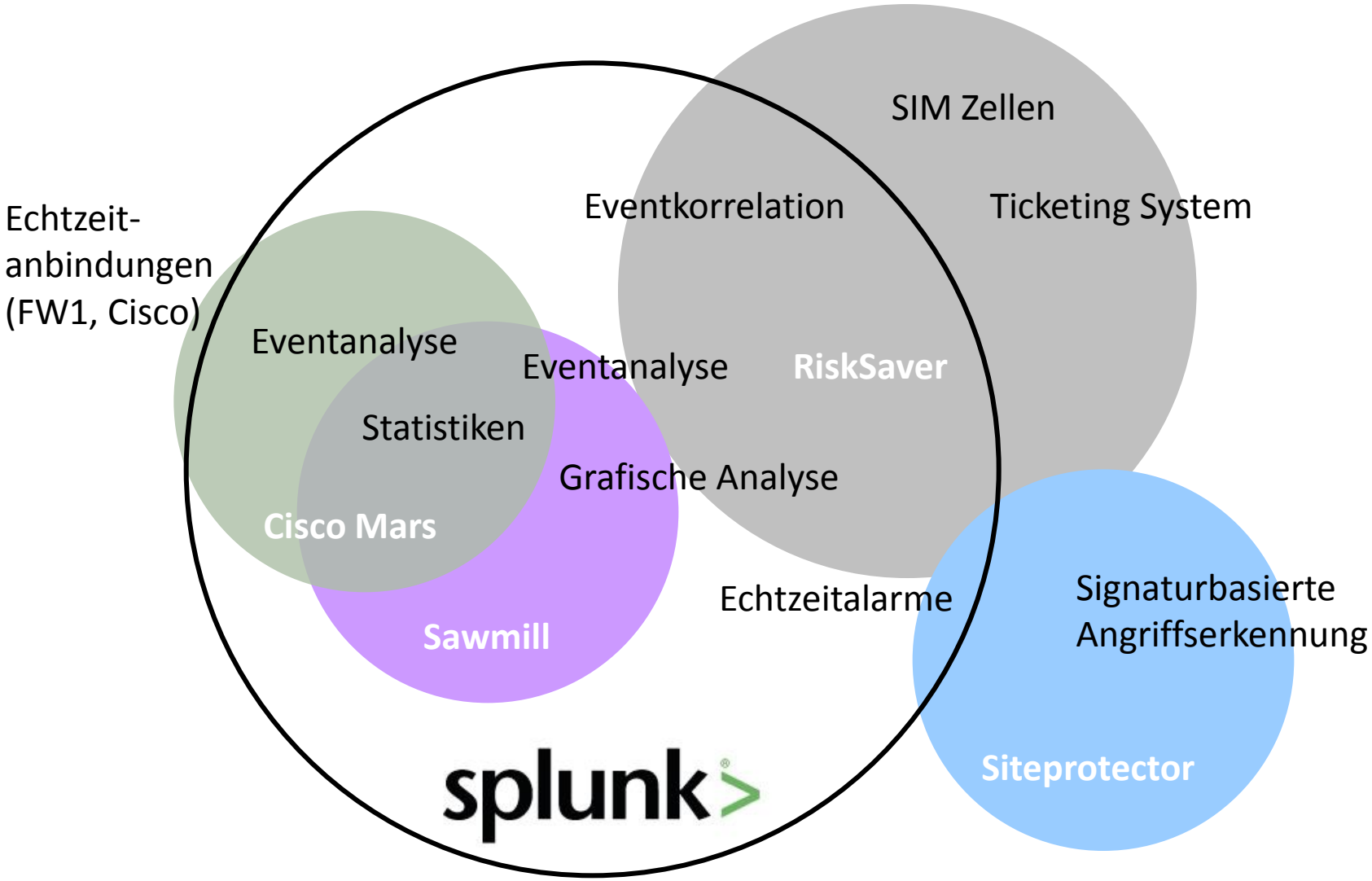

splunk>
powered by BSK Consulting GmbH

Was ist splunk> ?

Abdeckung und Vergleich

„Kann viel aber nicht alles“



Aussehen

„aufgeräumt, effizient, intuitiv“

Administration

Menü

Suchfeld

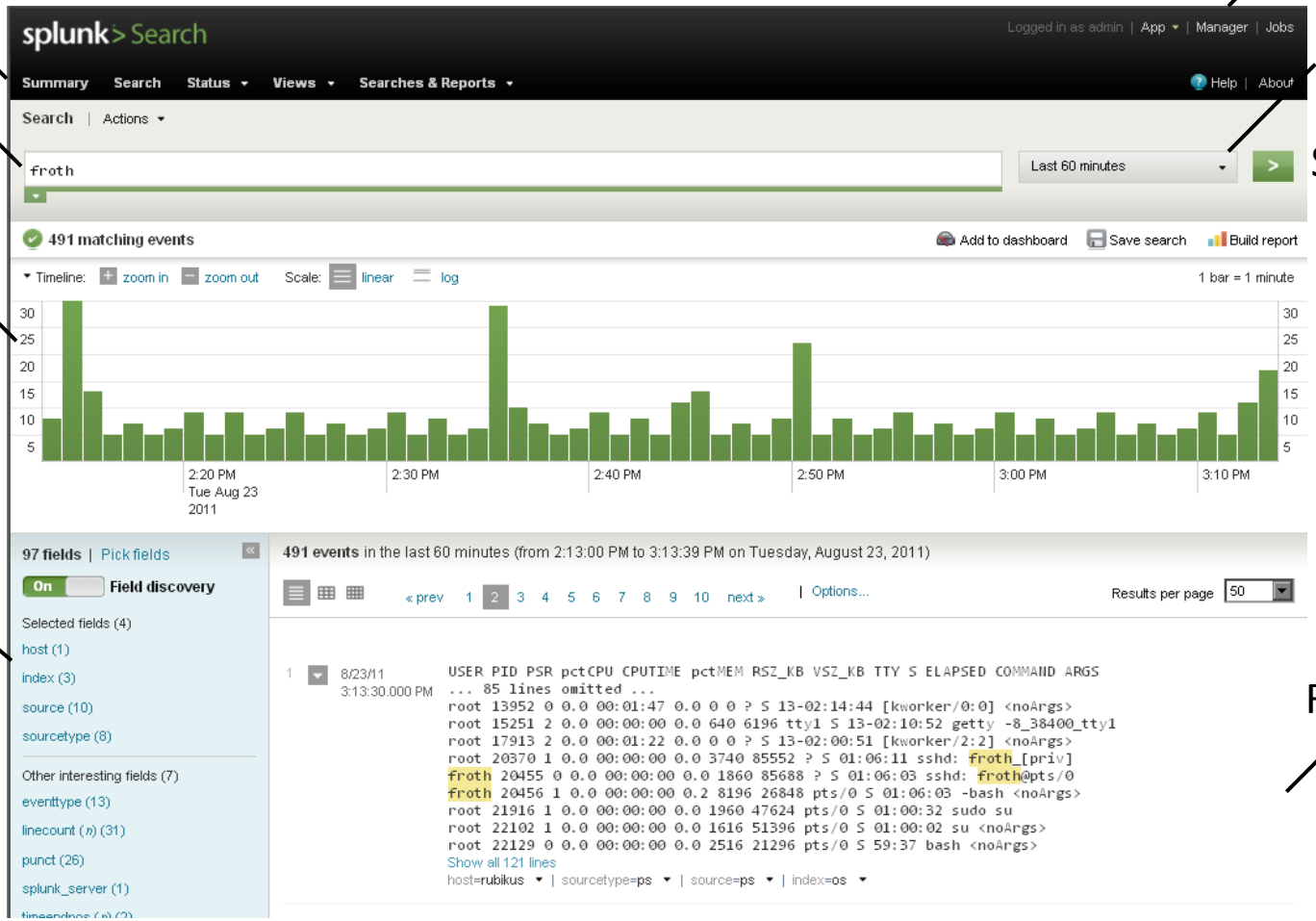
Zeitfenster

Suchbutton

Echtzeit-Statistik

Felder zur Filterung

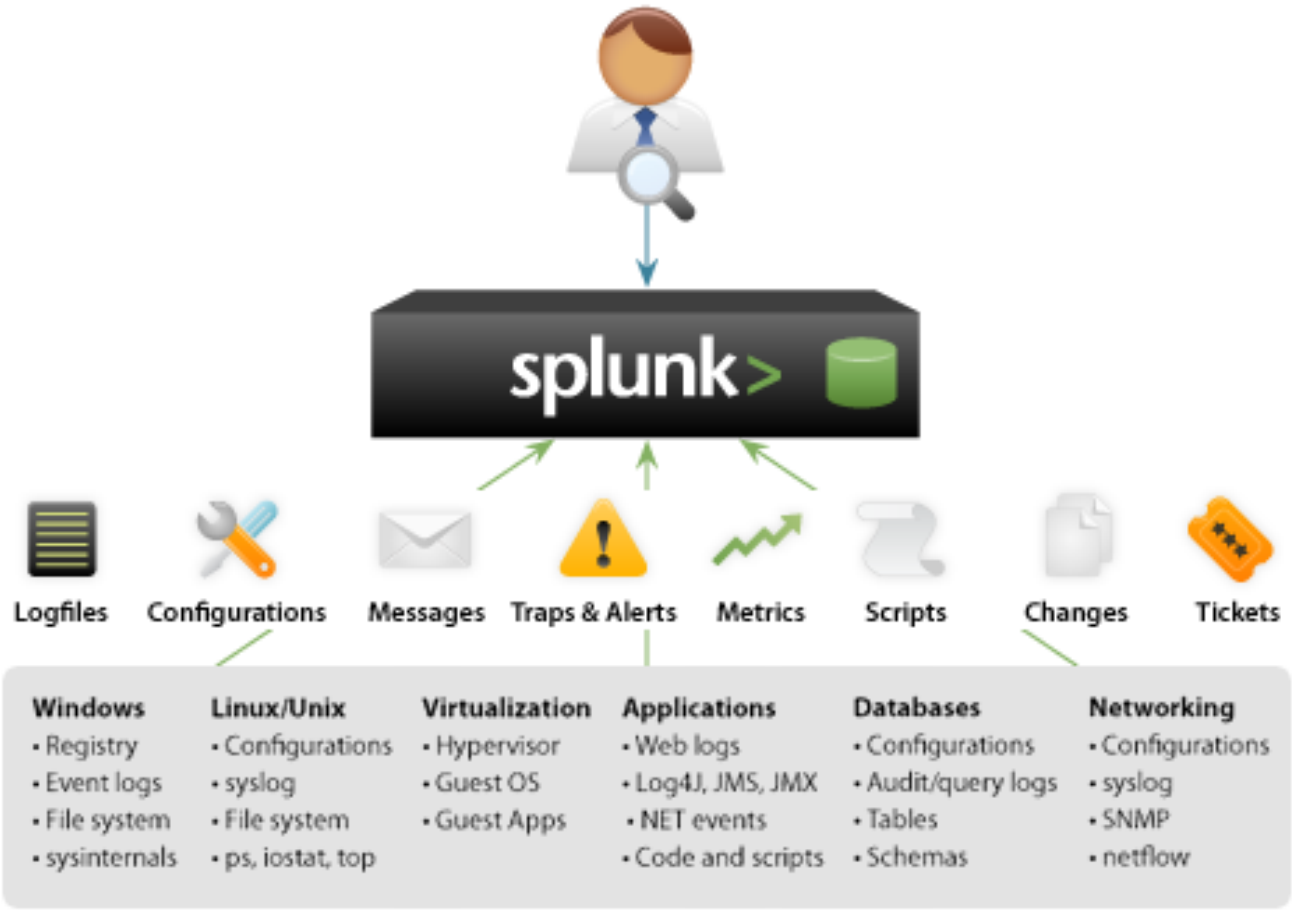
Rohdaten



Was kann splunk> ?

Datenquellen

„splunk saugt alles auf und indiziert es“

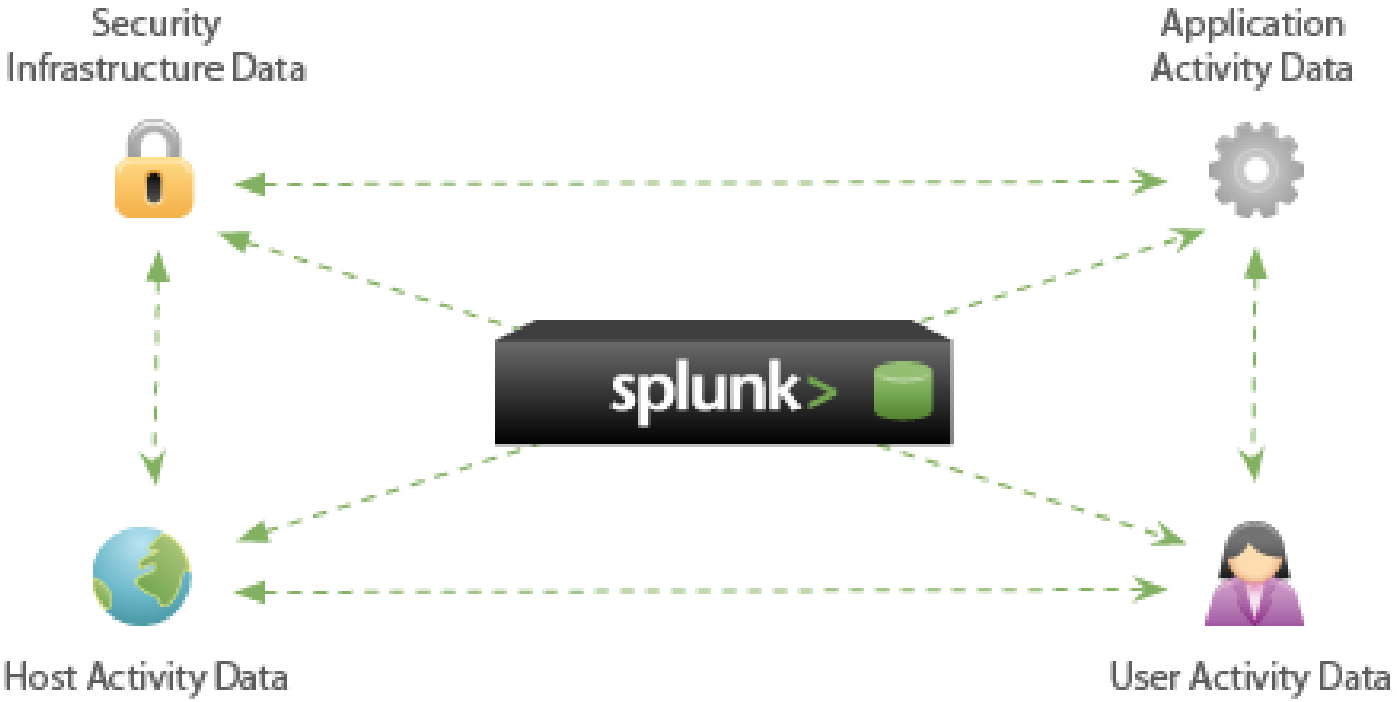


Datenbeschaffung

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

Datenkorrelation

„Alles in einen Topf“

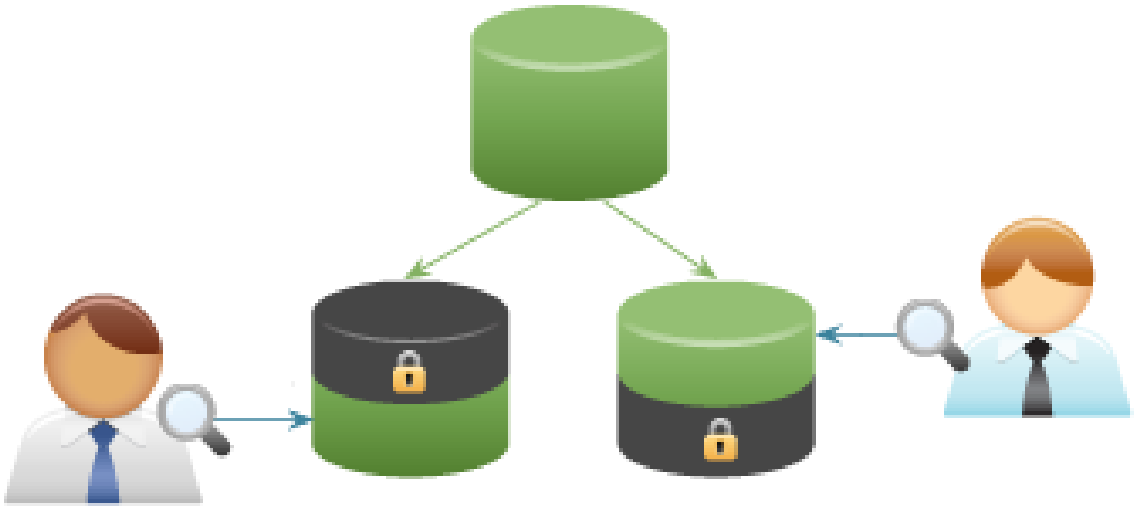


Suche

„Googlen in den Logdaten“

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

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)