Using the Modern Application Stack to Improve Security

Matthias Luft, mluft@ernw.de

ERNW
providing security.

ERNW

- Vendor-independent
- Established 2001
- 65 employees, 45 FTE consultants
- Continuous growth in revenue/profits
  - No venture/equity capital, no external financial obligations of any kind
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance

- Blog: www.insinuator.net
- Conference: www.troopers.de

ERNW
providing security.

DevOps

"DevOps is the philosophy of unifying Development and Operations at the **culture**, **system**, **practice**, and **tool** levels, to achieve **accelerated** and more **frequent delivery** of **value** to the customer, by improving quality in order to increase velocity."

Rob England, 2014

ERNW
providing security.

Continuous Delivery

"... is a software engineering approach in which teams produce software in **short cycles**, ensuring that the software can be **reliably released** at any time. It aims at **building**, **testing**, and **releasing** software **faster and more frequently**."

DOI: 10.1109/MS.2015.27

ERNW
providing security.

Infrastructure-as-Code

- Manage und provision **data centers** through **machine-readable** definition files
- Version control your infrastructure

- Documentation & Evolution
- Static/Dynamic analysis

ERNW
providing security.

Immutable Infrastructure

- ~~"Servers are cattle not pets"~~
- "Servers are **syringes**"
- Spawn your infra from a template or recipe
- **Update**, **Test** it, **Spawn** new, **Trash** old

ERNW
providing security.

Typical Interjections

- “Deployments to production can break everything!”
- “But we need security approval!”
- CI service must have deployment access
  - … and the security posture of a code-execution-as-a-service system is debatable.

- Let’s see how the described approaches can improve security!

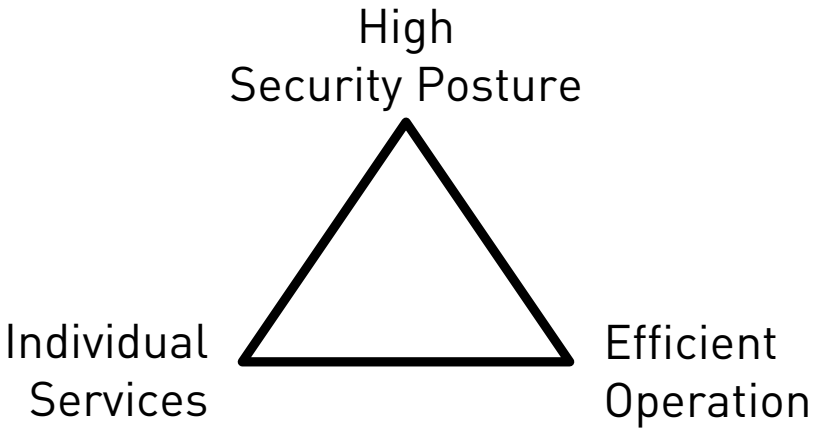
ERNW
providing security.

Standardization & Security

- Standardized platforms can be “security assessed” in standardized ways
- Individual solutions require intelligent analysis
  - Which, still, typically is human intelligence/time/capacity
    - Which, still, is the scarcest resource we have!

ERNW
providing security.

Standardization & Security – Pick Two!



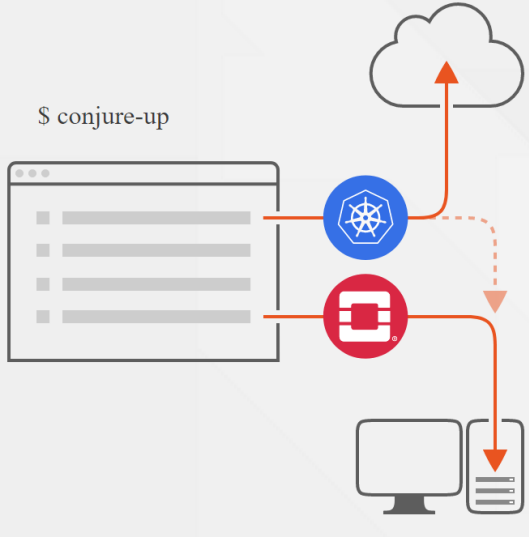
ERNW
providing security.

Standardization & Security

- Do not allow interactive system/container logins.
  - Some environments kill containers/systems after the password was checked out.
- All infrastructure must be deployed via script.
- All middleware must be deployed via script.
- All applications must be deployed via script.
- All updates/changes must be deployed via script.
- * must be done via script ;-)
- It must be possible to kill random instances.

ERNW
providing security.

Standardization & Security



juju

docker COMPOSE

ERNW
providing security.

Typical Answer: Container Scanners

- Desired capabilities:
  - Application Vulnerabilities
  - OS Package and Library Vulnerabilities
  - Build Script Breakout
    - As always, hard to detect.
    - Docker-less builds essential
  - Deployment Mal-/Mis-Configuration
- Products start to catch up with this feature list!

ERNW
providing security.

Security Integration

- Immutable Infrastructures
- Application-level Tests
- Infrastructure Analysis & Documentation
- Interactive Security
- Enforcement of Secret Management

- Relevant mention: Build Server Security

ERNW
providing security.

Immutable Infrastructures

- CD may also work without it.
- Definitely push towards it!
- Any non application-level change is a suspicious event!
- Baselining (of anything…) is typically the hardest part.
  - Ever worked with a SIEM or WAF? ;-)

ERNW
providing security.

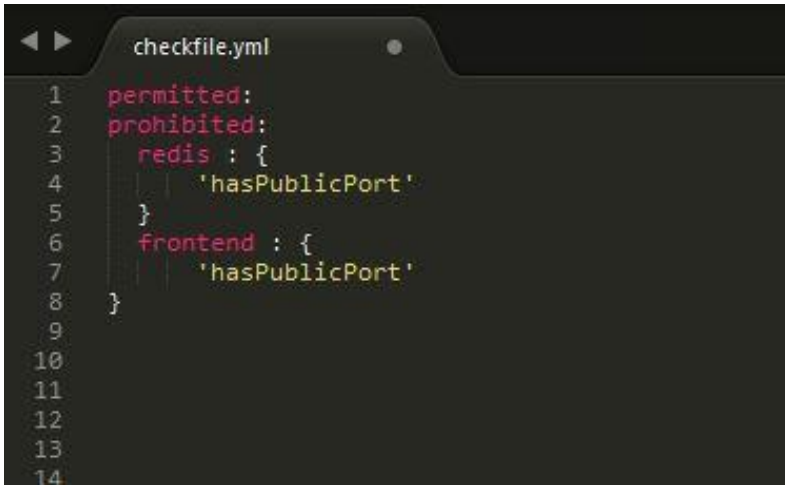
Application-level (Security) Tests

- Do we need DevOps for that?
- Run fuzz tests, application vuln scanners on relevant builds.
  - More SDLC than DevOps
  - Mantra of automated, reproducible builds may help with implementation.

ERNW
providing security.

Infrastructure Analysis

- Various independent projects
- Products start to cover this



ERNW
providing security.

Infrastructure Analysis - Checks

- Check for typical infrastructure anti-patterns
  - Publicly exposed database
    - … without authentication
  - Management protocols/services
  - High number of exposed services
  - Running as root/Use of volumes/Other container mal-practices
  - …

ERNW
providing security.

Interactive Security

- Mini Red Teams, Minion Pentesters, Micro Assessments, Continuous Penetration Testing, Chaos Pentester, ...
- **Relevant enabler:**
  - **Automated infrastructure deployment**
  - **Reproducible infrastructure**
- => Have assessment target on your local notebook!

ERNW
providing security.

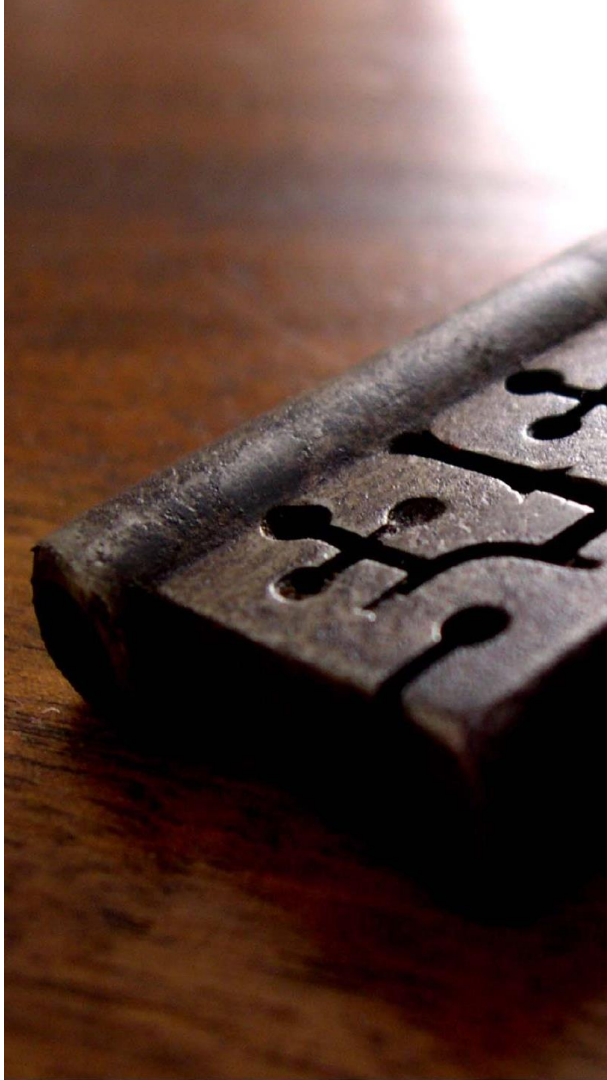
Interactive Security

- As a security team, provide
  - Training in the new CD approaches
  - Repository scaffolding
    - Commit hooks including checks for included secrets
    - `.gitignore`
    - `.gitlab-ci.yml` including all scanning checks
      - Provide scanning checks as well ;-)
  - Container security policies (e.g. K8s Pod Security Policies) available in the cluster

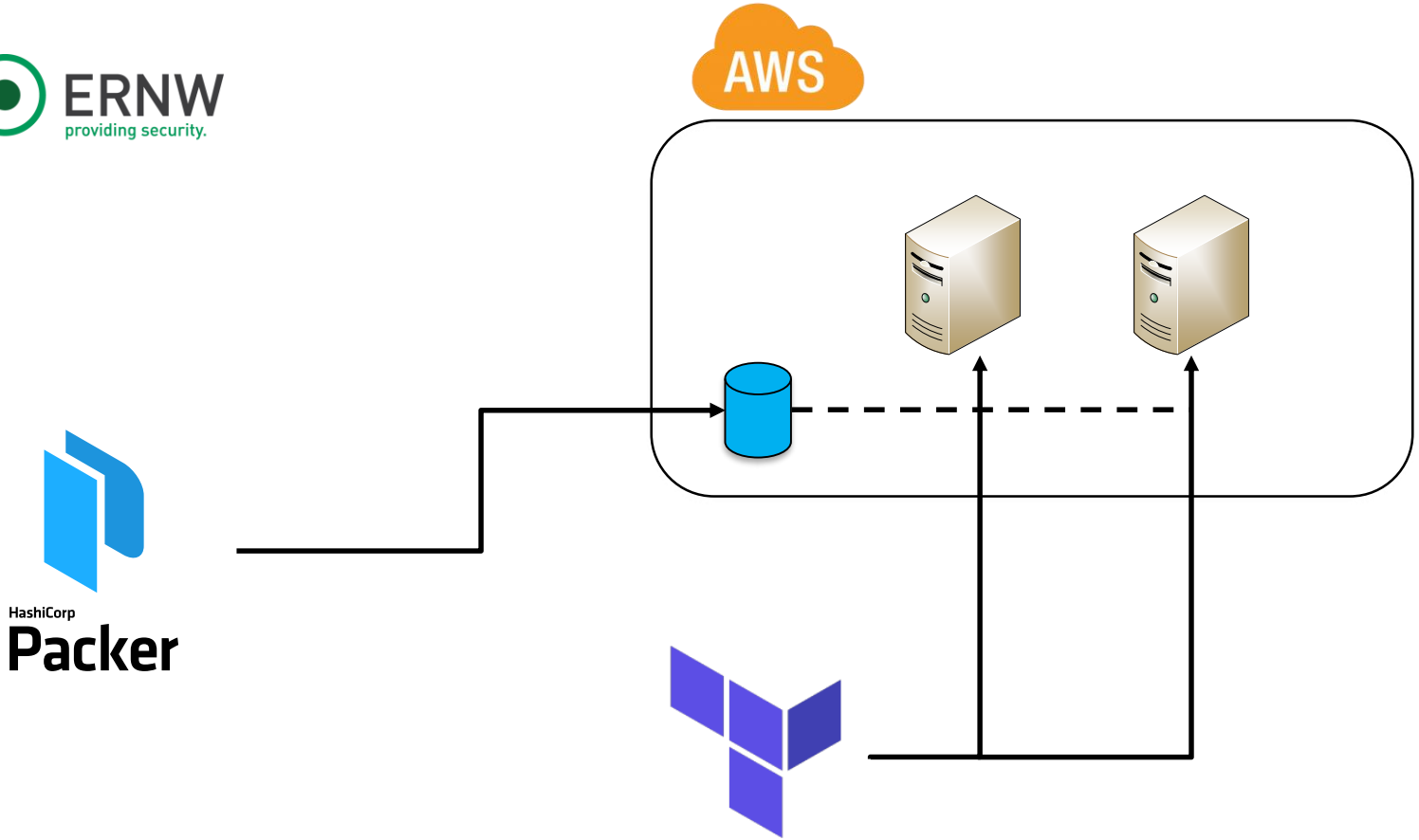
ERNW
providing security.

Enforcement of Secret Management

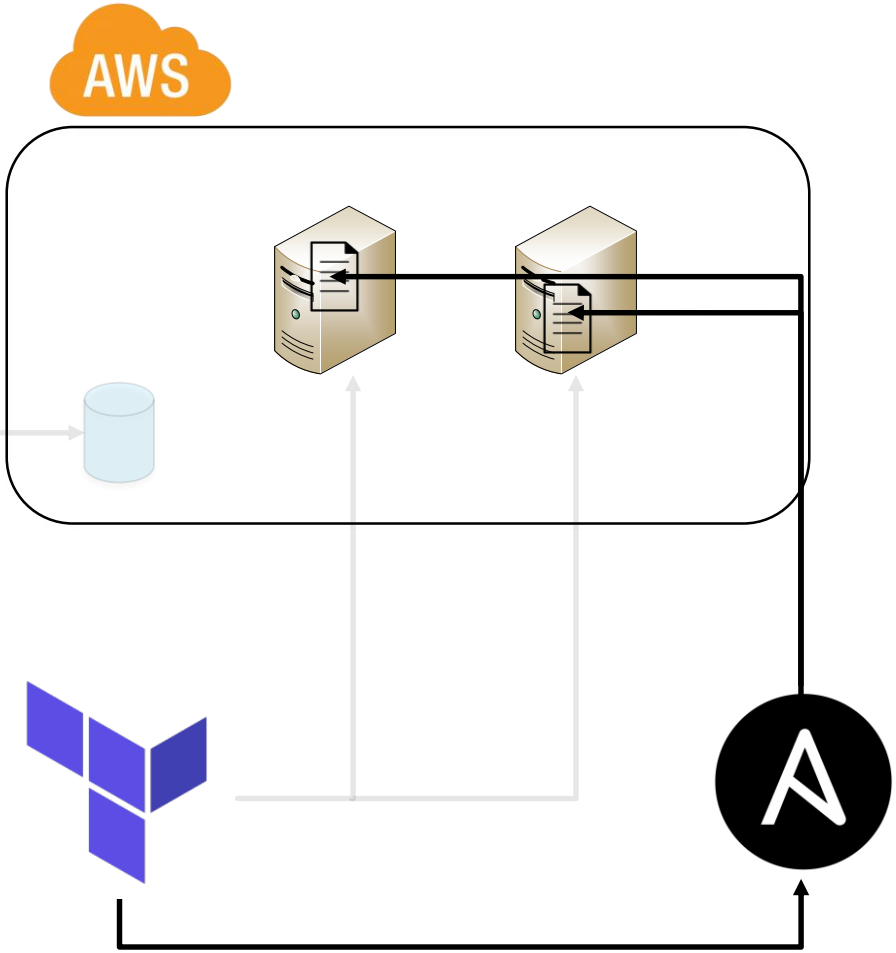
- One typical problem:
  - Secret/Technical User Sprawl
- DevOps tools help tremendously!
  - Docker/k8s/OpenShift/… secrets
  - Vault
- Enforce usage of those!
  - E.g.
    - https://github.com/devsecops/git-secrets
    - DumpMonitor



ERNW
providing security.

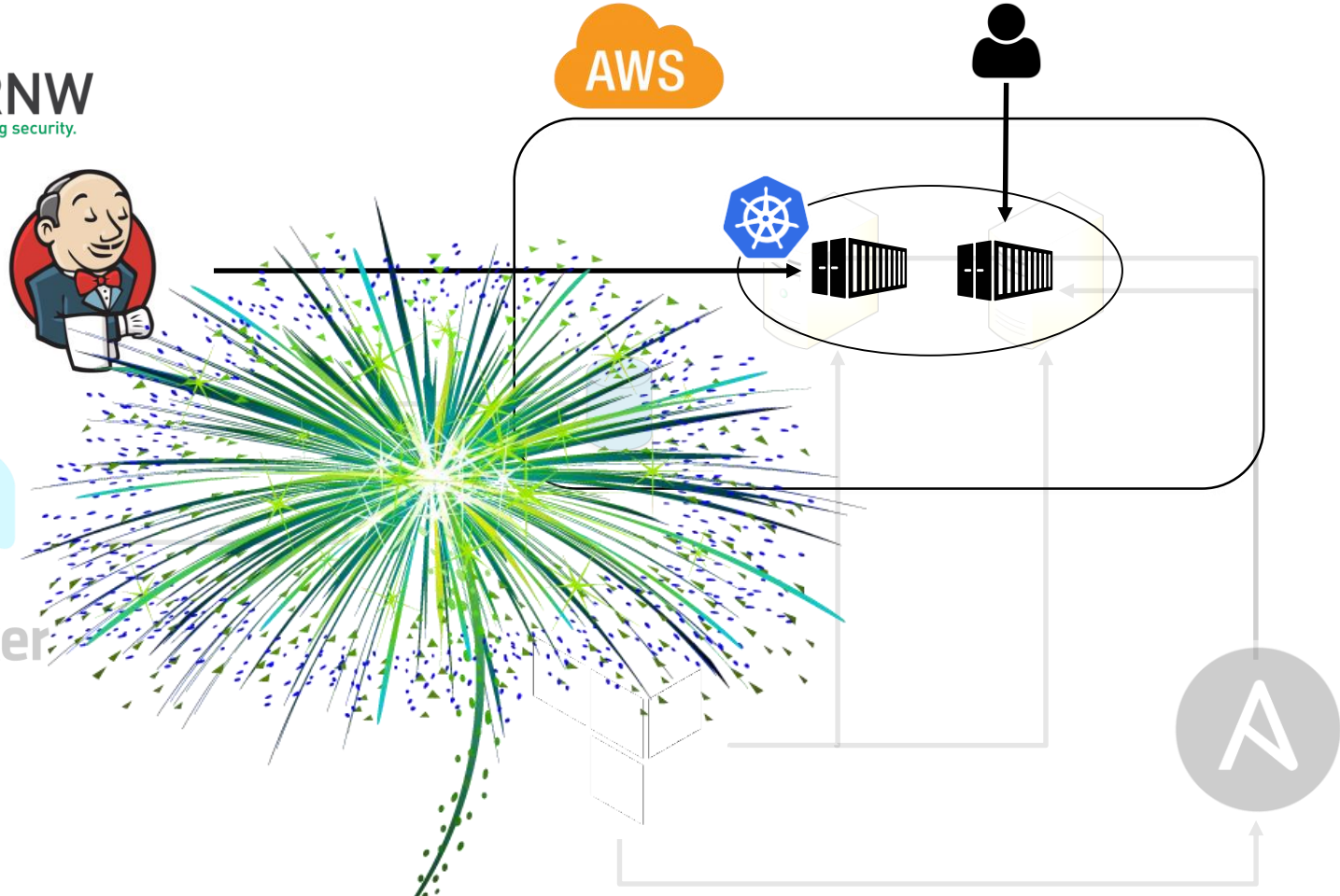


ERNW
providing security.



HashiCorp
Packer

ERNW
providing security.



HashiCorp
Packer

ERNW
providing security.

Further Challenges

- Build Server Breakout/Unprivileged Builds
- Secret Consolidation: Build System to Container Platform
- Maintenance of Trusted Images
- Security Zoning (thinking container/cluster breakout)
- RBAC for all components

ERNW
providing security.

Summary

- Standardization is both requirement and benefit for security in modern application stacks
- Cloud and container platforms allow for immutable infrastructures
  - Push for it! Requires disruptive changes!
- Push for platform with great UX
- Leverage the options of CD and…
  - Enforce secrets management
  - Facilitate micro assessments
  - Automate baselining and standardized/”standardizable” checks
    - Leaving room for individual work

ERNW
providing security.

Thank you for your Attention!

Questions?

mluft@ernw.de

@uchi_mata

www.ernw.de

www.insinuator.net

ERNW
providing security.

Disclaimer

- All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them and purely illustrates their existence.