SEARCH GUARD

ZERO TRUSTED NETWORKS

OR: WHY PERIMETER SECURITY IS DEAD

Search Guard

01.

ABOUT ME

- Jochen Kressin, Co-Founder & CTO of floragunn GmbH
- Makers of Search Guard
- Enterprise Security Suite for Elasticsearch
- Founded 2012
- Main office: Berlin, Germany
- Partner offices: Seattle, New York, Miami, Bordeaux
- Meet us at booth #15

02.

WHY THIS TOPIC?

- I talk a lot to customers that are using Elasticsearch
- Most of them store sensitive data inside Elasticsearch

→ Personally identifiable information: User- or customer data

→ Financial information: Transaction data

→ Healthcare information: Patient data

- Elasticsearch does not offer security out-of-the-box
- Natural question: How do you secure Elasticsearch?
- Answers are scary …

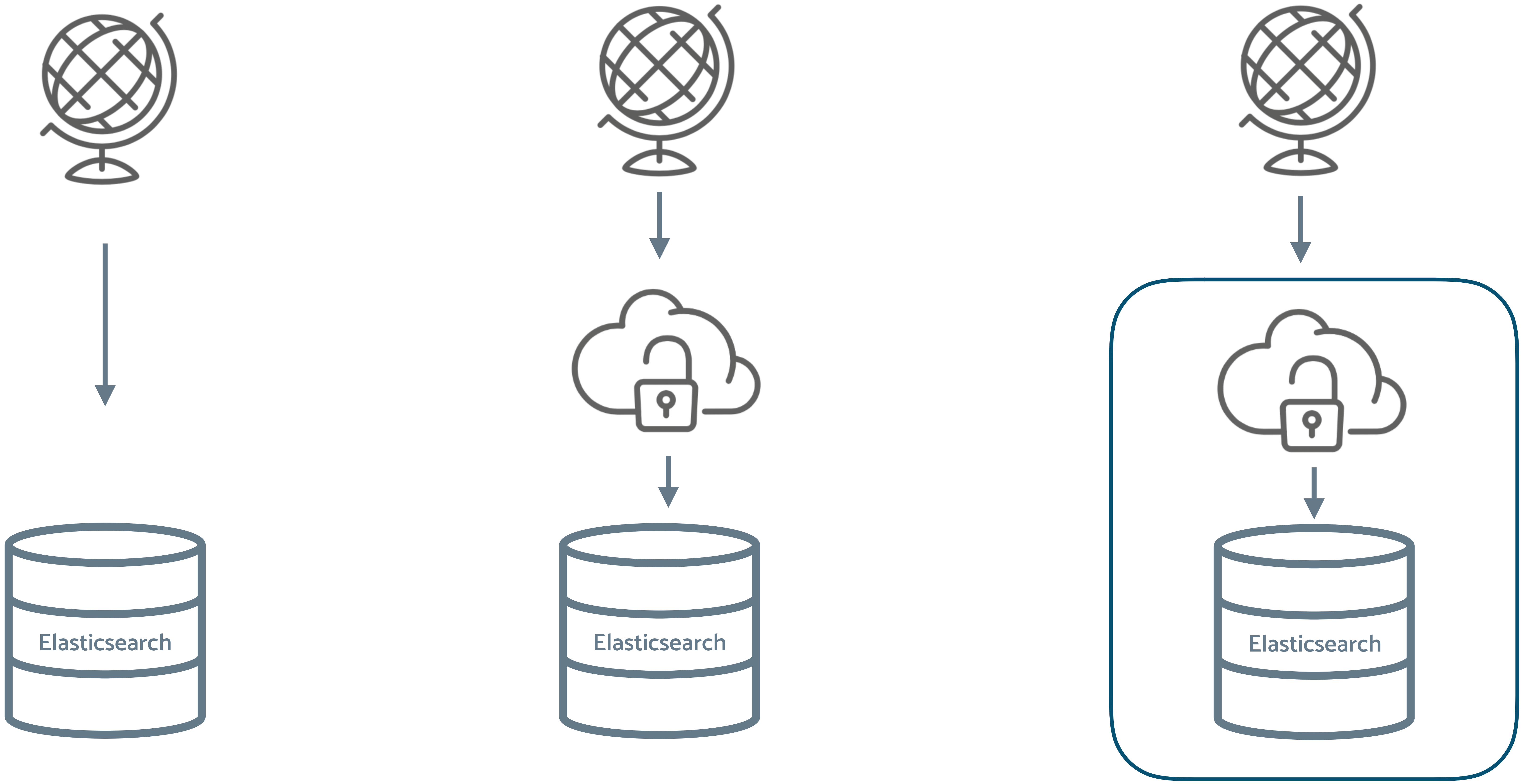
03.

ANSWERS

“It’s unprotected” “Firewall” “VPN and Firewall”

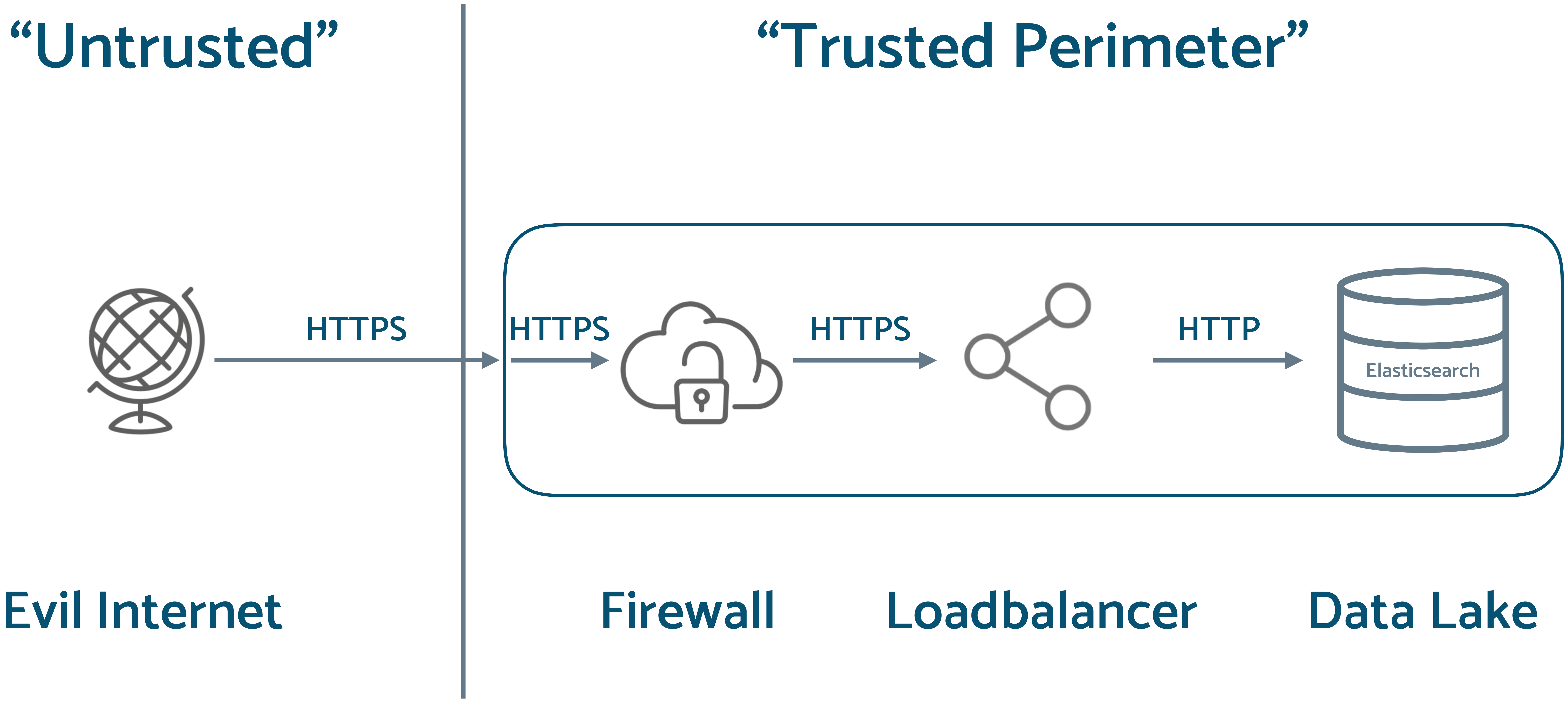
Evil Internet

Sensitive Data



04.

PERIMETER SECURITY



05.

ASSUMPTIONS

- **Traffic from the outside cannot be trusted**
- **Traffic inside the perimeter can be trusted**
- **Access to the perimeter can be controlled**
- **Consequences**

→ VPNs, firewalls and loadbalancers are sufficient

→ At any point in time, we know who has access to the data

→ Traffic inside the VPN does not need to be encrypted end-to-end

→ Performance is more important than encryption

→ Security breaches will be detected

06.

REALITY CHECK

- Does perimeter security work?
- If it works, why do we still suffer from security breaches and data loss?
- Data breach @ Exactis

→ Close to 340 million personal records leaked

→ Phone number, home address

→ Number, age and gender of children

- Elasticsearch cluster publicly accessible
- I don’t think this was on purpose, but a human mistake

07.

WHAT HAS CHANGED?

- **Access control**
  - → Partners, freelancers, part-time contractors etc.
  - → These are all potential inside threats
- **Locations**
  - → Remote offices
  - → Remote workers
- **Devices**
  - → Laptops, smartphone, tablets
  - → Bring your own device

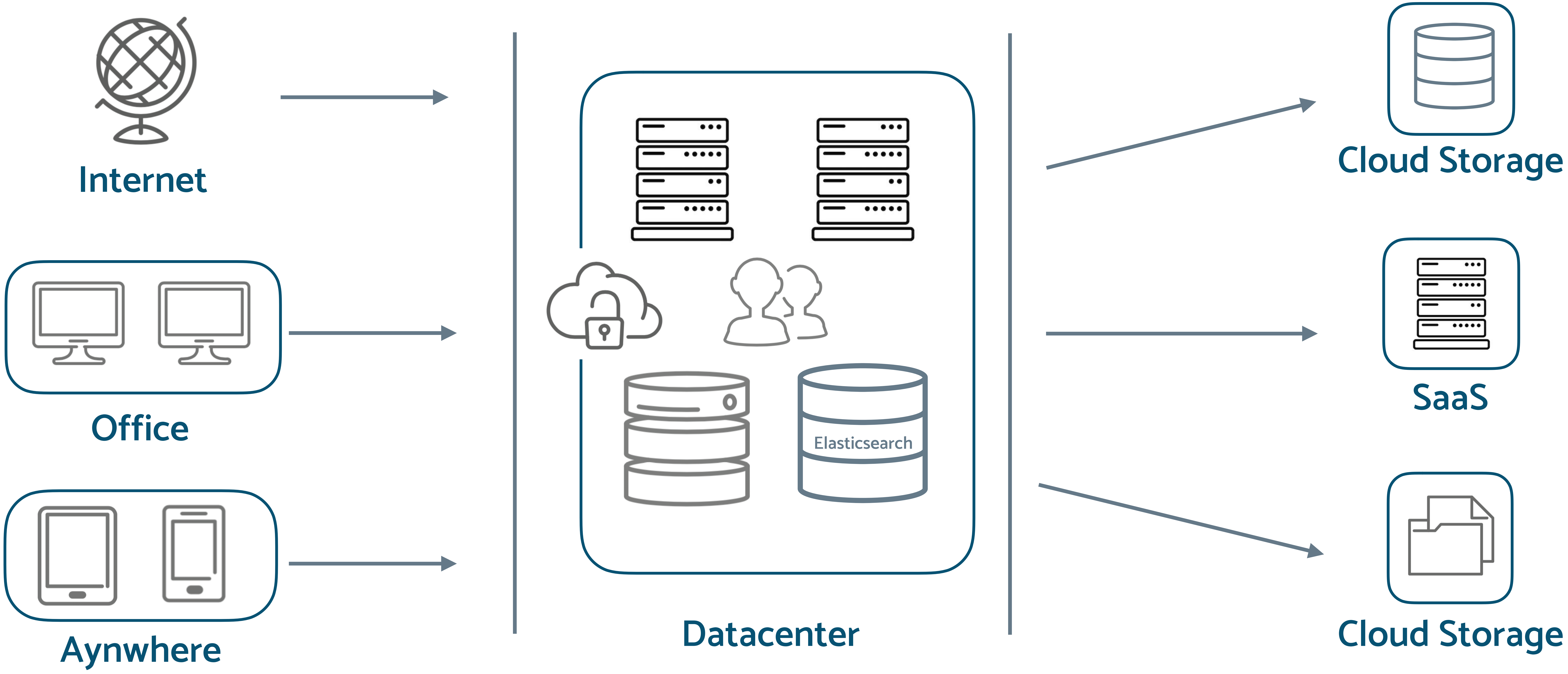
08.

WHAT HAS CHANGED?

- **Cloud computing**
  - → Cloud storage
  - → Microservices
  - → SaaS / PaaS / IaaS
- **Containerization**
  - → Docker, Kubernetes etc.
  - → How to apply IP-based security?
- **Decentralized systems / clusters**
- **Internet of things**

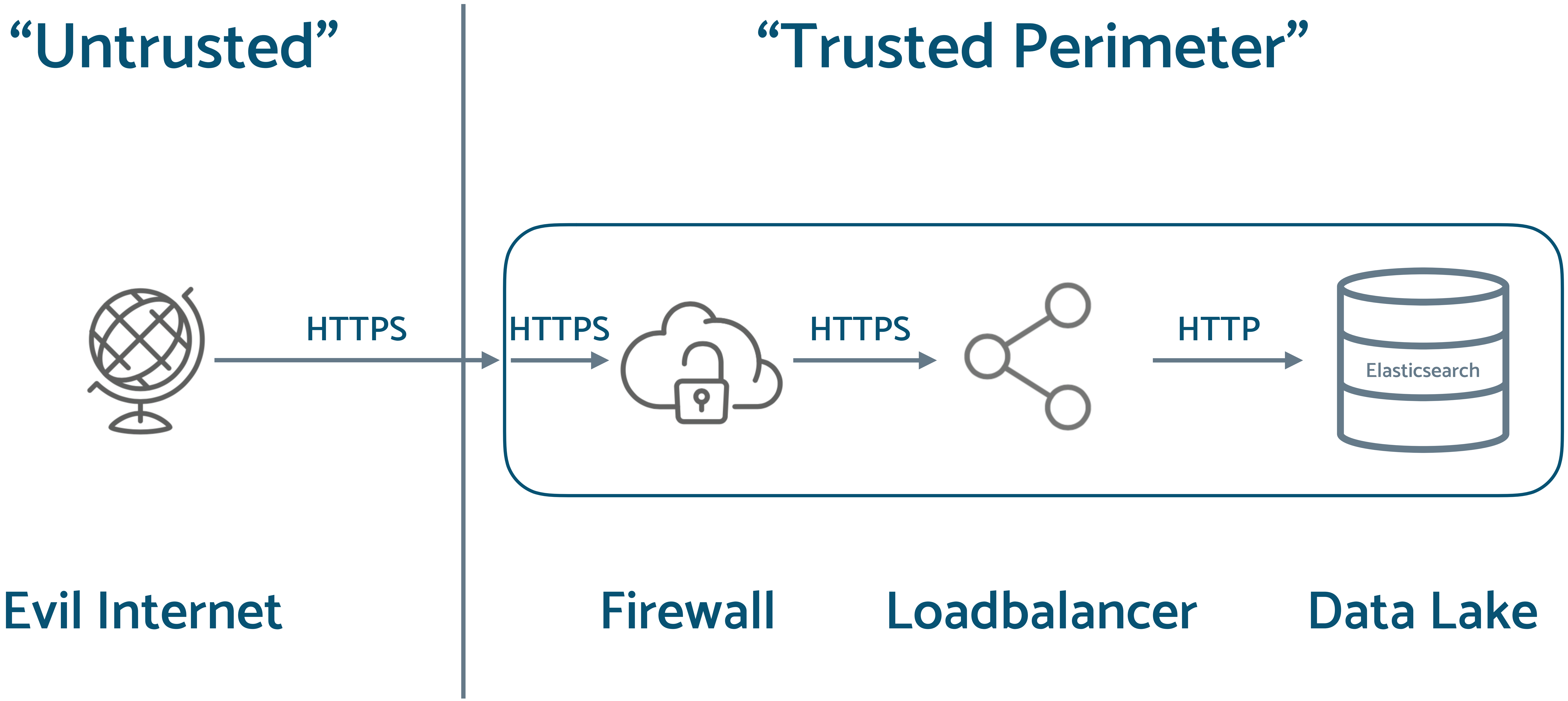
09.

WHERE IS THE PERIMETER NOW?



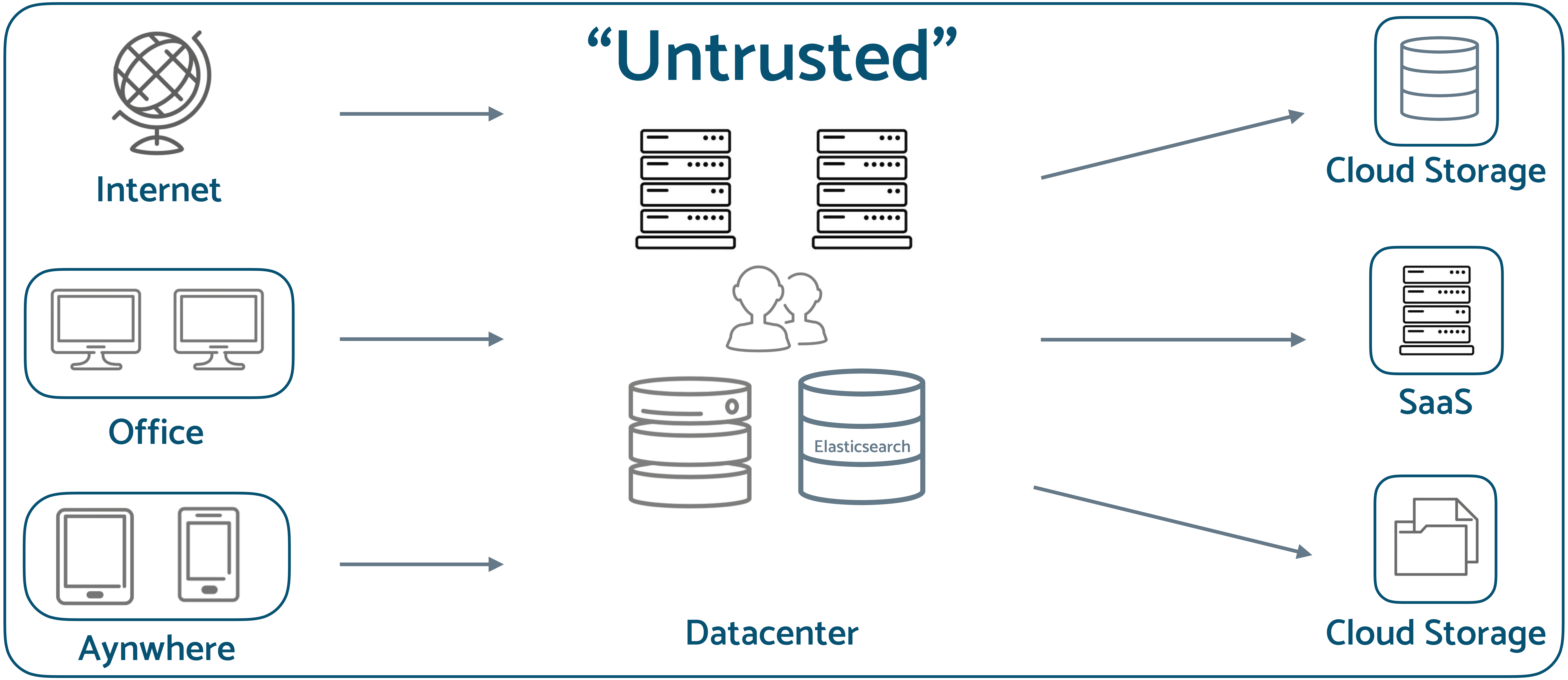
10.

PERIMETER SECURITY REVISITED



11.

ZERO TRUSTED NETWORK



12.

FACT CHECK

- **Companies do not have full control anymore**

→ Explosion of devices and locations

→ Data and services are moving to the cloud

→ Internet of Things

- **Inside attacks are ever increasing**

→ 60% of attacks originated from the inside (IBM study 2016)

→ Attacks via social engineering

- **Lines between inside and outside are blurry at best**

13.

PARADIGM SHIFT

- **No traffic can be trusted**

→ Regardless where it originates

→ Regardless from which device

- **No IP / port / application can be trusted**

→ Cloud, containers, IoT

→ Traditional firewall approach flawed

- **No user can be trusted**

→ Beware of inside attacks

→ Outside personell

14.

PARADIGM SHIFT

- **Move security to where the data lives**

→ No unsecured services

→ Not even in a VPN

- **No unencrypted traffic, anywhere**

→ Not even in a VPN

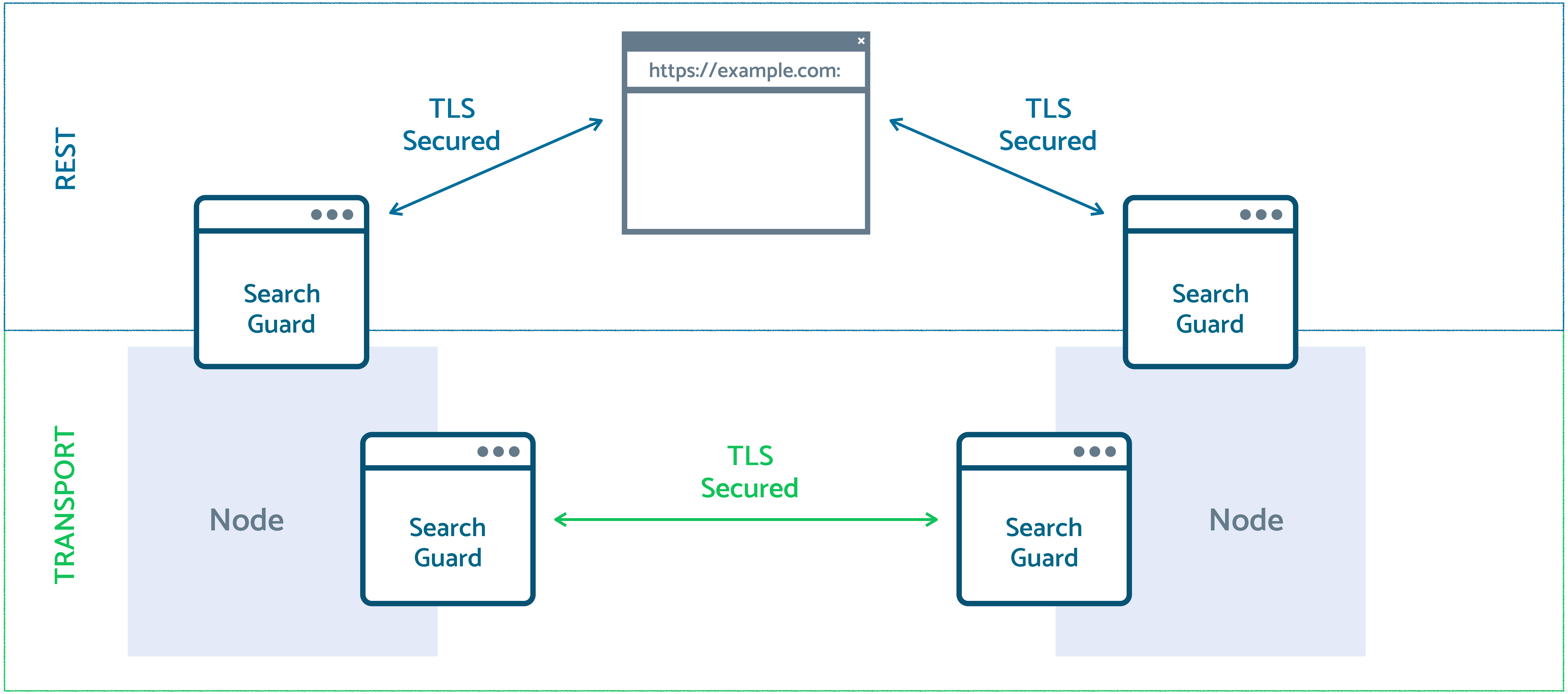
- **Assume attackers are already in your network**

→ Never trust, always verify

- **Apply least privilege strategies**
- **Inspect and log all traffic**

15.

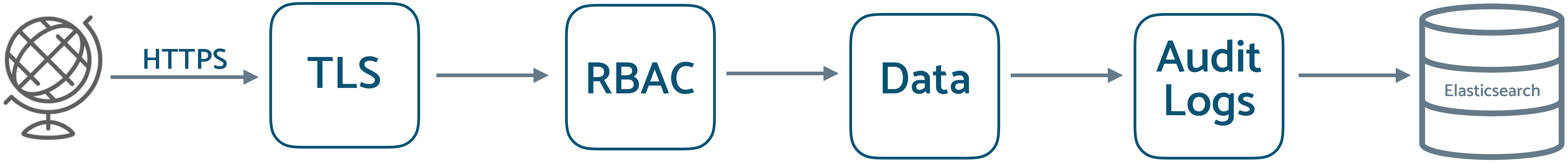
EXAMPLE: ELASTICSEARCH



16.

EXAMPLE: ELASTICSEARCH

Search Guard



Any location

Any device

Validate certificates

Hostname verification

DNS Lookups

Authentication

Certificate revocation

Role-based access control

Least privilege approach

No defaults

Document-level

Field-level

Filtering

Anonymization

Track access

Monitor anomalies

Alerting

Data Lake

17.

OPEN SOURCE / OPEN CODE

- **Complete Search Guard code has always been publicly accessible**
- **Code has been audited several times**
  - → By the community
  - → By security experts and auditors of customers
  - → Verified by Veracode
- **Download, inspect, audit, compile**
  - → https://github.com/floraguncom/search-guard
  - → https://github.com/floraguncom/search-guard-enterprise-modules

18.

RESOURCES

- **Search Guard website**

→ https://search-guard.com/

- **Documentation**

→ https://docs.search-guard.com

- **Community Forum**

→ https://groups.google.com/d/forum/search-guard

- **GitHub**

→ https://github.com/floraguncom

SEARCH GUARD
send us a message:

info@search-guard.com

Search Guard

floragunn GmbH
Tempelhofer Ufer 16
D-10963 Berlin, Germany

E-Mail: info@search-guard.com
Web: search-guard.com

Managing Directors: Claudia Kressin, Jochen Kressin
Registergericht: Amtsgericht Charlottenburg
Registernummer: HRB 147010 B
E-Mail: info@floragunn.com

Search Guard