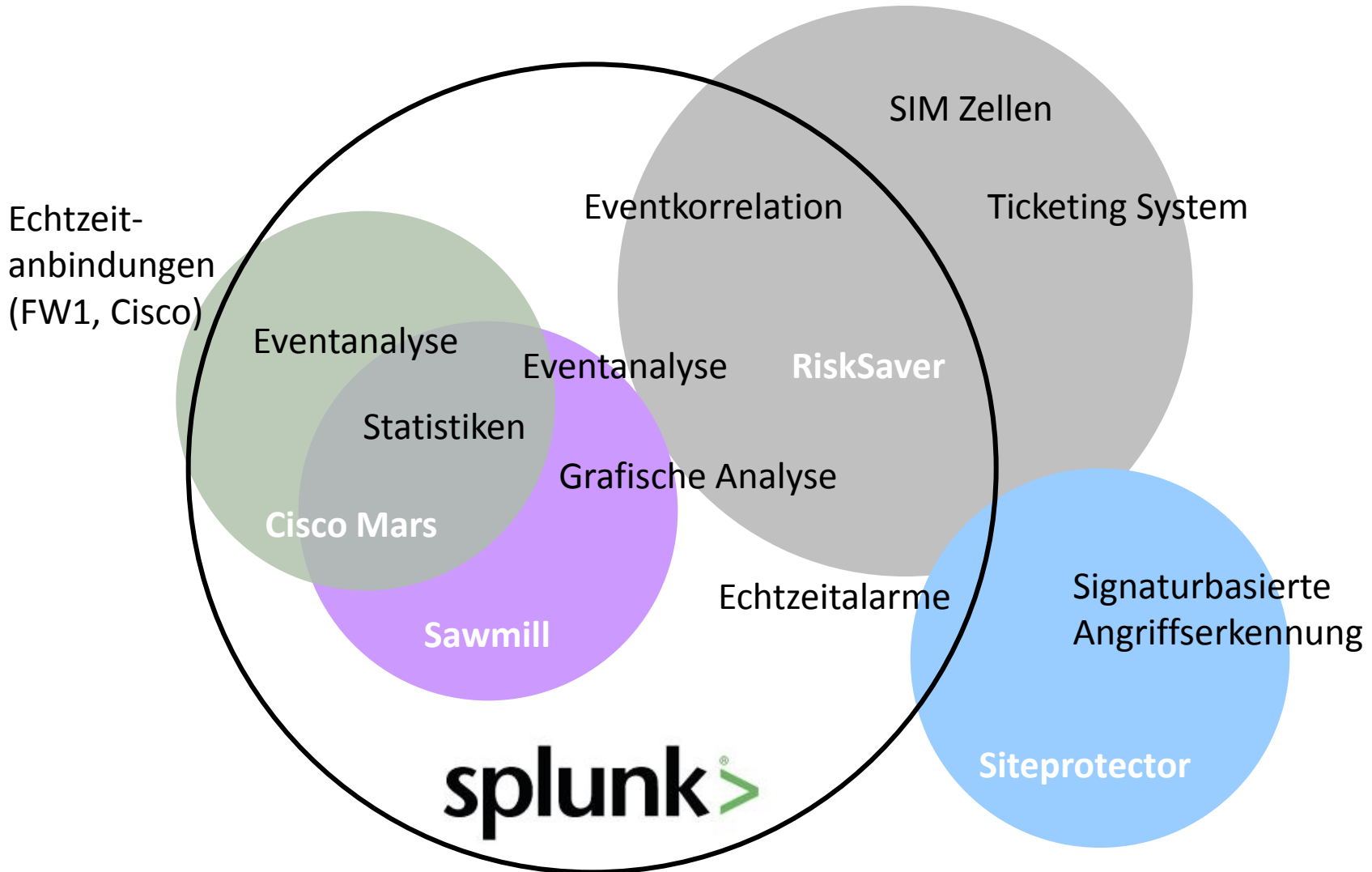
splunk [®] >

powered by BSK Consulting GmbH

Was ist **splunk**> ?

Abdeckung und Vergleich

„Kann viel aber nicht alles“



Aussehen

„aufgeräumt, effizient, intuitiv“

Menü

Suchfeld

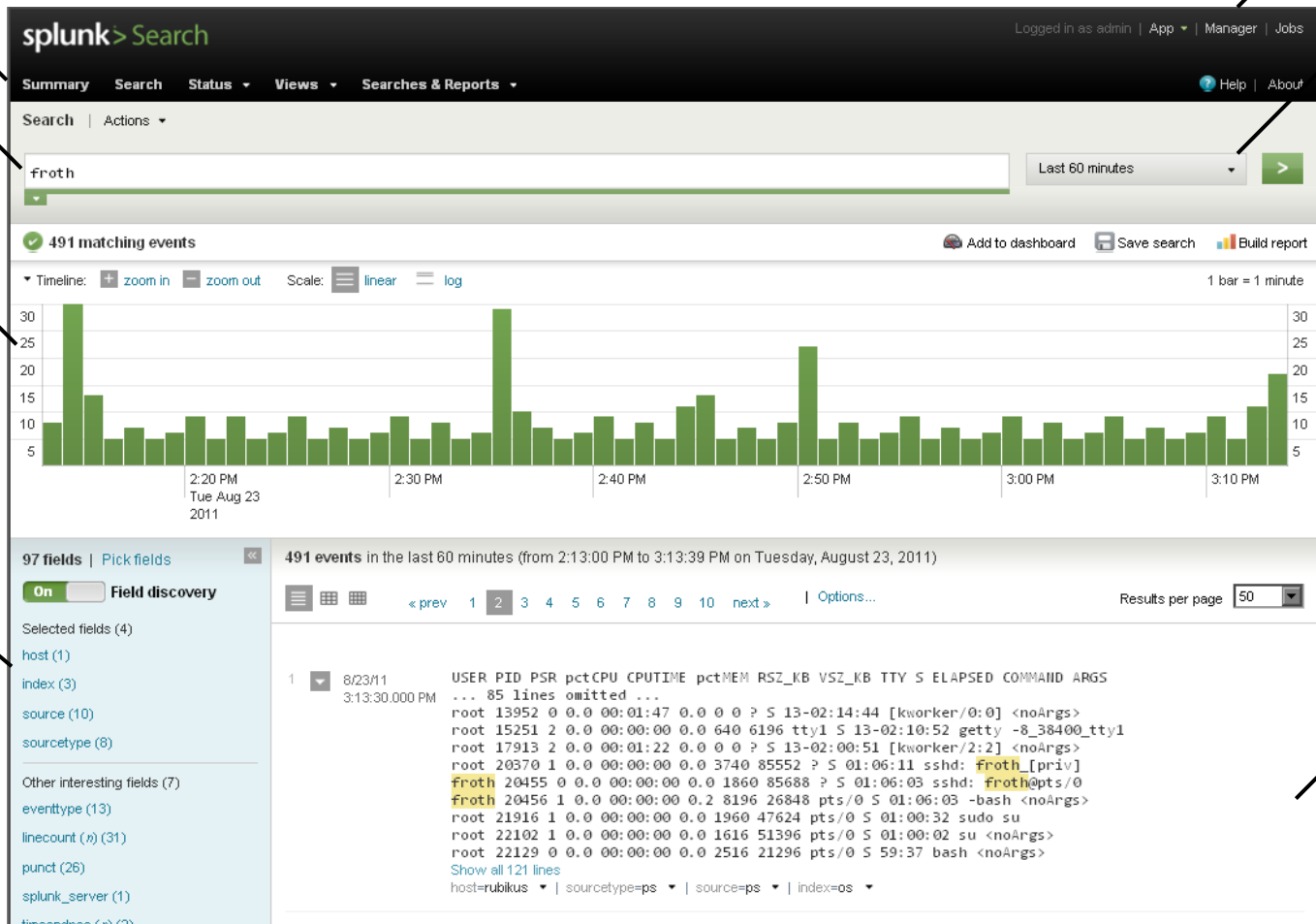
Echtzeit-
Statistik

Felder zur
Filterung

Administration

Zeitfenster

Suchbutton



Rohdaten

Was kann `splunk>` ?

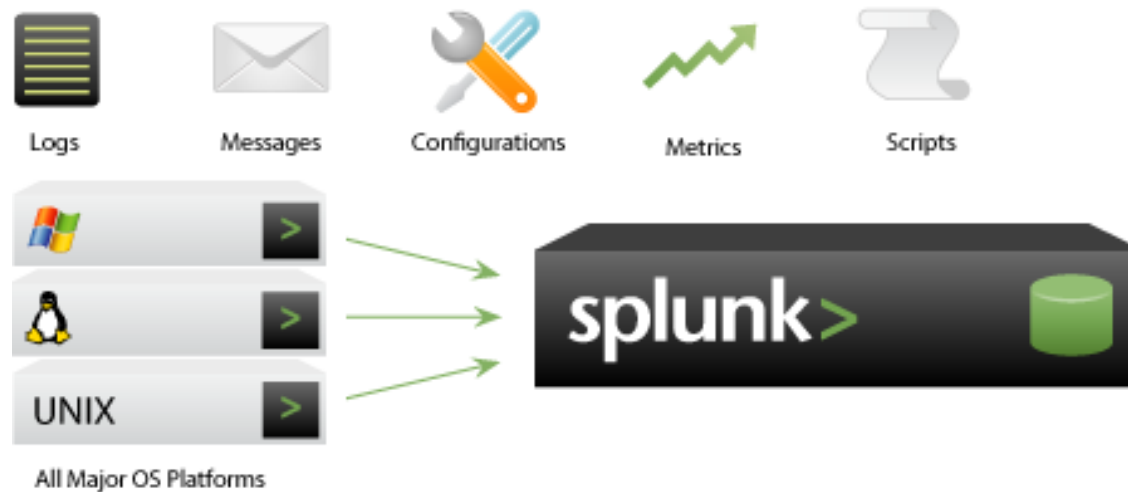
Datenquellen

„splunk saugt alles auf und indiziert es“



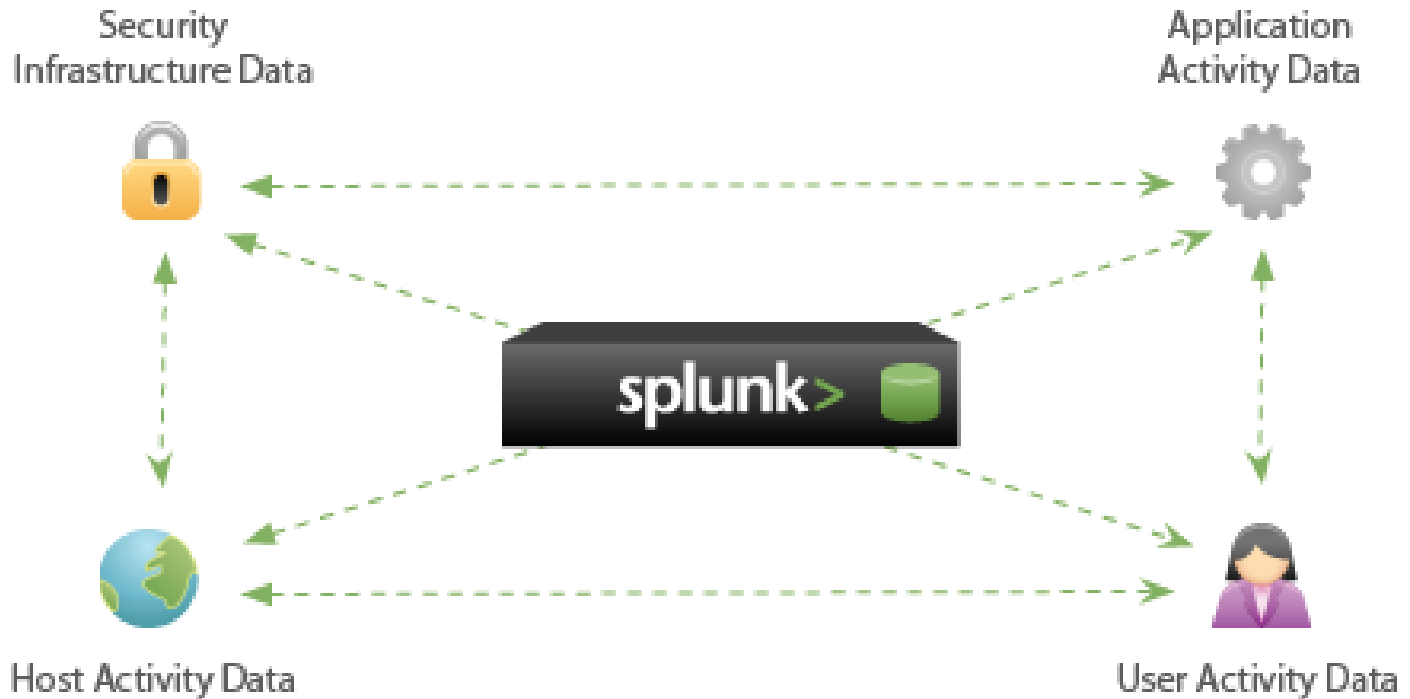
Datenbeschaffung

- Netzwerkfreigabe (Windows, NFS)
- Syslog
- „Universal Forwarder“



Datenkorrelation

„Alles in einen Topf“



Suche

„Googlen in den Logdaten“

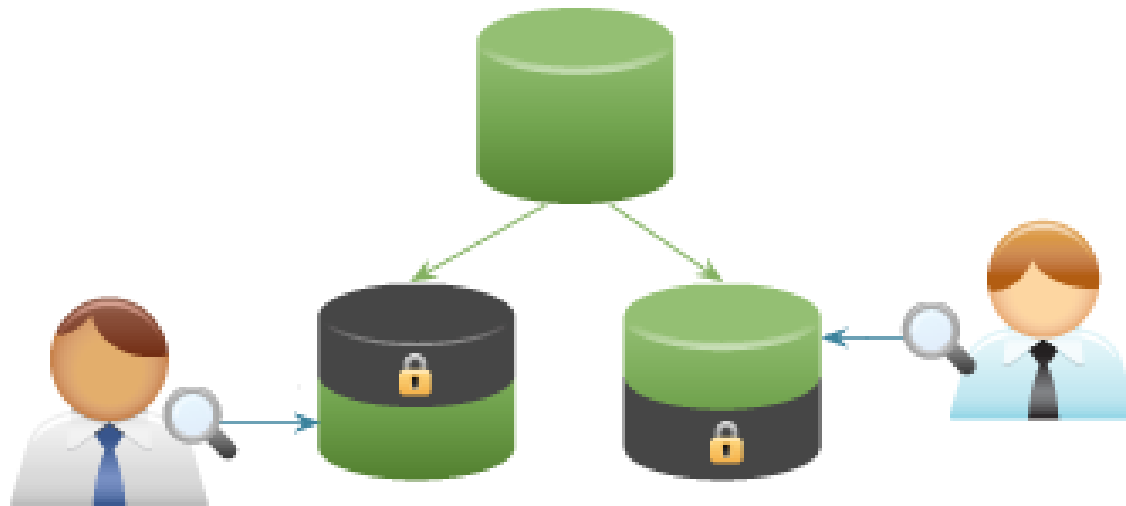
The screenshot displays the Splunk search interface. At the top, there is a search bar containing the term "froth" and a dropdown menu set to "Last 24 hours". Below the search bar, a green checkmark indicates "13,592 matching events". To the right of this status are buttons for "Add to dashboard", "Save search", and "Build report".

The timeline view shows a scale of "linear" and a zoom level of "1 bar = 1 hour". The search results are displayed in a list format, with the following entries:

- 2 8/23/11 2:35:08.000 PM 193.141.92.4 - froth [23/Aug/2011:14:35:08 +0200] "POST /splunk/en-US/util/log/js 1438 "https://rubikus.dyndns.org/splunk/en-US/app/search/flashtimeline" "Mozilla/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)" host=rubikus | sourcetype=access_combined | source=/var/log/apache2/ssl_access.log | index=webserve
- 3 8/23/11 2:35:07.000 PM 193.141.92.4 - froth [23/Aug/2011:14:35:07 +0200] "GET /splunk/en-US/api/messages/ 1603 "https://rubikus.dyndns.org/splunk/en-US/app/search/flashtimeline" "Mozilla/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)" host=rubikus | sourcetype=access_combined | source=/var/log/apache2/ssl_access.log | index=webserve
- 4 8/23/11 2:35:04.000 PM 193.141.92.4 - froth [23/Aug/2011:14:35:04 +0200] "POST /splunk/en-US/app/search/fl 1500 "https://rubikus.dyndns.org/splunk/en-US/app/search/flashtimeline" "Mozilla/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)" host=rubikus | sourcetype=access_combined | source=/var/log/apache2/ssl_access.log | index=webserve

Zugriffssteuerung

„Jedem das seine“



Was macht **splunk**> besonders?

Besonderheiten

„die nächste Evolutionsstufe des Monitorings“

- Schnell
- Realtime Graphing / Interactive Graphing
- Komprimierte Speicherung der Logdaten
 - geringer Speicherplatzverbrauch (1-5%)
 - große Log-Historie möglich (> 1 Jahr)
- Multiline Support
- Auto-Field-Discovery
- Auto-Regex-Builder
- Webapplikation und plattformunabhängig durch Python
- Herausragende Usability
- Knowledge-Import

splunk> Demo

Was kostet **splunk>** ?

Free vs. Professional

„Kosten nach Logvolumen“

- Free
 - bis zu 500 MB Logdatenvolumen pro Tag
 - keine Zugriffssteuerung (d.h. nur ein administrativer User)
 - Search, Dashboards, Reporting, Knowledge, Community Apps
 - kostenlos
- Professional
 - ab 500 MB Logdatenvolumen pro Tag
 - Echtzeitalarme
 - PDF-Reporting
 - Volle Zugriffssteuerung
 - ab 5000 Euro im Jahr (abhängig vom zu verarbeitenden Volumen)