sqrrl

Target. Hunt. Disrupt.

R-SCOPING THE HUNT

An integrated solution with Reservoir Labs

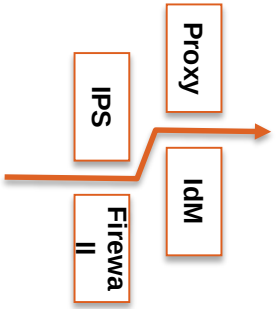
THE DETECTION AND RESPONSE GAP

What?

205 days on average to detect a breach

Advanced adversaries

Perimeter defenses and current detection not sufficient

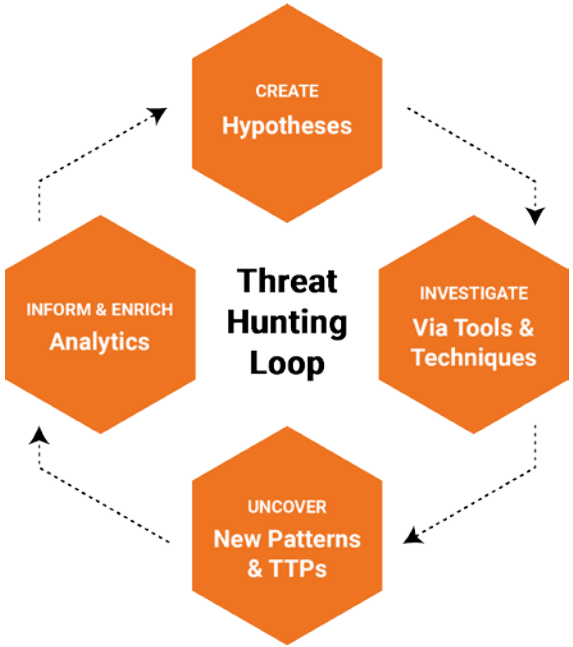


Why?

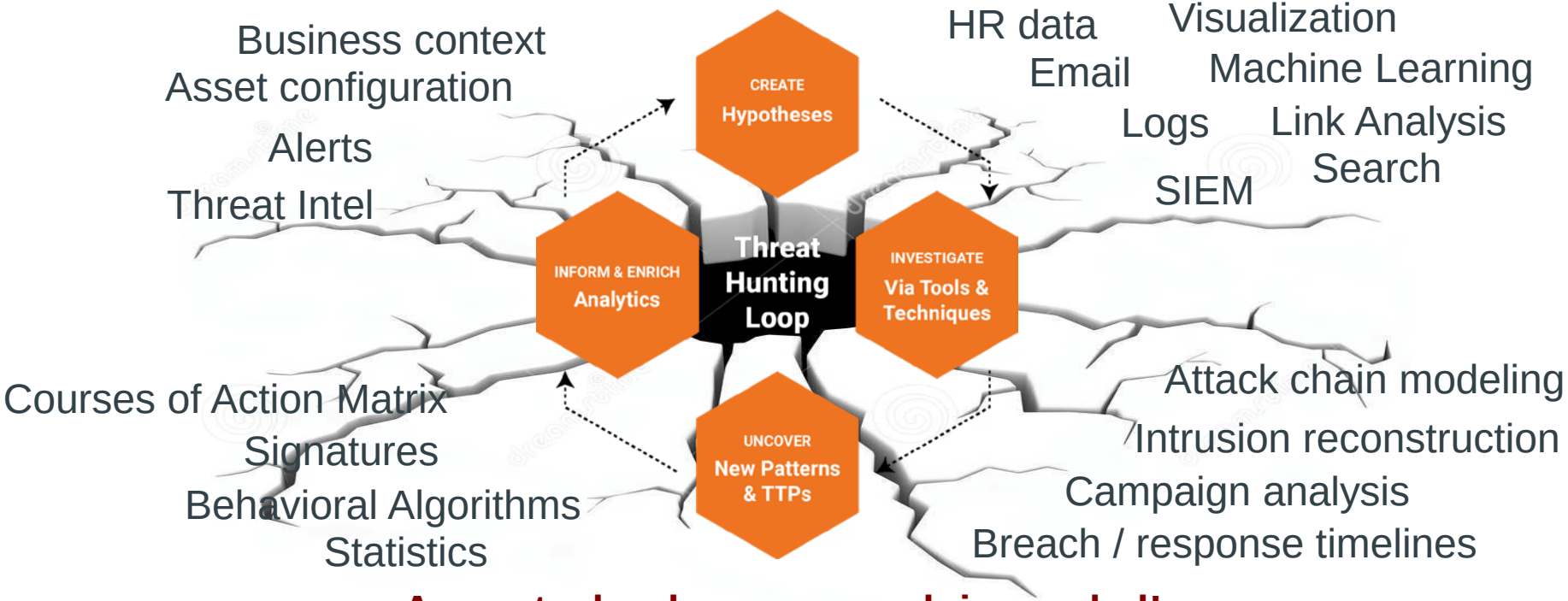
1. **Limited effectiveness of signatures and rules**
2. **Increased attack surface and hacking tool availability**
3. **Drowning in alerts and data**
4. **Not enough security ninjas**

Faster and more powerful detection and response capabilities are required

WHAT IS THREAT HUNTING?



HUNTING PROCESS FRAGMENTED BY TOOLS



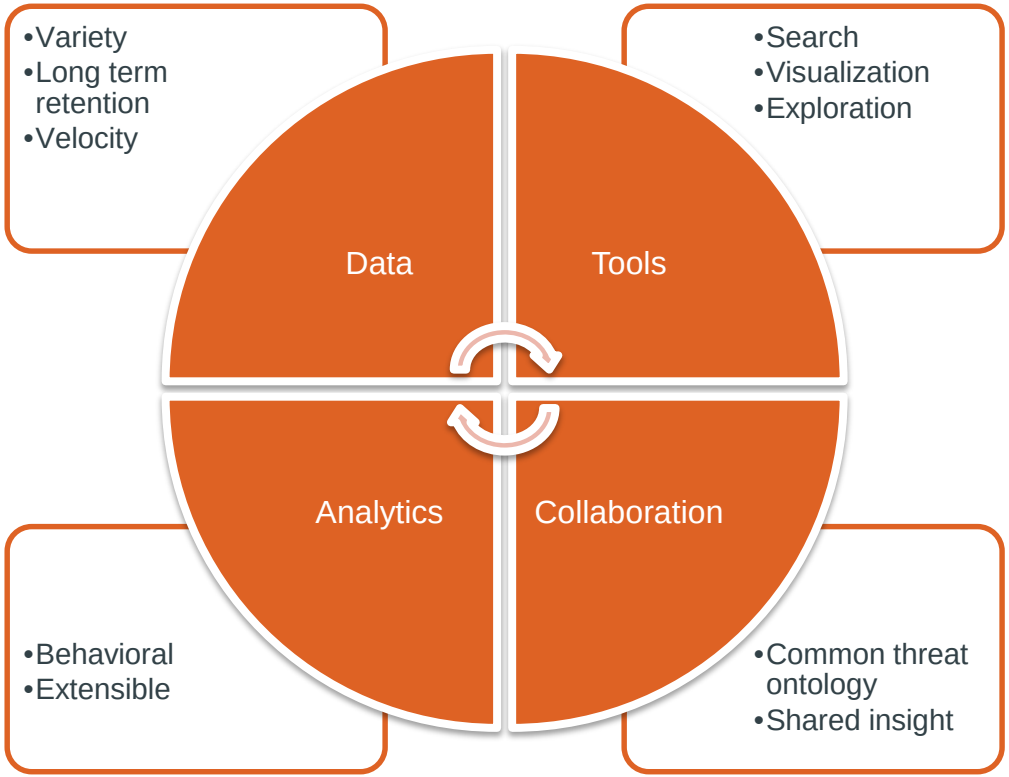
A new technology approach is needed!

HOW YOU'RE PROBABLY HUNTING NOW

Log-oriented techniques can only get you so far

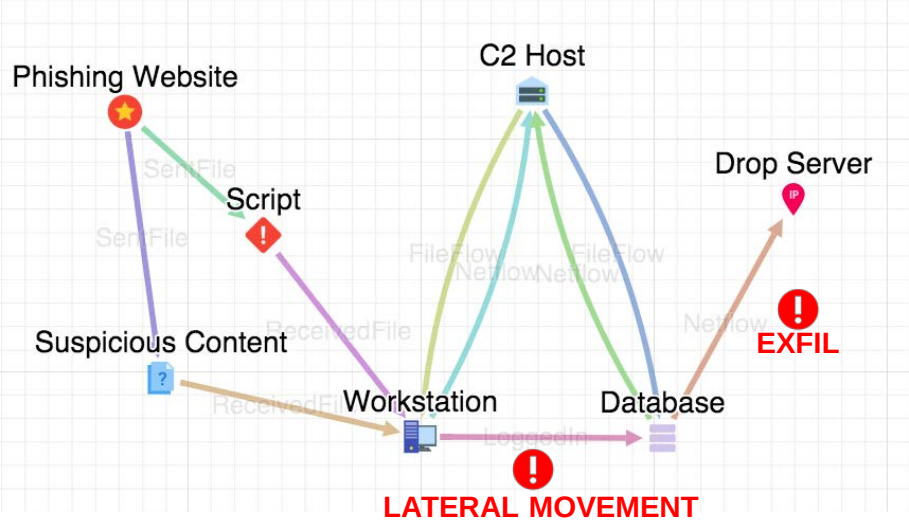
```
Davids-MacBook-Pro-2:/Users/bianco/temp> grep 6d01739d1d56c64209098747a5756443 *.log
files.log:922712498.188977      Fz892b2SFbpSayzLyl      172.16.113.204  194.7.248.153
        Cr4RV91FD8iPXBuoT6      SMTP 1  MD5,SHA1        text/x-c        0.000000        T       F       1522    -       0
        0       F       -       6d01739d1d56c64209098747a5756443 0d1c6b7dcc82b05c719d4cc9dd8d8577e8cb36cb
        -
Davids-MacBook-Pro-2:/Users/bianco/temp> grep Cr4RV91FD8iPXBuoT6 *.log
conn.log:922712498.086765       Cr4RV91FD8iPXBuoT6      194.7.248.153   1027    172.16.113.204  25      tcp
        smtp    0.113325        1923    336     SF      ShAdDafF        13      2447    12      820     (empty)
files.log:922712498.188977      Fz892b2SFbpSayzLyl      172.16.113.204  194.7.248.153
        Cr4RV91FD8iPXBuoT6      SMTP 1  MD5,SHA1        text/x-c        0.000000        T       F       1522    -       0
        0       F       -       6d01739d1d56c64209098747a5756443 0d1c6b7dcc82b05c719d4cc9dd8d8577e8cb36cb
        -
smtp.log:922712498.119932       Cr4RV91FD8iPXBuoT6      194.7.248.153   1027    172.16.113.204  25      1
        delta.peach.mil         <hamishs@delta.peach.mil>       <tierneyr@goose.eyrie.af.mil>   Mon, 29 Mar 1999
08:01:38 -0400  -       tierneyr@goose.eyrie.af.mil     -       <19990329080138.CAA2048>        -       Phonetics
software Tech,  -       (from mail@localhost) by delta.peach.mil (SMI-8.6/SMI-SVR4)\x09id: CAA2048; Mon, 29
Mar 1999 08:01:38 -0400 -       250 Mail accepted       172.16.113.204,194.7.248.153    -       F
        Fz892b2SFbpSayzLyl      F
```

HUNTING TECHNOLOGY REQUIREMENTS



SQRRL BEHAVIOR GRAPH

Unique approach to managing security data



KEY CAPABILITIES:

- Asset / activity modeling
- Visualization, exploration, search
- Behavioral analytics
- Big data scale & security

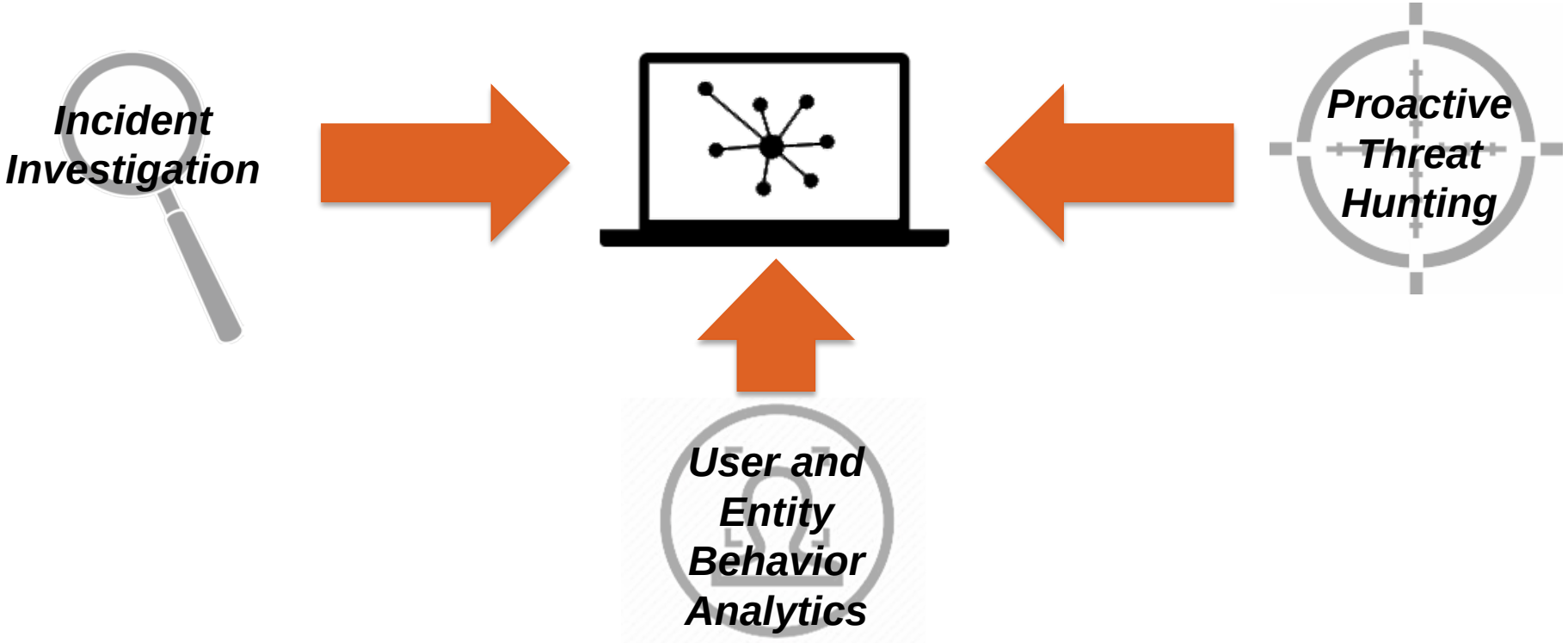
SOLUTION: THREAT HUNTING PLATFORM (THP)

A unified environment for:

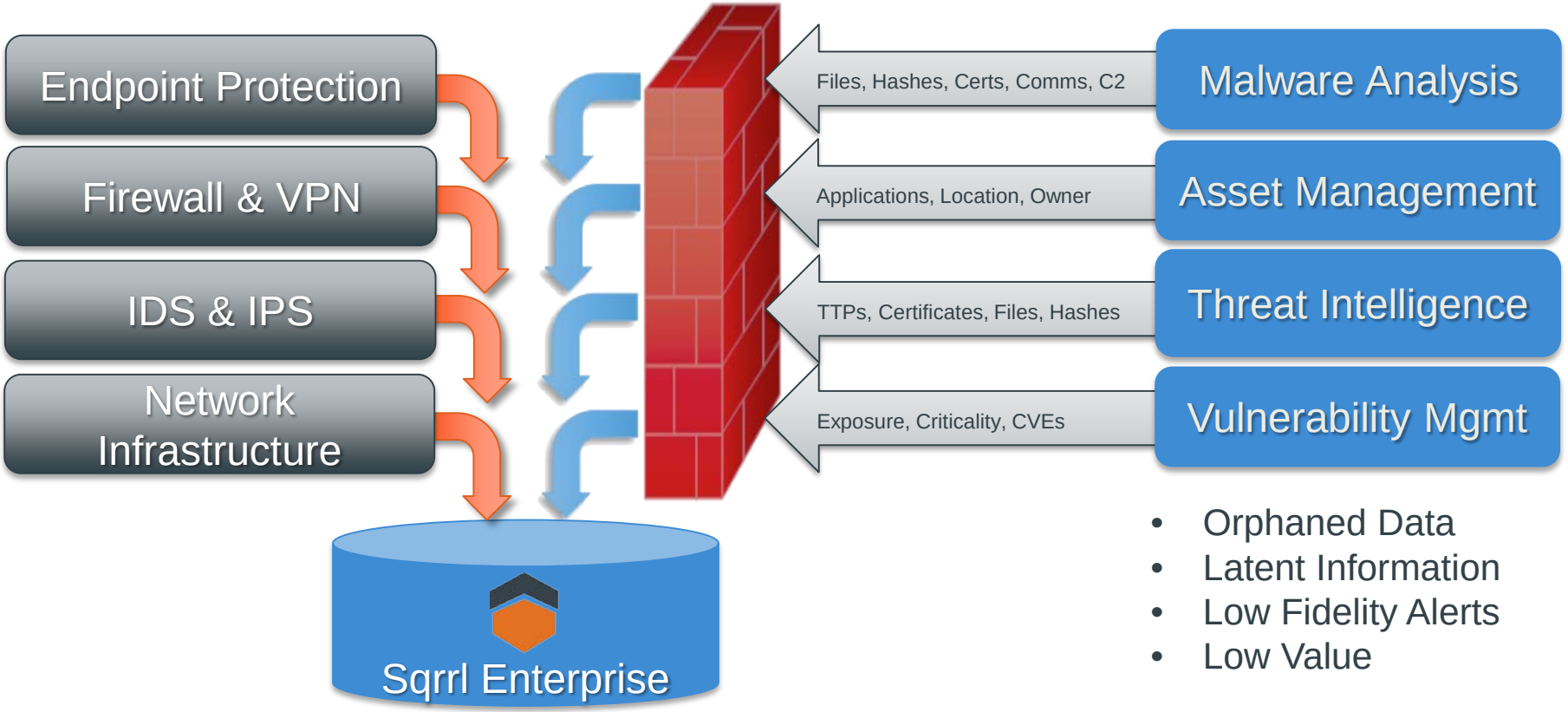
- Collecting and managing big security data
- Detecting and analyzing advanced threats
- Visually investigating attack TTPs and patterns
- Automating hunt techniques
- Collaborating amongst security analyst teams

SQRRL ENTERPRISE

Sqrrl's approach to the THP

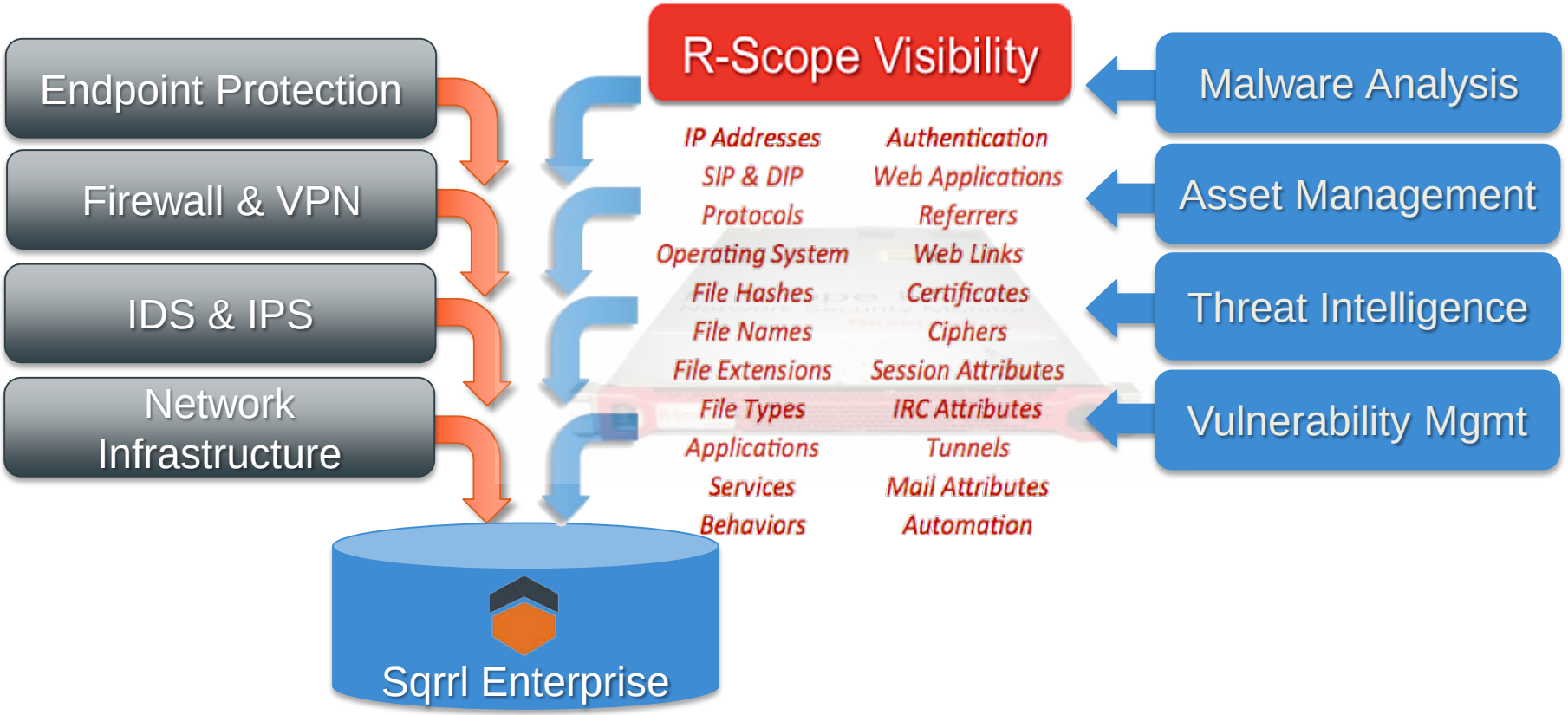


SECURITY DATA CONTEXT GAP



- Orphaned Data
- Latent Information
- Low Fidelity Alerts
- Low Value

R-SCOPE BRIDGES THE CONTEXT GAP



THE BEST THREAT HUNTING EXPERIENCE

sqrrl

Reservoir Labs

THANK YOU!

Reservoir Labs

How To Learn More?

To learn more about Sqrrl:

- Download Sqrrl's Threat Hunting eBook from our website
- Download the Sqrrl Product Paper from our website
- Request a Test Drive VM from our website
- Reach out to us at info@sqrrl.com