



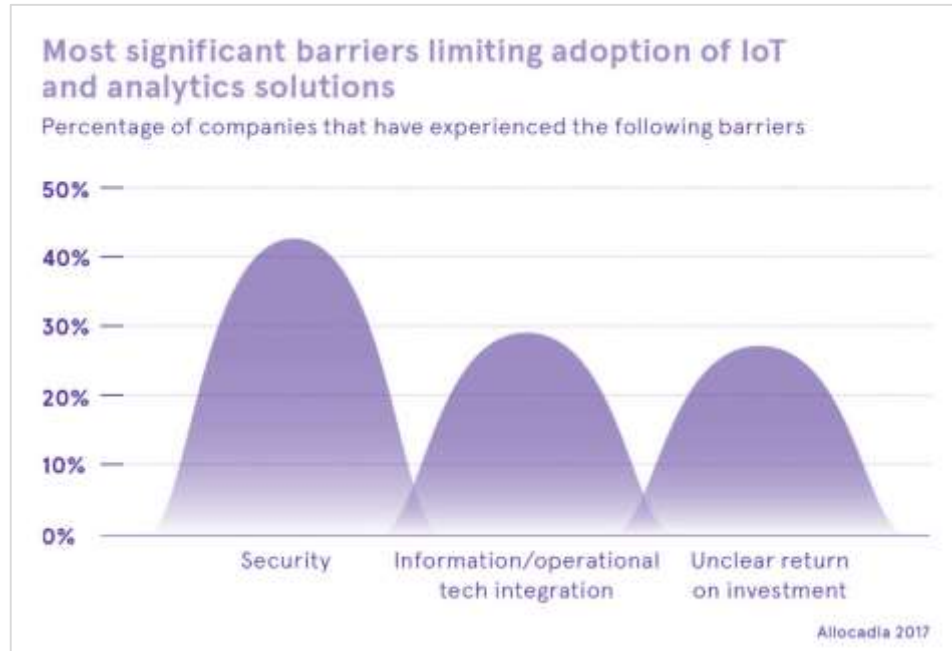
ExtremeAI Security

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)

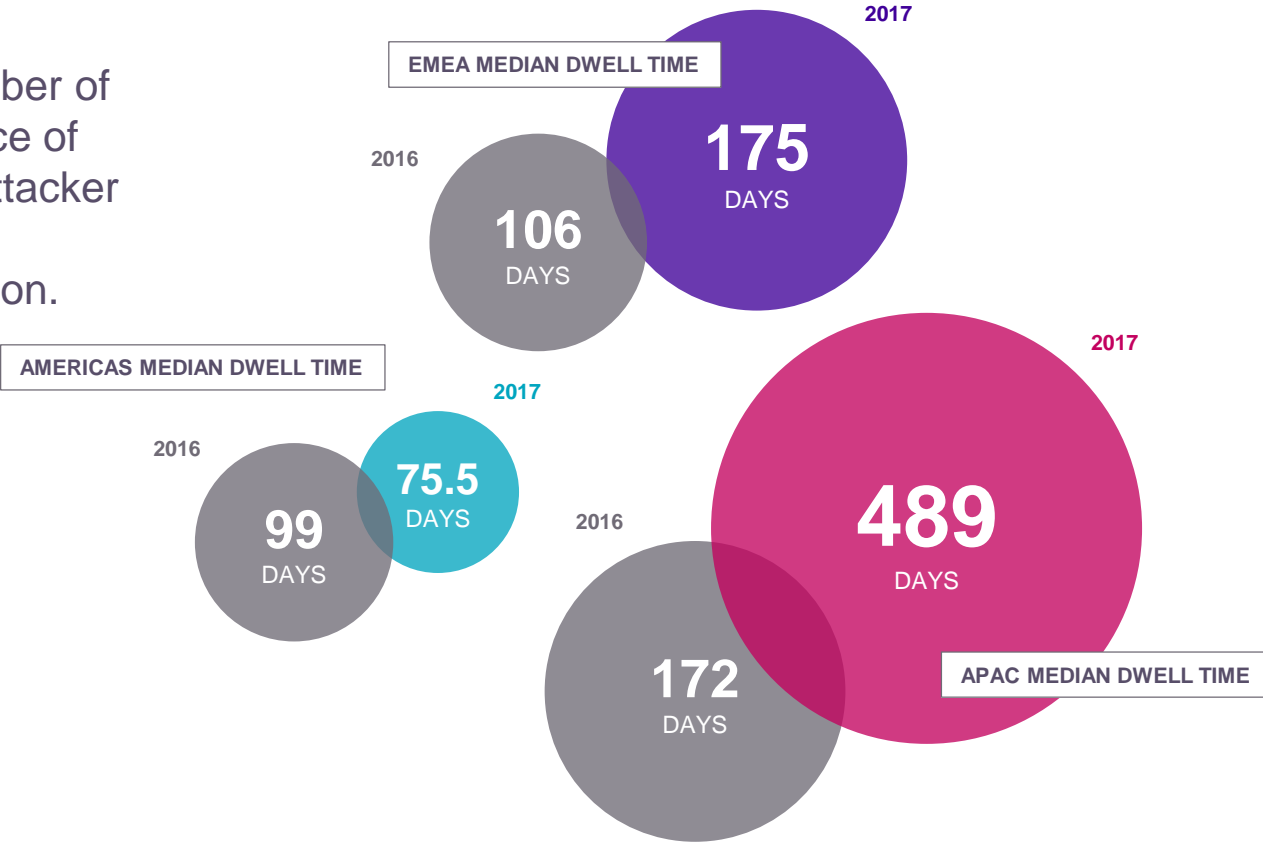
Gartner estimates that only 5% of IoT devices deployed today are segmented.

3. Network Traffic Analysis & Anomaly Detection (=ExtremeAI Security)

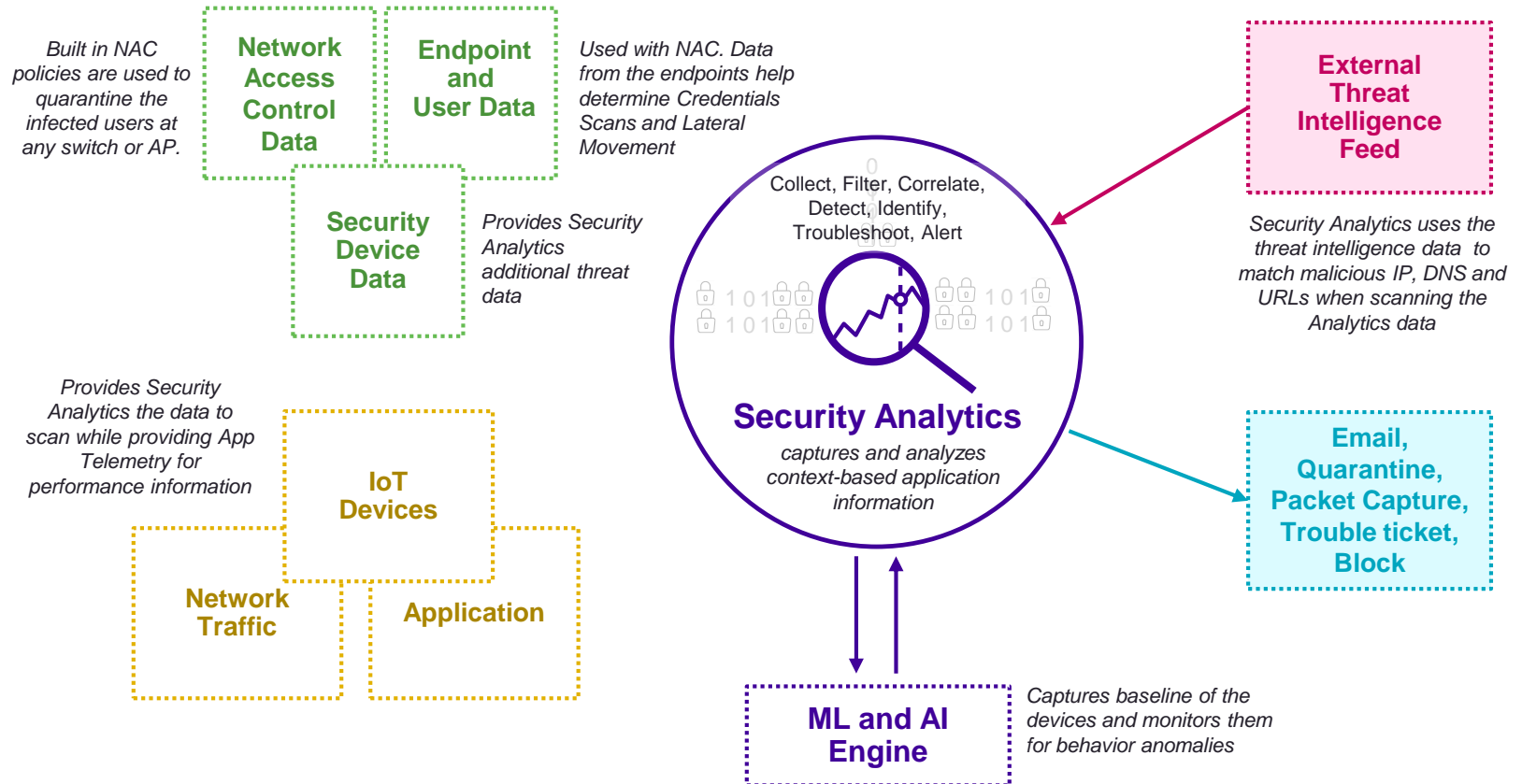
Observing network data flows and reporting on unusual or anomalous traffic patterns as they occur.



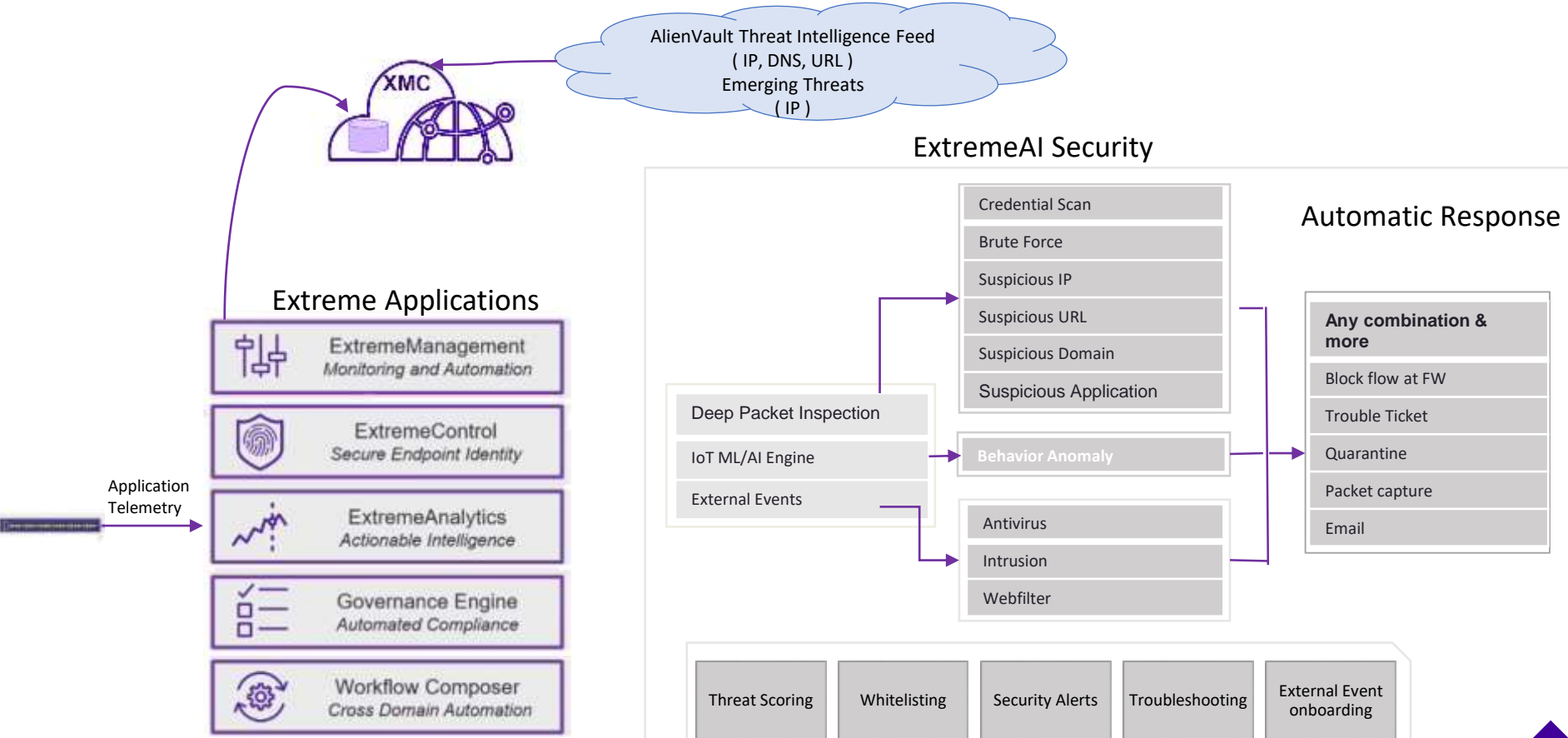
Dwell time is the number of days from first evidence of compromise that an attacker is present on a victim network before detection.



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, ...*

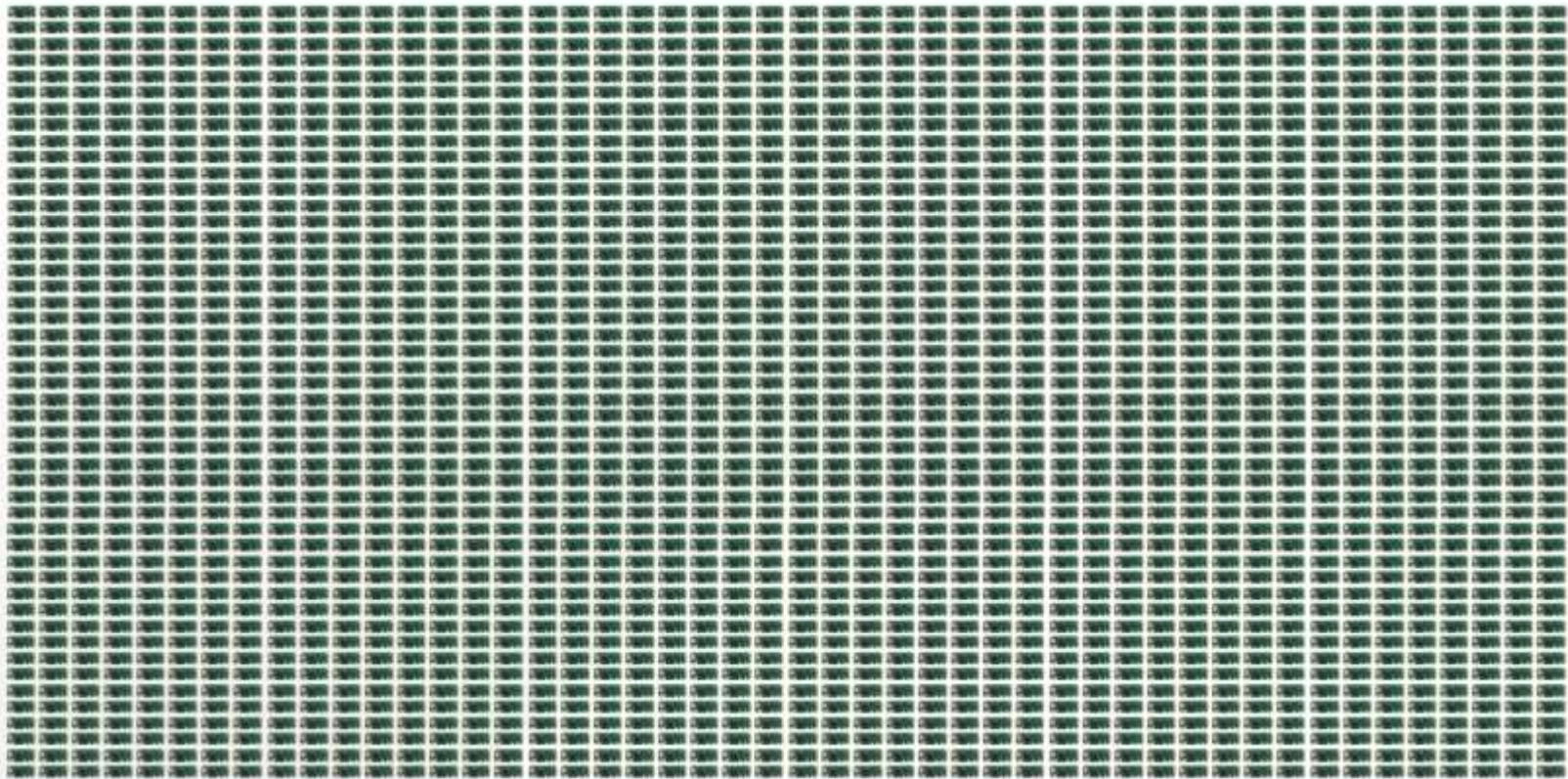


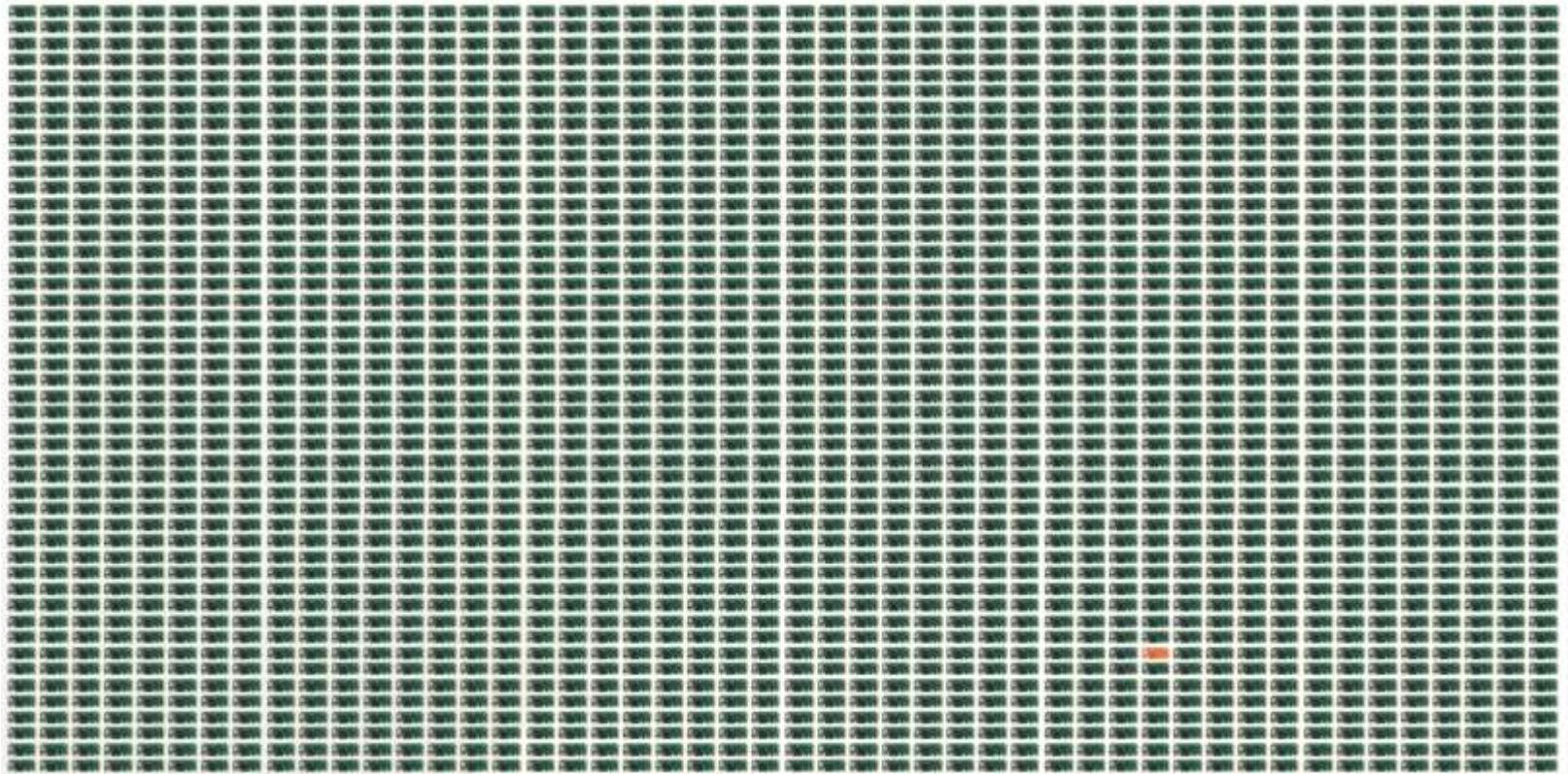

```
12:30:00 - 260B sent - 260B rcvd - NTP - 172.16.0.1:123
12:30:01 - 320B sent - 74B rcvd - HTTPS - iot.example.org:443
12:35:02 - 324B sent - 72B rcvd - HTTPS - iot.example.org:443
12:40:01 - 310B sent - 70B rcvd - HTTPS - iot.example.org:443
12:42:34 - 1KB sent - 1KB rcvd - SNMP - 172.32.0.5:161
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)

Distributed Representations of Words and Phrases and their Compositionality
Tomás Mikolov, Google Inc., Mountain View, CA
Greg Corrado, Google Inc., Mountain View, CA

Efficient Estimation of Word Representations in Vector Space
Tomás Mikolov, Google Inc., Mountain View, CA
Kai Chen, Google Inc., Mountain View, CA
Greg Corrado, Google Inc., Mountain View, CA
Jeffrey Dean, Google Inc., Mountain View, CA

Enriching Word Vectors with Subword Information
Piotr Bajkowski, Edouard Grave, Armand Joulin, and Tomáš Mikolov, Facebook AI Research

Bag of Tricks for Efficient Text Classification
Armand Joulin, Edouard Grave, Piotr Bajkowski, Tomáš Mikolov, Facebook AI Research

Abstract
We propose two novel neural architectures for computing continuous vector representations of words from very large data sets. The quality of these representations is measured in a word similarity task, and the results are compared to the previously best performing techniques based on different types of neural networks. We observe large improvements in accuracy at much lower computational cost. In fact, it takes less than a day to learn high quality word vectors from a 1.6 billion word

Abstract
In this work, we explore ways to make these baselines so very large corpora with a large output space, in the context of text classification. Inspired by the recent work in efficient word representation learning (Devlin et al., 2015; Luyckx, 2014), we show that linear models with a rank constraint and a feed-forward neural network can perform a similar task with an accuracy, while achieving the performance on par with the state-of-the-art. We explore the quality of our approach in a context of two different tasks, namely text classification and cross-domain analysis.

Abstract
Most of these techniques represent each word of the vocabulary by a dense vector, without parameter sharing. In contrast, this process is shared

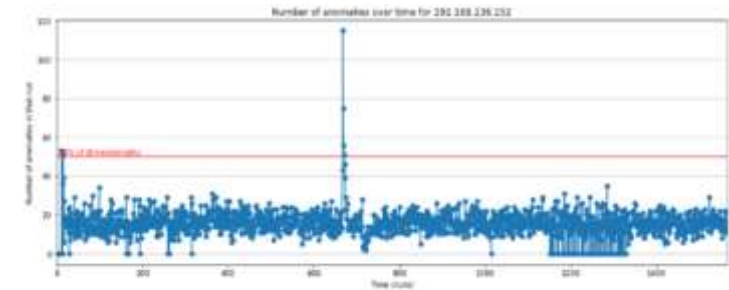
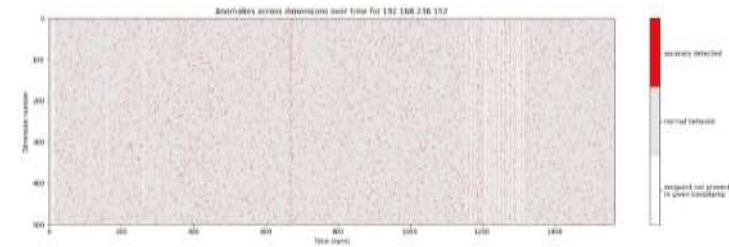
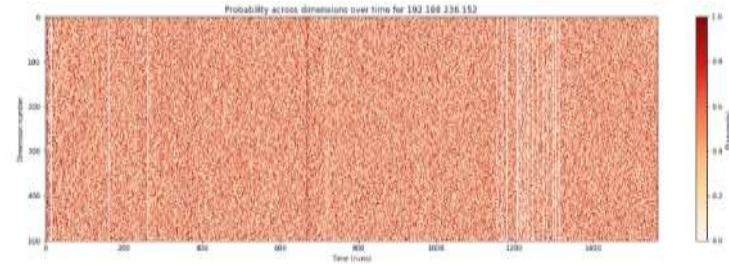


6_6363_670_2049_11979_7_7 17_6363_123_123_12001_z_7 17_6363_h_111_11992_7_7
6_6363_878_2049_11979_10_10 6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_7_7
6_6363_670_2049_11979_8_8 6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_12_12
6_6363_h_111_11991_10_9 17_6363_h_1234_11980_7_7 17_6363_h_111_11992_7_7
6_6363_h_2049_11979_9_9 6_6363_h_111_11991_9_9 17_6363_h_2049_11980_8_8
17_6363_h_111_11992_9_9 6_6363_h_2049_11979_10_10 6_6363_h_111_11991_10_10
17_6363_h_53_12818_z_7 6_6363_h_111_11991_10_10 6_6363_h_2049_11979_10_10
17_6363_h_2049_11980_8_8 17_6363_h_111_11992_9_9 17_6363_h_1234_11980_7_7
17_6363_h_111_11992_7_7 6_6363_h_2049_11979_12_12 6_6363_h_111_11992_7_7
6_6363_938_2049_11979_7_7 **A word is a network flow** 11992_7_7
6_15169_h_80_11212_11_9 6_6363_938_2049_11979_7_7 17_6363_h_53_12818_7_7
17_6363_h_53_12818_z_7 17_6363_h_53_12818_z_7 17_6363_h_53_12818_z_7
17_6363_h_53_12818_z_7 6_6363_914_2049_11979_12_12 6_6363_h_111_11991_10_9
17_6363_h_1234_11980_7_7 17_6363_h_111_11992_7_7 6_6363_h_2049_11979_9_9
6_6363_h_111_11991_9_9 17_6363_h_2049_11980_8_8 17_6363_h_111_11992_7_7
6_6363_h_1234_11980_7_7 **A document is a network endpoint** 11992_7_7
17_6363_h_1234_11980_7_7 17_6363_h_111_11992_7_7 6_6363_890_2049_11979_10_10
6_6363_914_2049_11979_7_7 6_6363_914_2049_11979_7_7 6_6363_914_2049_11979_8_8
17_6363_h_53_12818_z_7 17_6363_h_53_12818_7_7 17_6363_h_53_12818_z_7
6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_8_8
6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_12_12 6_6363_h_111_11991_10_9
17_6363_h_1234_11980_7_7 17_6363_h_111_11992_7_7 6_6363_h_2049_11979_9_9
6_6363_h_111_11991_9_9 6_6363_670_2049_11979_7_7 6_6363_670_2049_11979_7_7



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

