

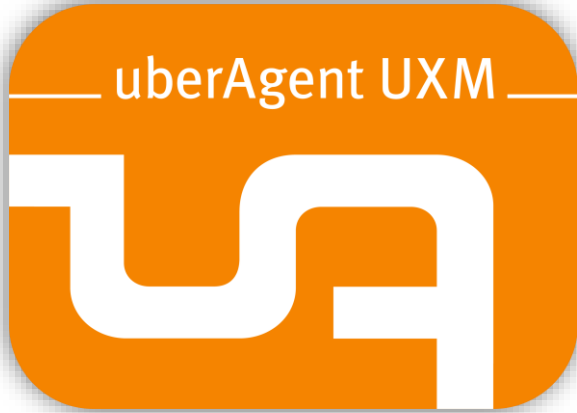
Helge Klein, vast limits

uberAgent

Endpoint security & performance monitoring

- **Threat** detection
 - **Application** analytics
 - **Performance** monitoring
- 
- An abstract graphic at the bottom of the slide featuring overlapping line charts and bar charts in shades of blue and yellow, set against a teal background.

One agent, two products



Performance



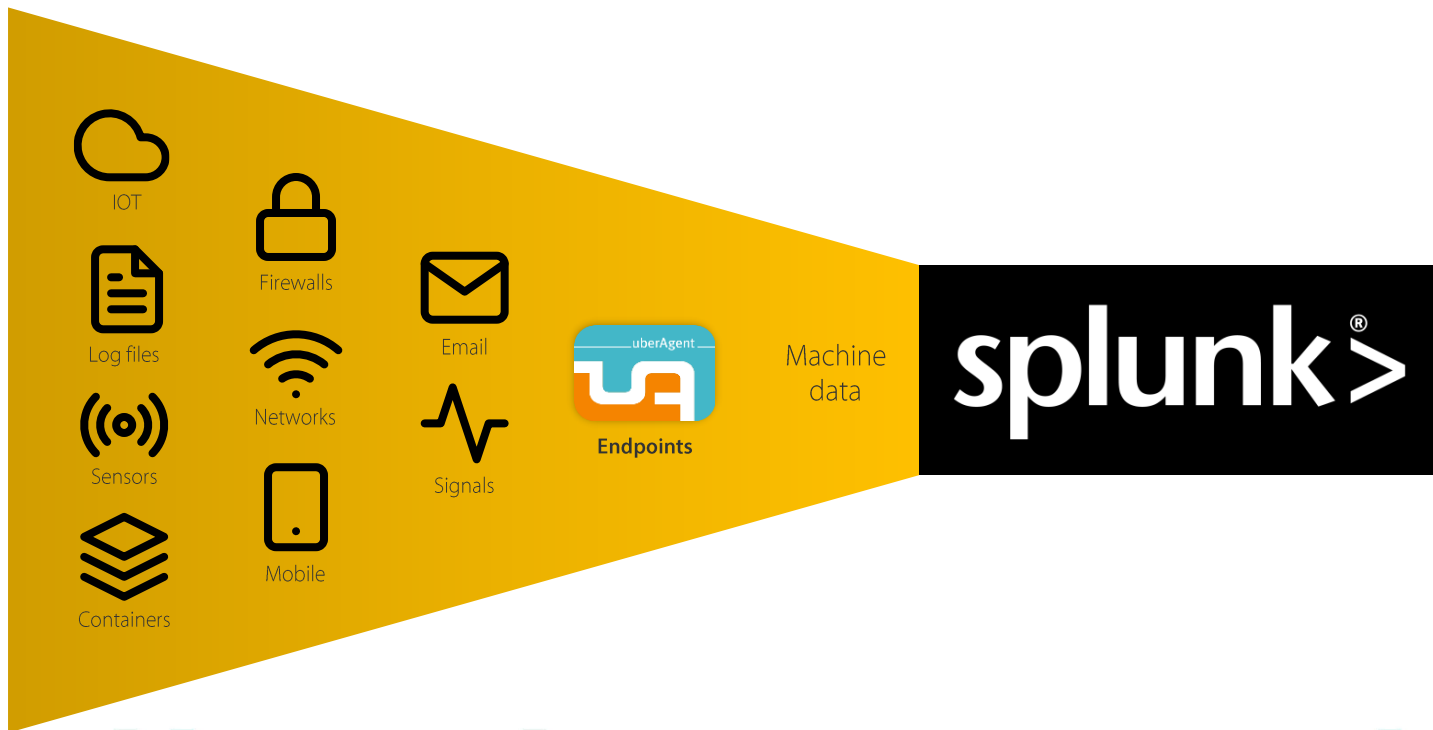
Security



Architecture



Architecture

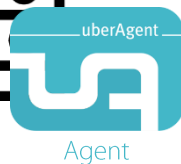
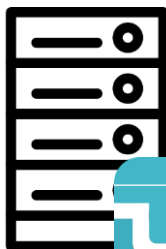


Architecture



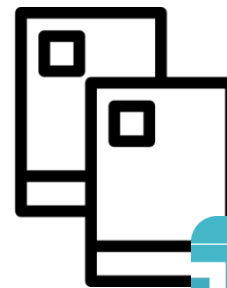
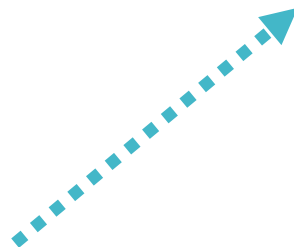
SBC
VDI

CITRIX[®]
vmware
Microsoft



PCs

Windows
macOS



splunk>



uberAgent ESA

Endpoint Security Analytics



Endpoint security market

EDR

- Detection **gaps**
- Customers lulled into **false sense of security**
- Splunk: **integration not great**
- No visibility of normal behavior
- Rule customizations can be difficult



Endpoint security market



EDR

- Detection **gaps**
- Customers lulled into **false sense of security**
- Splunk: **integration not great**
- No visibility of normal behavior
- Rule customizations can be difficult

Homegrown

- Sysmon + custom scripts + Splunk
- Requires intensive **development & testing**
- Rule maintenance: **customer**
- Dashboard creation: **customer**



Endpoint security market



EDR

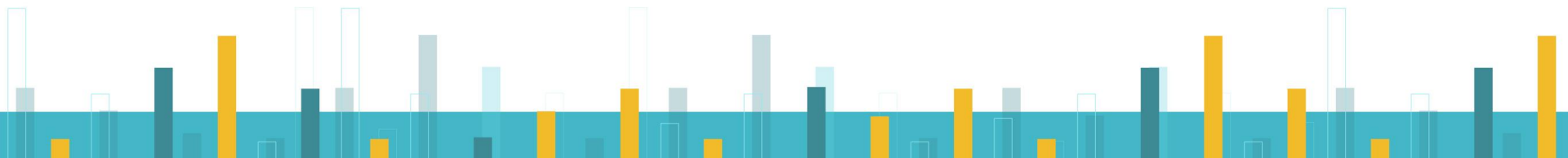
- Detection **gaps**
- Customers lulled into **false sense of security**
- Splunk: **integration not great**
- No visibility of normal behavior
- Rule customizations can be difficult

uberAgent

- **Ready-to-use**
- Sysmon & Sigma **rule converters**
- Splunk: **perfect integration**
- Visibility into anomalous & normal behavior
- Customizations easily possible

Homegrown

- Sysmon + custom scripts + Splunk
- Requires intensive **development & testing**
- Rule maintenance: **customer**
- Dashboard creation: **customer**



EDRs need uberAgent



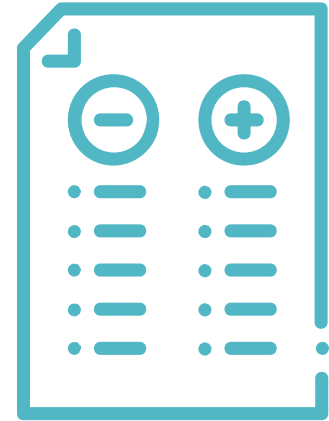
Why you should **add uberAgent to your EDR:**

1. Visibility into **normal behavior**
2. Second opinion
 - **Verify the data** collected by the EDR
3. Consistency
 - **EDRs detections are opaque**
 - Know what you're collecting with a transparent, rule-based product



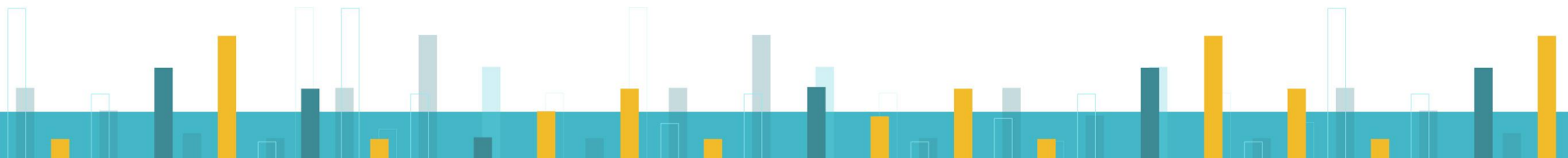
ESA vs. Sysmon

- **Easy start** through predefined rules
- Rule **converters** (Sigma/Sysmon → ESA)
- Rule definitions: **no XML**
- Rule **editor** (uAQL Studio)
- Splunk **dashboards** & Splunk ES integration
- No additional log collection agent
- **Support**



UXM

- Citrix sessions
- Network connections
- Browser activity
- User logon/logoff
- Application usage
- App & machine inventory



Activity Monitoring Engine

- Registry
- DNS queries
- Image load
- File ACLs
- Authenticode
- PE hashes
- Process start/stop
- Network connect/send/recv
- Remote thread creation
- Process tampering
- *More to come*

UXM

- Citrix sessions
- Network comm. & issues
- Browser activity
- User login/logoff
- Application usage
- App & machine inventory



Value proposition



Value proposition

- Our **mission**:
 - Visibility
- Help IT understand what's going on
 - **Don't drown them in data**
 - Provide valuable information instead
- **Partner-friendly**
 - Easy to build solutions on top of



Why uberAgent?



- **One agent** for security, UX & performance
 - Minimal footprint
 - **Quality** metrics
- Proven **scalability**
 - Largest deployments: **250,000+ endpoints**
- Built for **enterprise IT**
 - Easy to use but flexible to configure



More information



<https://uberagent.com>



info@uberagent.com



The uberAgent company

We create enterprise software that IT pros enjoy working with.

