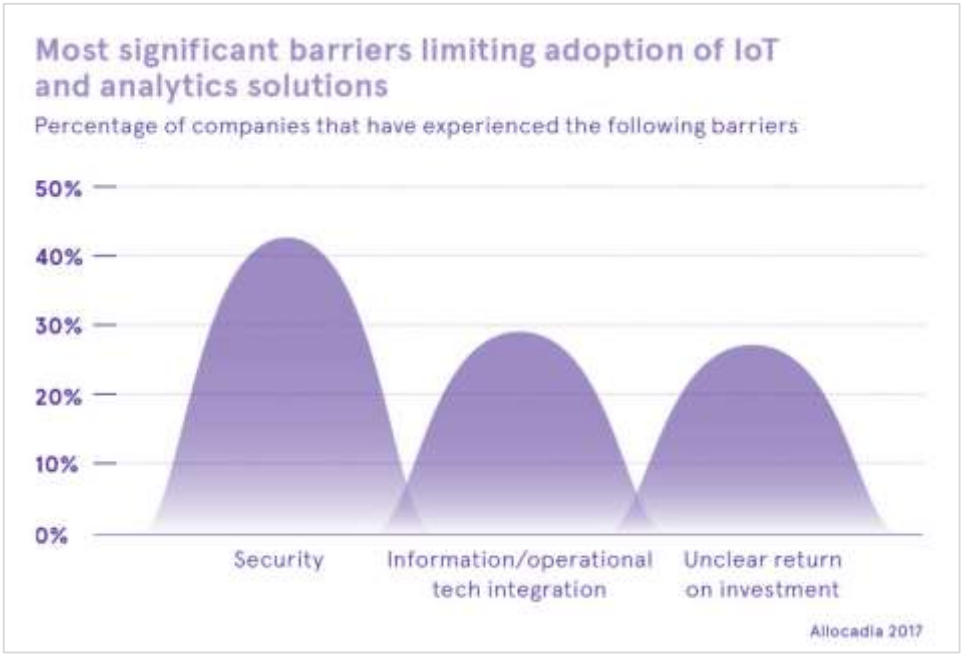
ExtremeAI Security

Extreme
Customer-Driven Networking

Disclaimer

- This product roadmap represents Extreme Networks current product direction.
- All product releases will be on a when-and-if available basis.
- Actual feature development and timing of releases will be at the sole discretion of Extreme Networks.
- Not all features are supported on all platforms.
- Presentation of the product roadmap does not create a commitment by Extreme Networks to deliver a specific feature.
- Contents of this roadmap are subject to change without notice.

Security is the Biggest Factor Slowing IoT deployments



Financial and Reputation Risks

Casino Breached through Fish Tank

WannaCry impacts PC and medical devices

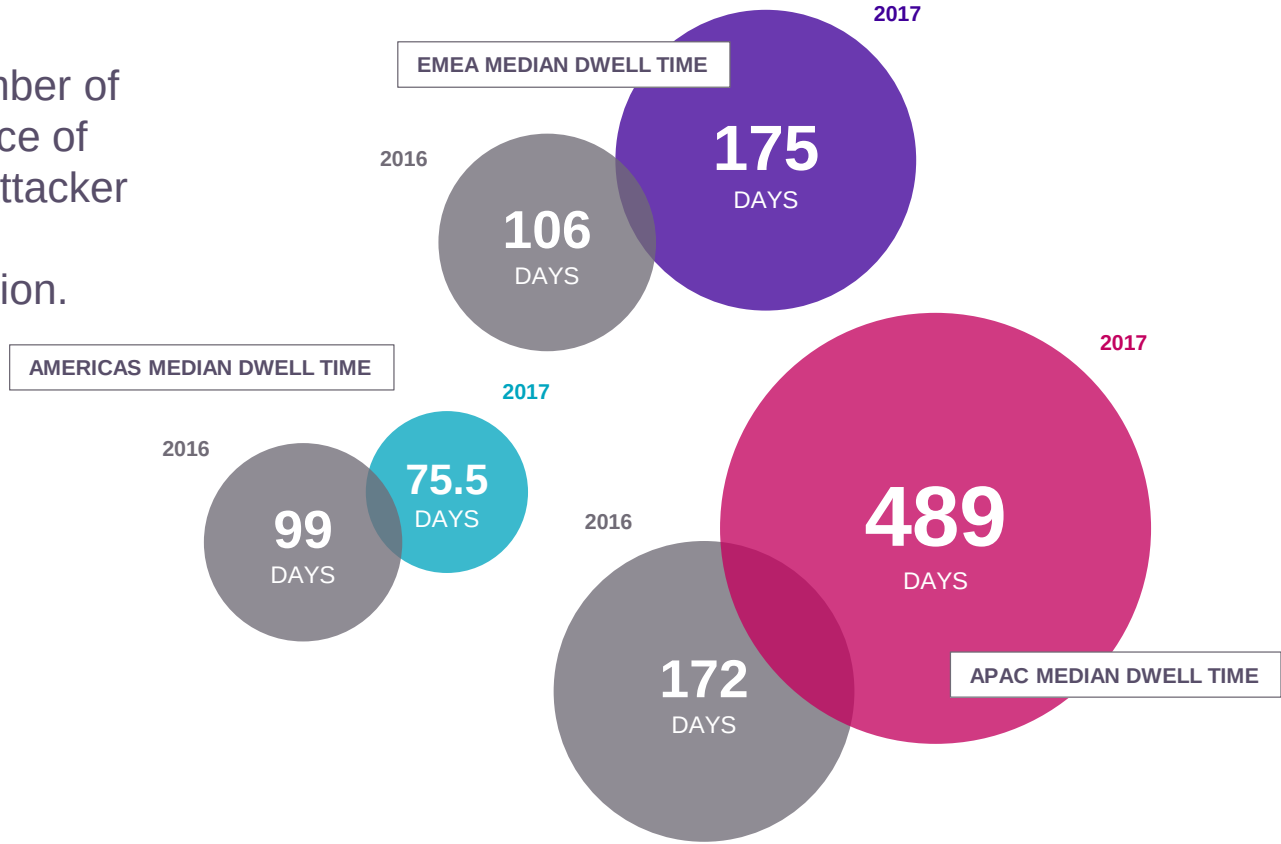
Ultrasound breached in 2 clicks (RSA 2018)

Gartner’s Three Tiers of IoT Security

1. **Device Cataloging (=ExtremeControl)**
   In a recent ZK survey 61% of networking professionals had low to no confidence that they knew every device connected to their network.
2. **Network Segmentation (=Fabric Connect and Policy)**

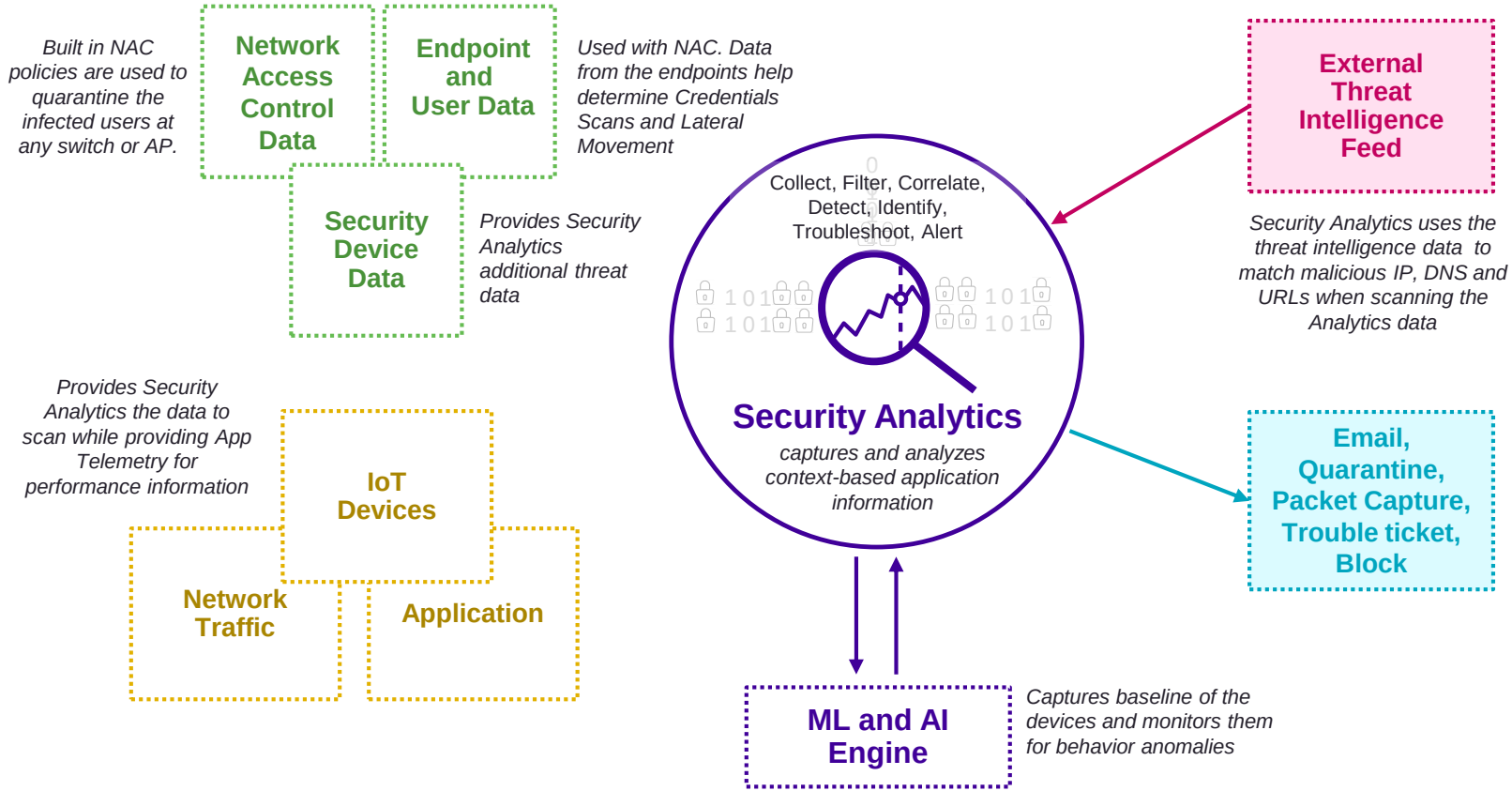
   Gartner estimates that only 5% of IoT devices deployed today are segmented.
3. **Network Traffic Analysis & Anomaly Detection (=ExtremeAI Security)**
   Observing network data flows and reporting on unusual or anomalous traffic patterns as they occur.

Dwell time is the number of days from first evidence of compromise that an attacker is present on a victim network before detection.

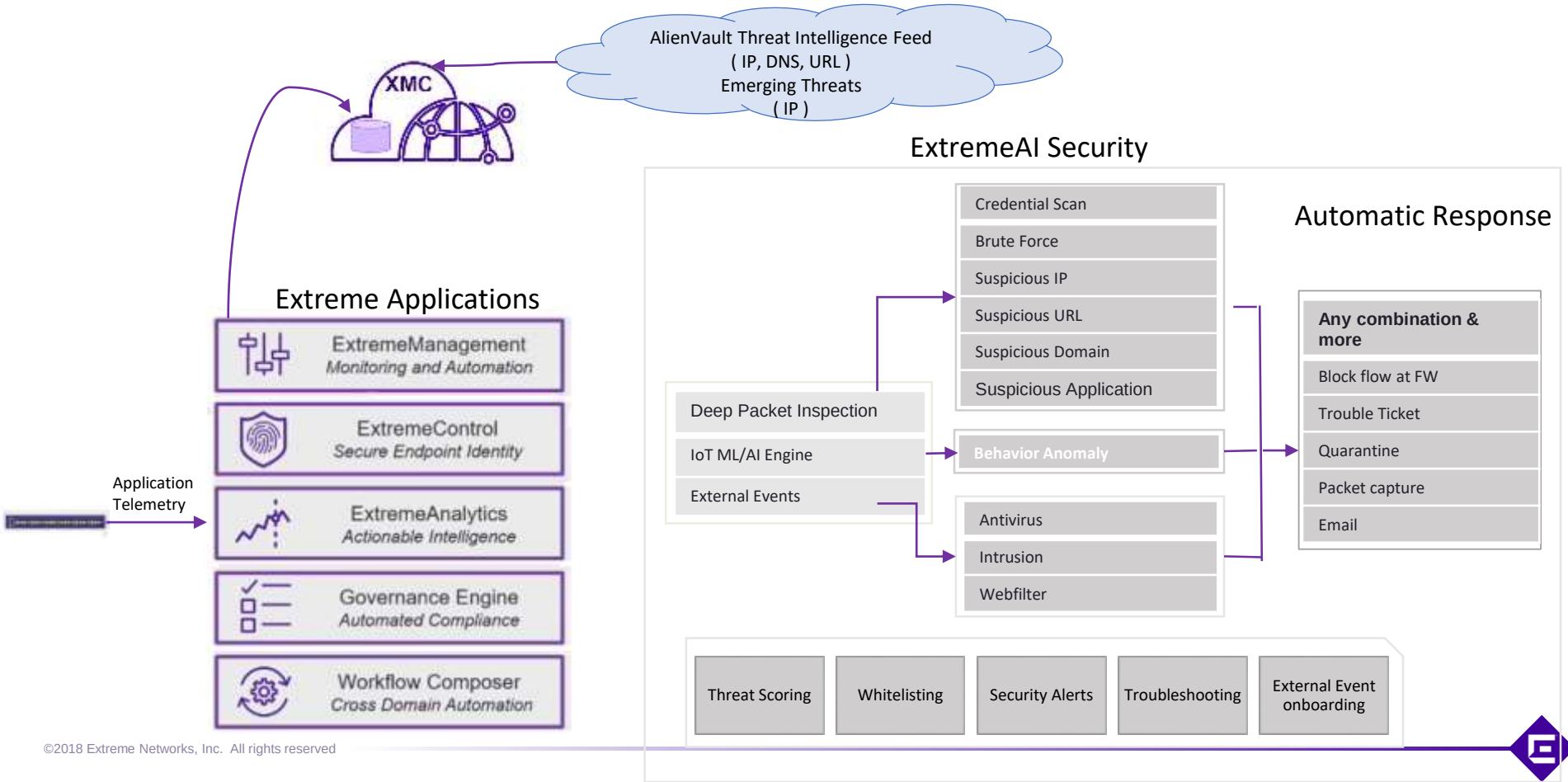


Source: FireEye M-Trend2018 Report

A Deeper Look into the ExtremeAI Security



Double Click – Detection and Response options

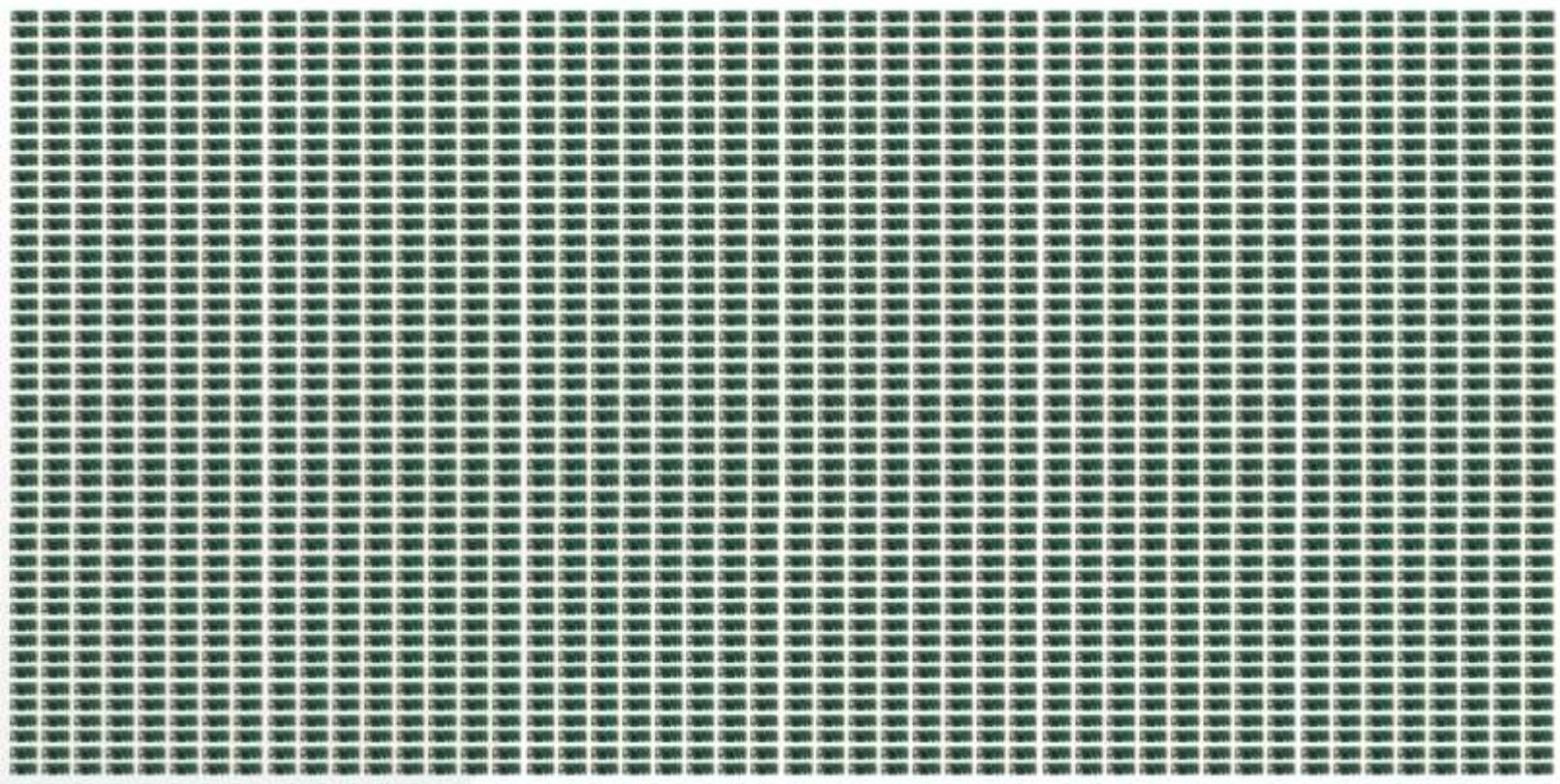


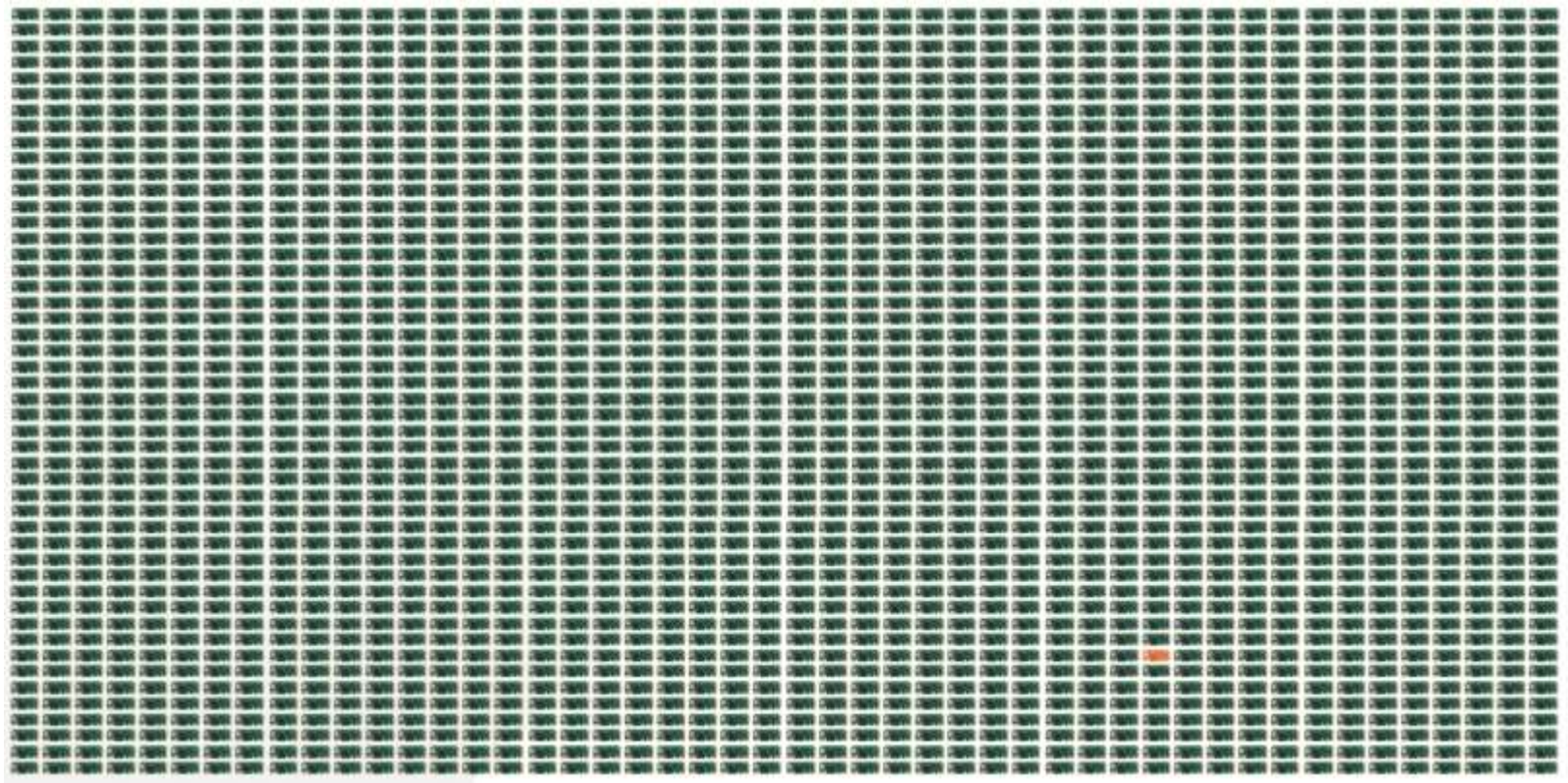
sensors,
actuators,
CCTVs,
badge readers,
building automation, …

Aim at **IoT** devices first,
not at **human-driven** endpoints.

laptops,
workstations,
smartphones, …

```
12:30:00 - 260B sent - 260B rcvd - NTP - 172.16.0.1:123
12:30:01 - 320B sent - 74B rcvd - HTTPS - iot.example.org:443
12:35:02 - 324B sent - 72B rcvd - HTTPS - iot.example.org:443
12:40:01 - 310B sent - 70B rcvd - HTTPS - iot.example.org:443
12:42:34 - 1KB sent - 1KB rcvd - SNMP - 172.32.0.5:161
12:45:02 - 324B sent - 90B rcvd - HTTPS - iot.example.org:443
12:50:02 - 330B sent - 70B rcvd - HTTPS - iot.example.org:443
12:55:03 - 310B sent - 80B rcvd - HTTPS - iot.example.org:443
12:00:00 - 260B sent - 260B rcvd - NTP - 172.16.0.1:123
12:00:01 - 308B sent - 84B rcvd - HTTPS - iot.example.org:443
12:03:12 - 1KB sent - 1KB rcvd - SNMP - 172.32.0.5:161
12:05:02 - 330B sent - 85B rcvd - HTTPS - iot.example.org:443
```





Zero-footprint Behavioral Modelling

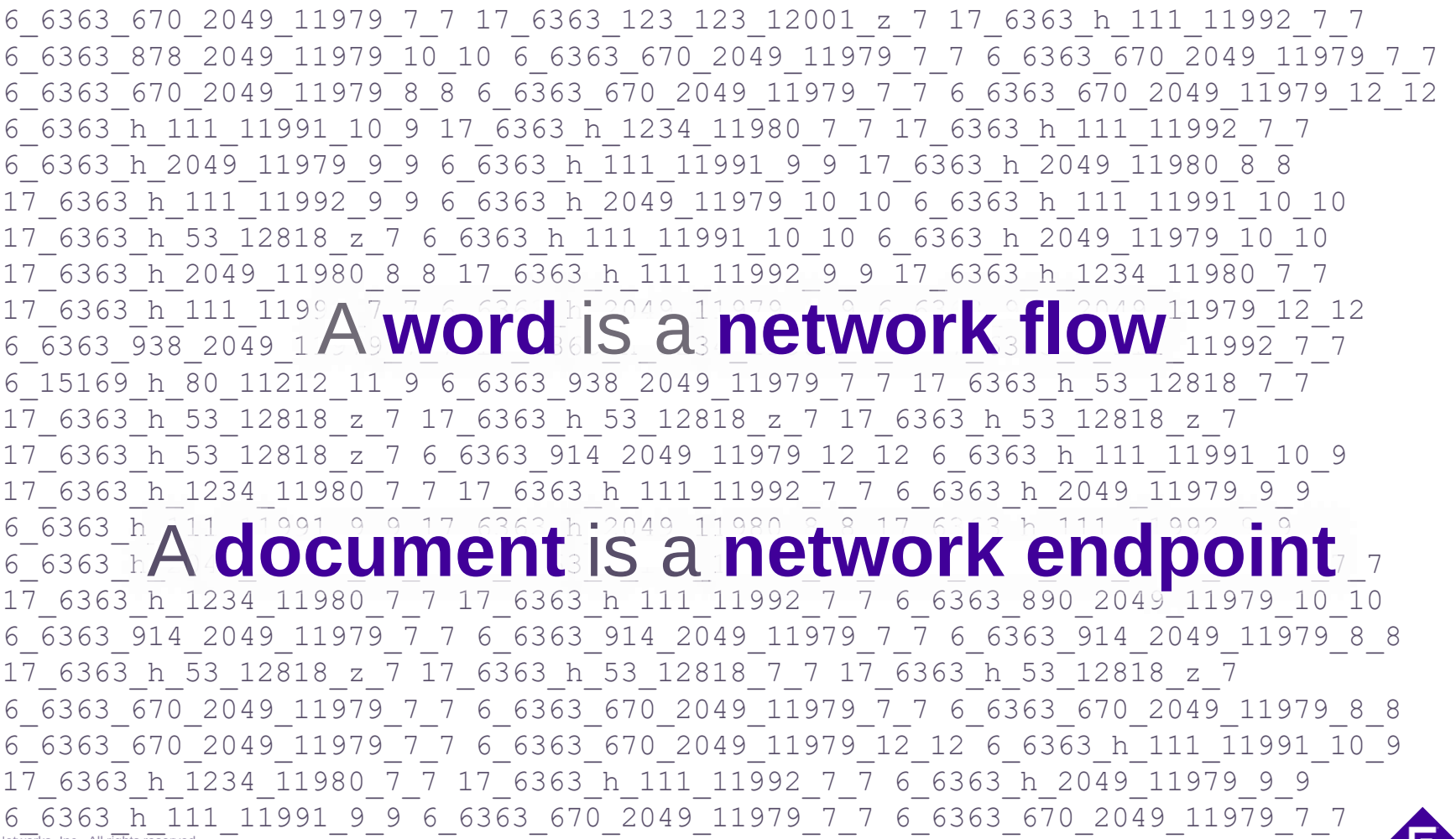
- No mountains of flows and metadata
- No technical, operational, financial and legal complexities
- No user-sensitive data (unless you want to)

~~Big data backend~~

Online-learning

Our inspiration: Based on Natural Language Processing

> ***"You shall know a word by the company it keeps."***
> – John Rupert Firth (1957)

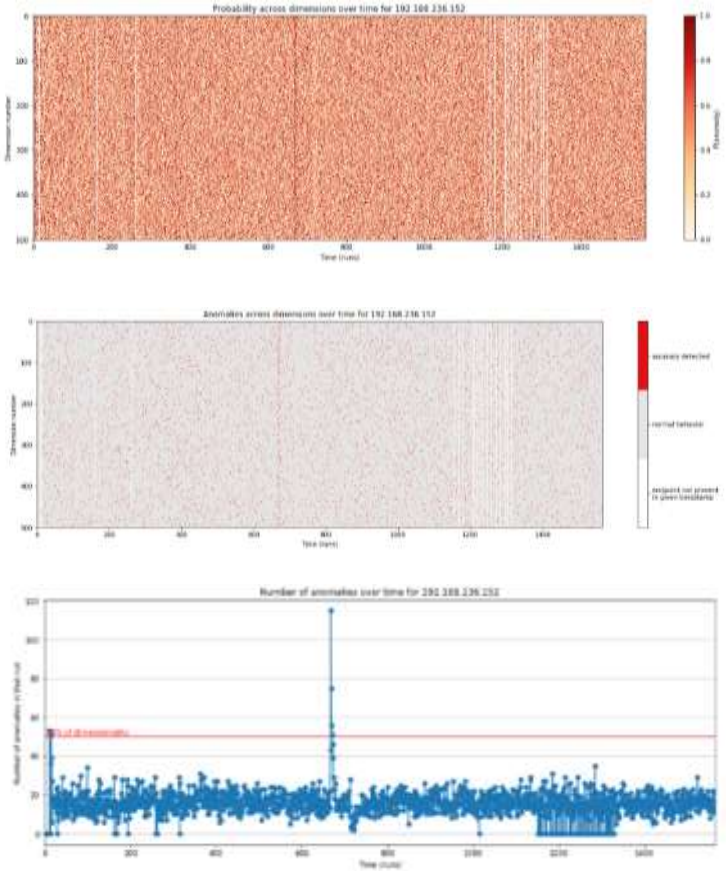


Zero-Footprint Anomaly Detection

- Each endpoint's behavior at a given point in time is **~5KB**
  - **Millions** of endpoints can be modelled on the current XMC appliances
  - L2-to-L5 flow data, augmented with **Extreme DPI** technology

- We use probabilistic programming to model the **likelihood of a given behavior being "anomalous"**

- Longer goal is to enable network **higher-order cognitive reasoning** (analogy, causality, mapping, etc.) for IT and Security analytics



WWW.EXTREMENETWORKS.COM