glueck kanja

The Worst Case

Recovery zum Anfassen –
statt PowerPoint, Papier und Panik
bei Cyberangriff

Azure **E**mergency **R**esponse **E**nvironments

glueck kanja

Florian Stöckl

— **Azure Lead**

— Florian.Stoeckl@glueckkanja.com

… / florianstoeckl

glueck kanja

Ransomware

[ˈɹɛnsəmwɛːɐ̯]

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.

glueck kanja

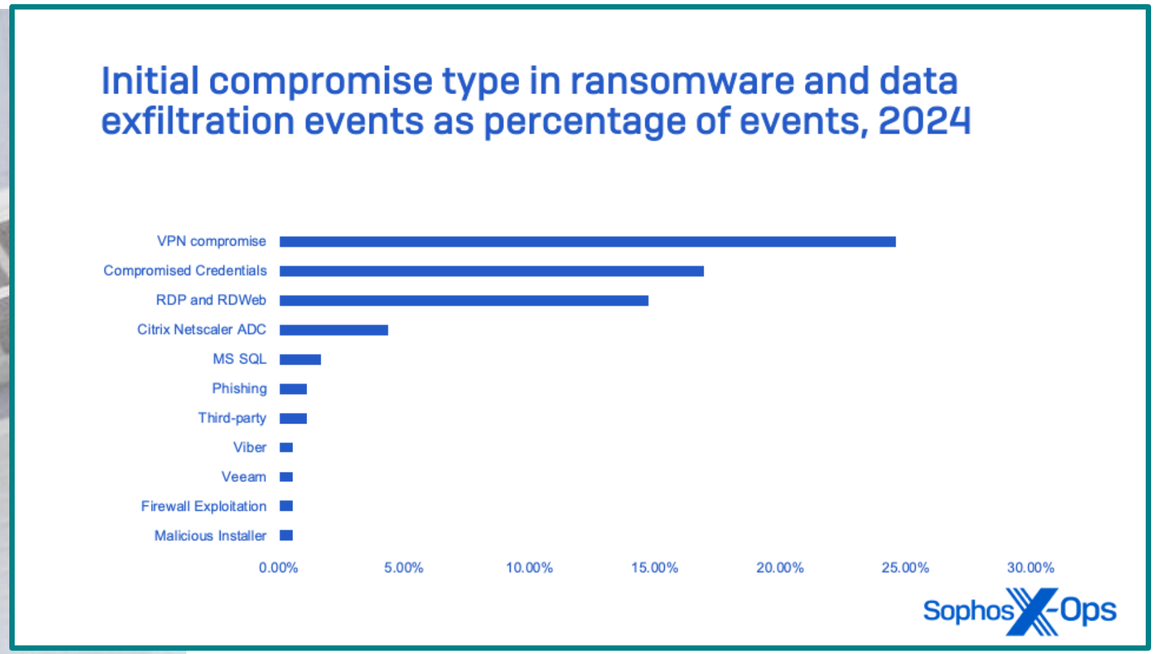
Sophisticated Attacks vs. Reality

Reality Check

glueck kanja

Sophisticated Attacks vs. Reality

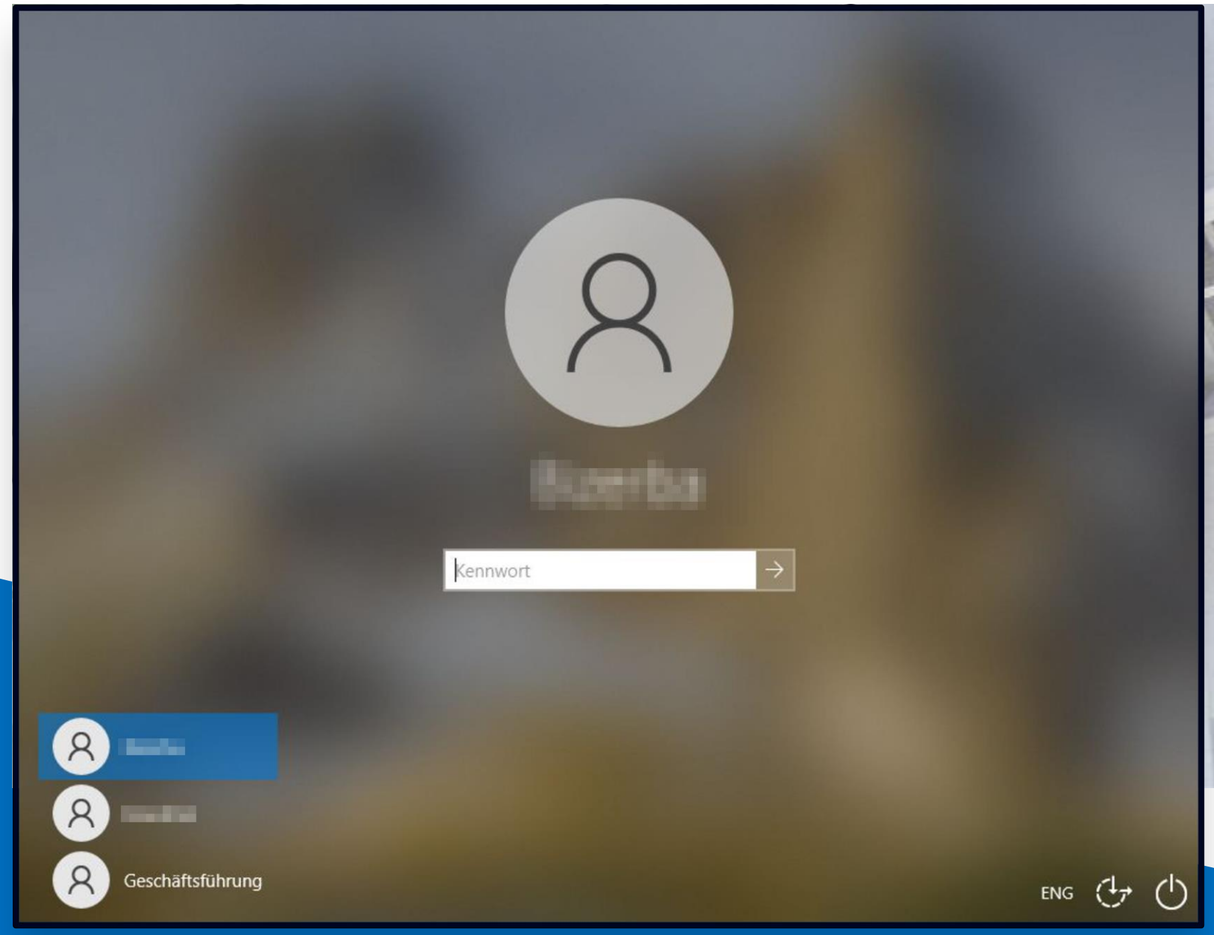
Reality Check

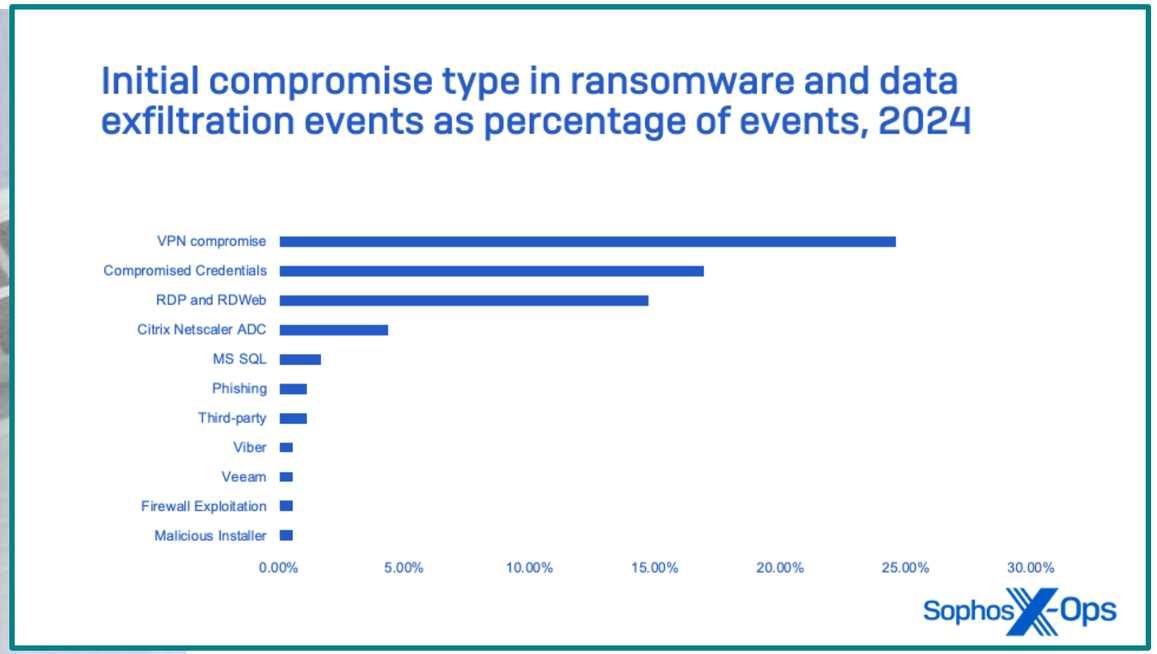


glueck kanja

Sophisticated Attacks vs. Reality

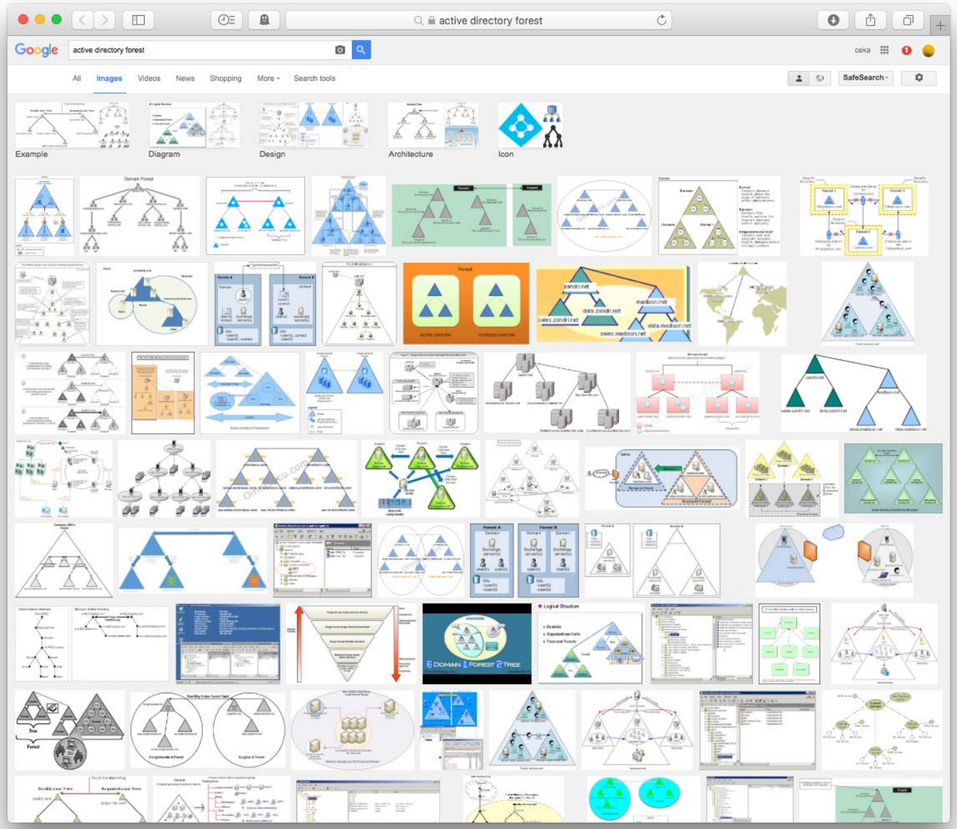
Reality Check





glueck kanja

30 Years of Identity: Active Directory



- Initially not developed for Cloud and “Zero-Trust”
- 1001 configuration possibilities
- Historical grown setups: OUs, Trusts, Delegations, Service Principals, ….
- One of the most popular “lateral movement tools”

Surprises @ work

~~0010 SYSTEM FAILURE 0010~~

****

Attention! Your documents, photos, databases, and other important files have been encrypted!

****

The only way to decrypt your files, is to buy the private key from us.

You can decrypt one of your files for free, as a proof that we have the method to decrypt the rest of your data.

In order to receive the private key contact us via email:
getmyfilesback@airmail.cc

CODE:

00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000

Remember to hurry up, as your email address may not be avaliable for very long.
Buying the key immediatly will guarantee that 100% of your files will be restored.

Below you will see a big base64 blob, you will need to email us and copy this blob to us.
you can click on it, and it will be copied into the clipboard.

If you have troubles copying it, just send us the file you are currently reading, as an attachment.

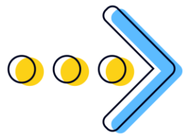
00000
00000
00000
00000
00000
00000
00000
00000

Base64:

uALejkvaX3X1Ywp+Humm7Kz8PyOAgQCFphYLHRMybD600e8Hhn2PZwK2lgAh38jp2PQ/dJFPN6IyDefNk6MTTUZxqWekru0YYSCELyn18FlKrJYt3y0NdkFt57qIlUaI0AQ33EuQAEDfQM8adxRwE1rYNrmM2e/WfaP3NiT31IKeVPe7KZcwA2JqkhYQV7J

Experiences from the field

Digital Communication
is broken

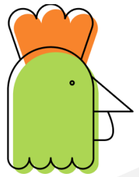


Identities are starting point for restore
Domain Controller is the foundation
for most (legacy) application

Missing trust in existing
infrastructure

External parties delaying restore

Greenfield for AD Domain
is almost impossible



Processes are not in place, time is
running away

glueck kanja

Experiences from the field

Di
is

ies are starting point for restore
in Controller is the foundation
st (legacy) application

M
inf

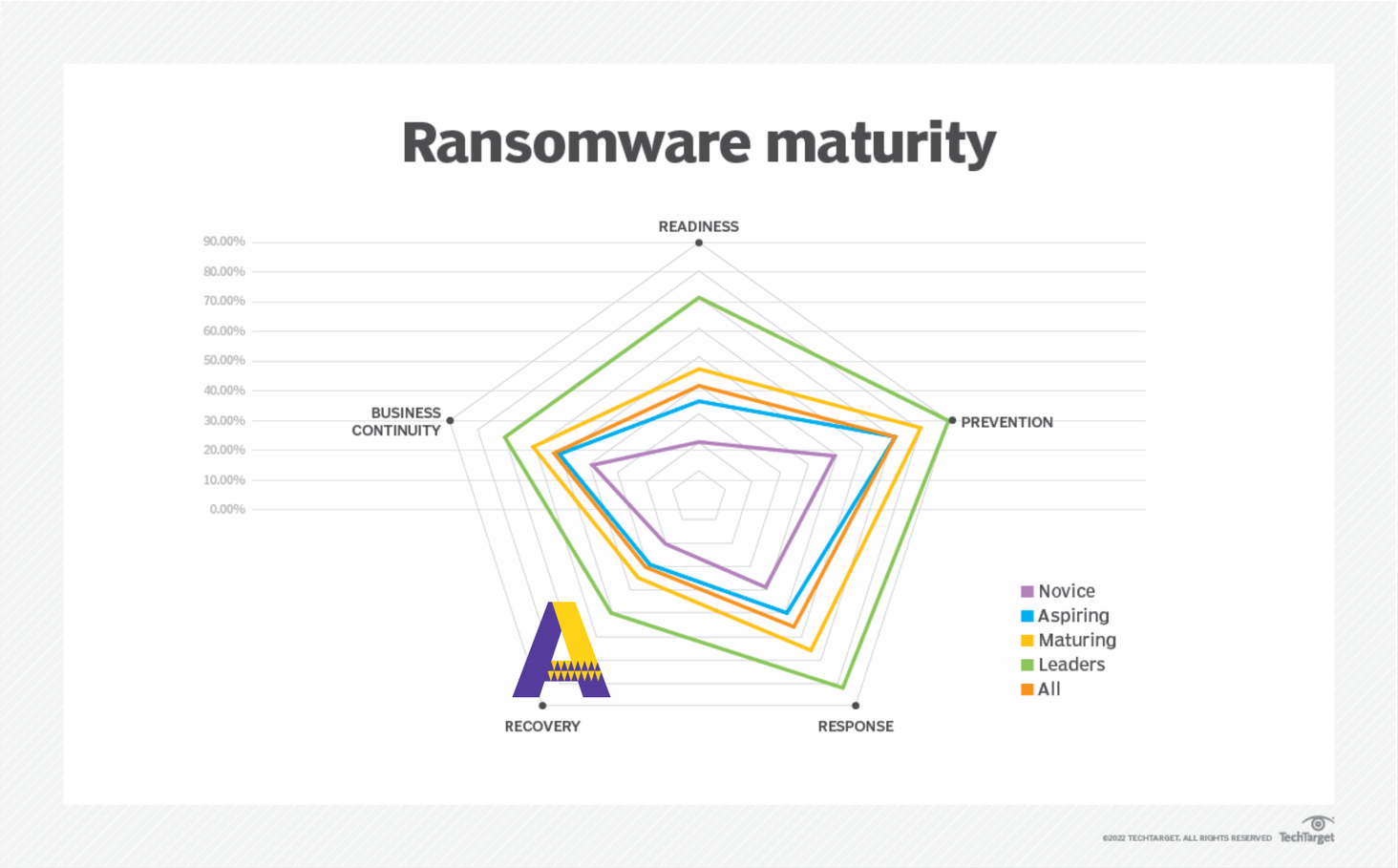
al parties delaying restore

Gr
is

sses are not in place, time is
g away

glueck kanja

Experiences from the field



glueck kanja

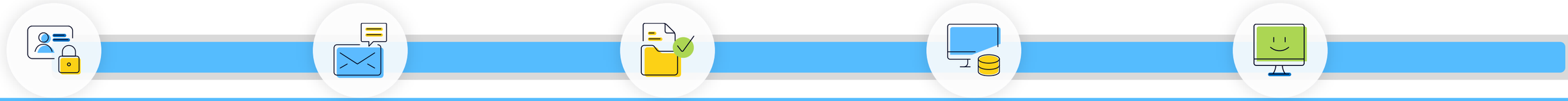
The Idea of a Minimum Viable Company (MVC)

The Minimum Viable Company is not about doing less – it's about doing what matters most.

glueck kanja

Minimum Viable Company Recovery – From Incident to Operability

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
0-4 hours	0-1 days	2-4 days	5-7 days	2-4 weeks



MVC Core Process

Access & Control

- Activate Break-Glass accounts
- Disable compromised user identities
- Isolate affected devices or systems
- Begin incident documentation

Communication Channels

- Restore email access
- enable internal communications (Teams, mobile)
- Inform key stakeholders and partners

Minimal Business Continuity

- Access key operational documents, customer and project data
- Support critical business operations manually

Service Readiness

- Bring essential business applications back online
- Restore access to ERP, CRM, and key SaaS platforms
- Reconnect EDI integrations or partner APIs

Full Restoration

- Resume full operations, including finance, HR, and logistics systems
- Restore CI/CD pipelines, monitoring, and reporting platforms
- Conduct forensic review and implement long-term security improvements

AzERE

glueck kanja

Introducing AzERE

Azure **E**mergency **R**esponse **E**nvironments

glueck kanja

Goals of AzERE

Design a solution that protects critical business services and withstands a **successful** ransomware attack.

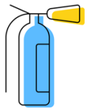
Critical business services consists of

- Active Directory
- Identities
- Critical documents and data
- Optional: A defined set of critical business applications

An automated process to provide a collaboration platform to a subset of users within the first hours after the attack.

Deploy scalable and secured Virtual Desktop Infrastructure

After a successful ransomware attack, the RTO for the most critical services should be only a few hours



Strong focus on REGULAR fire testing

The environment is built with 100% DevOps including Infrastructure as Code with terraform.

glueck kanja

Non-goals of AzERE

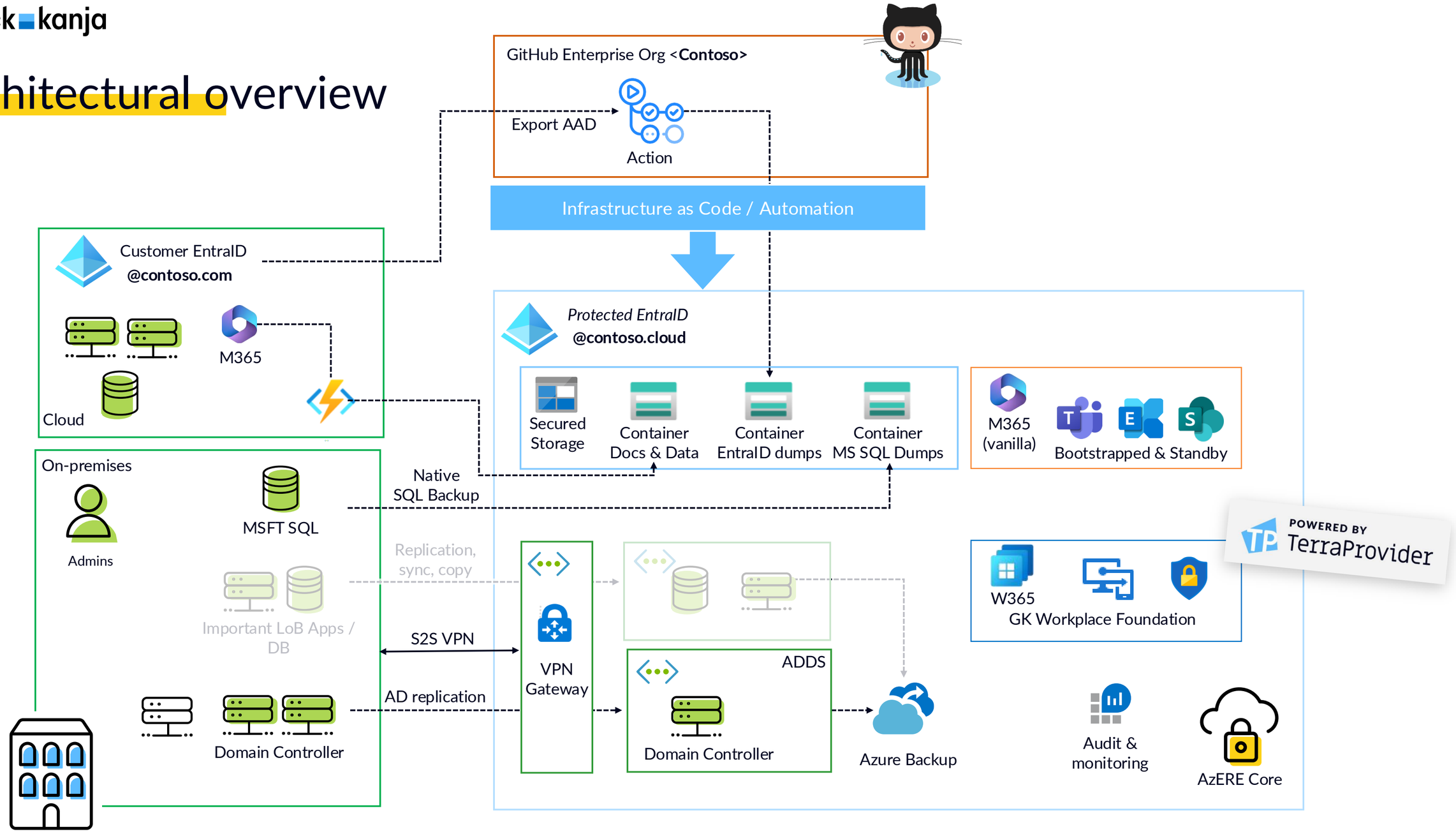
The solution is **not a backup replacement**.

This solution is **not a complete business continuity** and disaster recovery (BCDR) strategy. AzERE can be a part of your BCDR strategy to quickly recover from a successful ransomware attack.

In case of disaster AzERE will **not replace your production environments**. It is a temporary environment to support the restore process of your production environments.

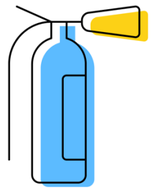
glueck kanja

Architectural overview



glueck kanja

AzERE Services by glueckkanja



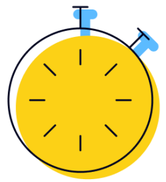
Monthly Fire-Drilling and Emergency Testing

Keep AzERE up-to-date with platform changes (M365 & Azure updates)

Ongoing Development of new AzERE features

24/7 On-call Hotline for Emergency Activation (technical)

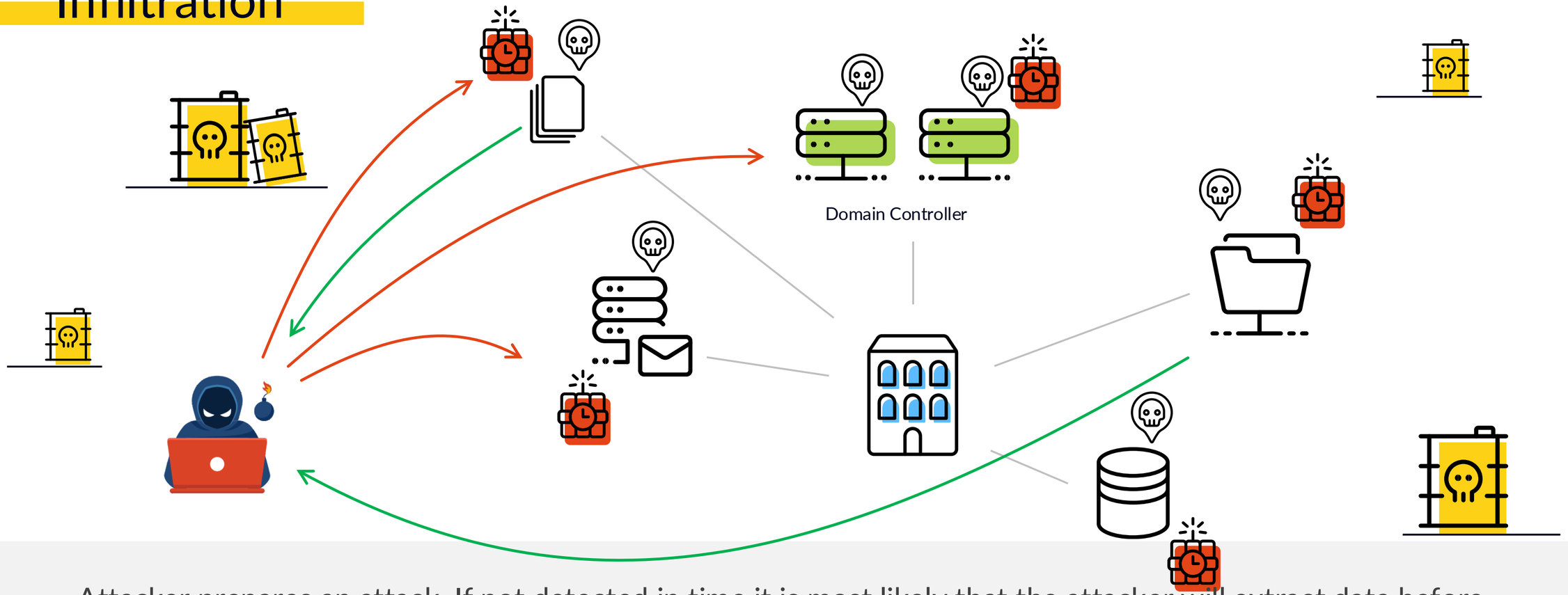
24/7 Manager On Duty (organizational)



Fasttrack to APT response services

glueck kanja

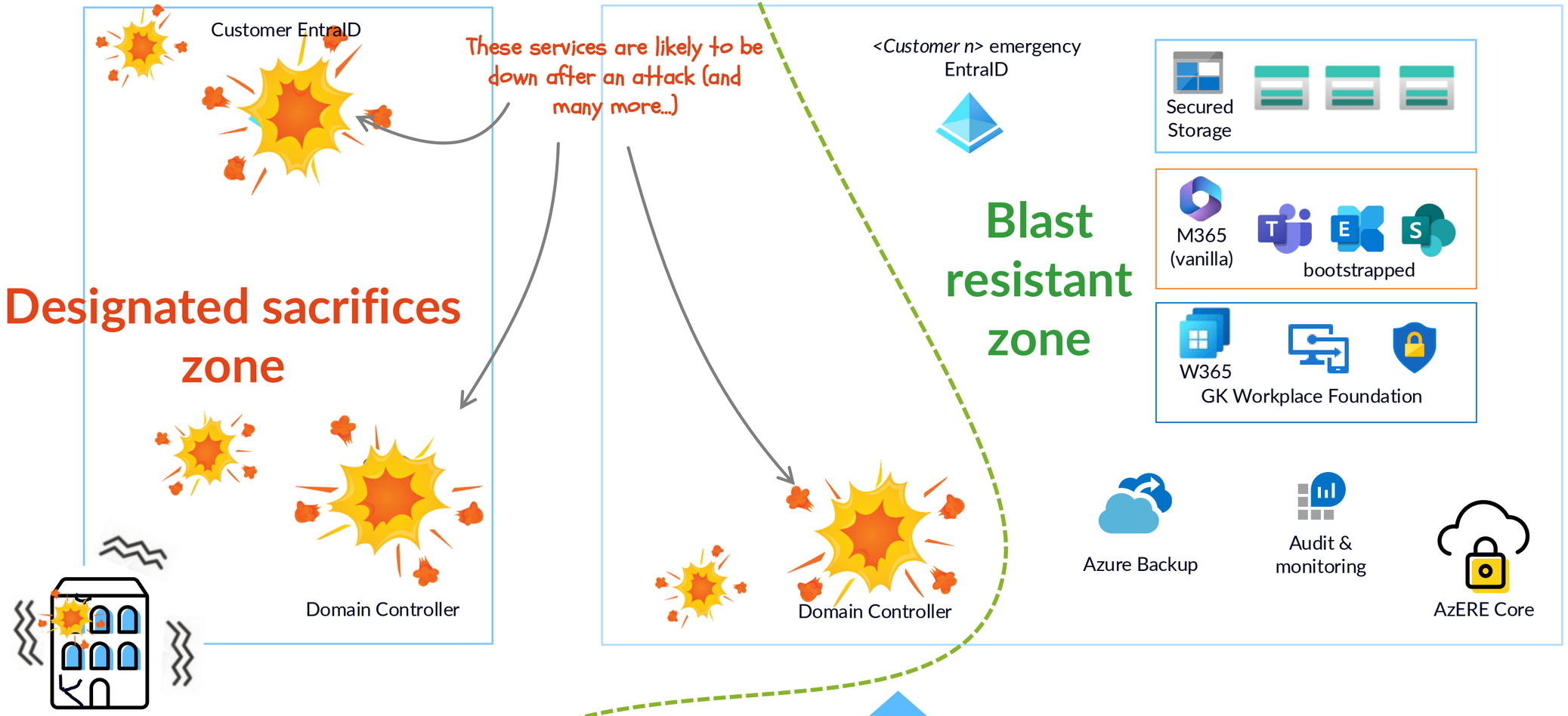
Infiltration



– Attacker prepares an attack. If not detected in time it is most likely that the attacker will extract data before encrypting as much systems as possible

glueck kanja

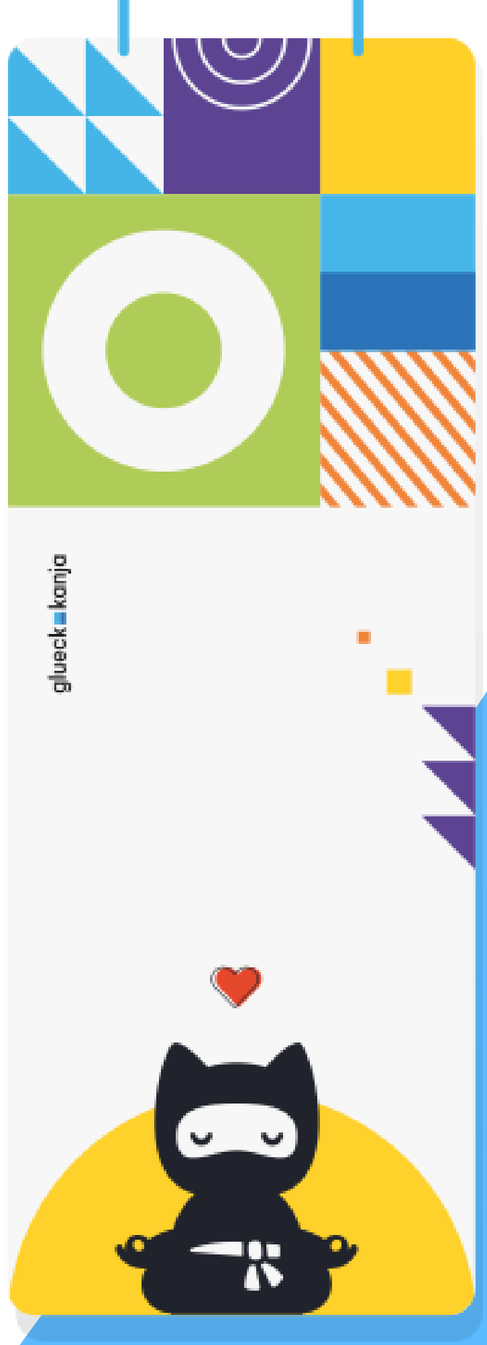
The successful attack



glueck kanja

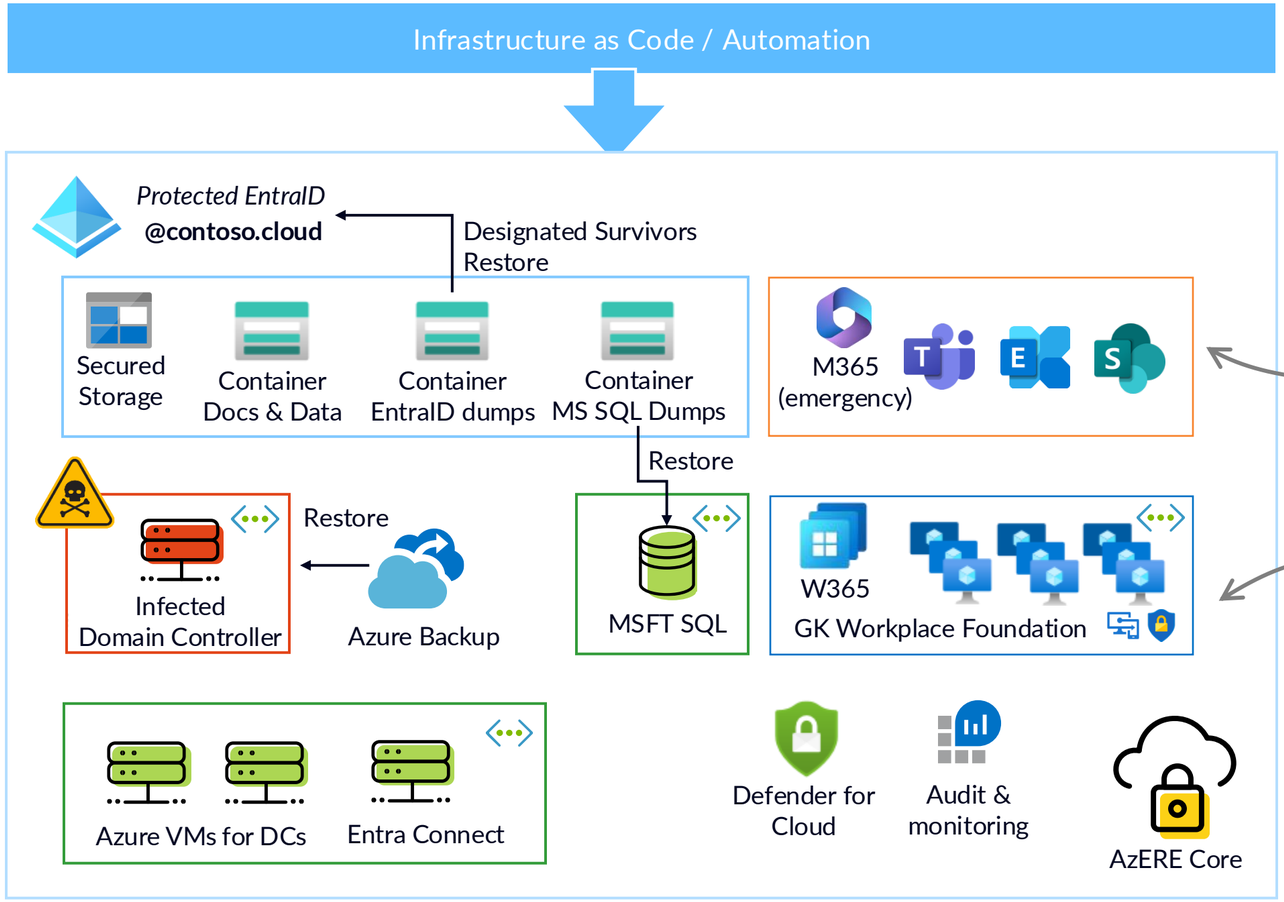
The ZenMat

YES, TAKE ME WITH YOU.



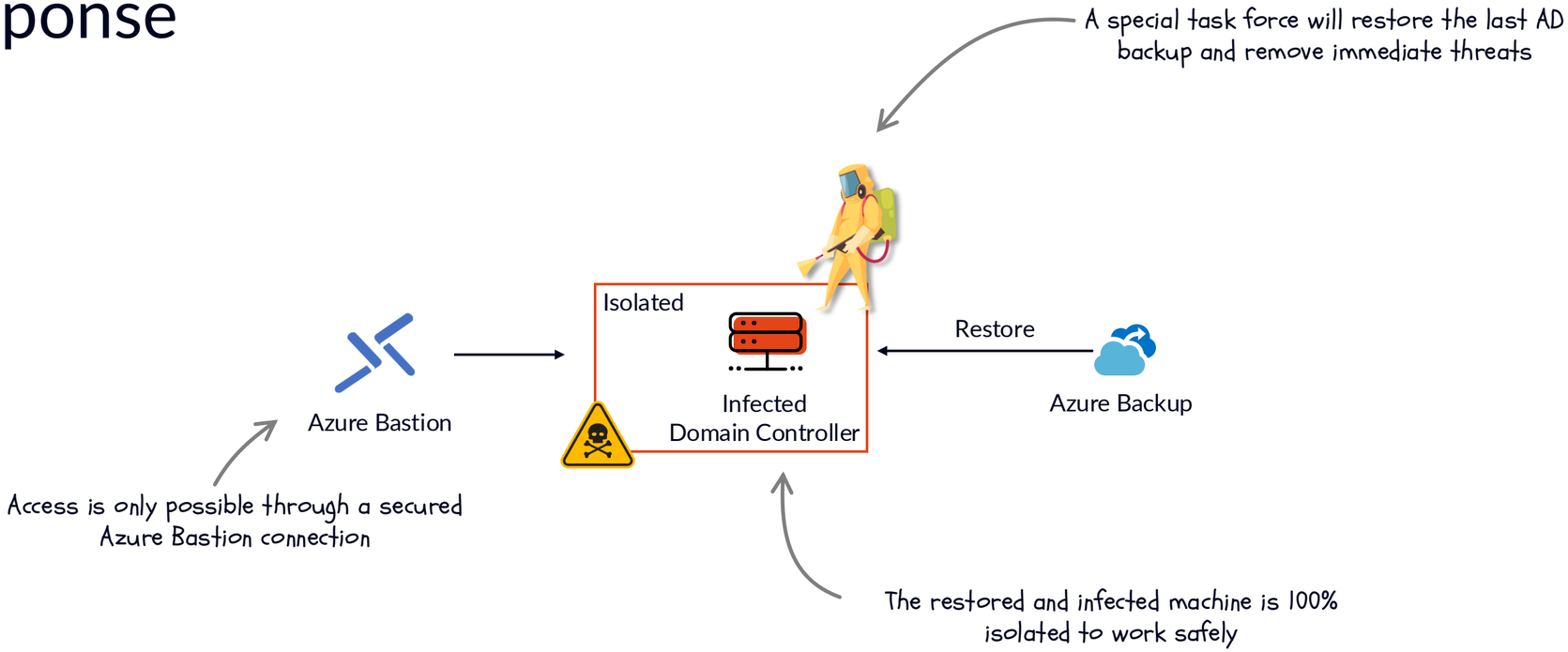
Emergency Response Activation

Ground Zero – First Response



glueck kanja

APT response



- Quick start, independent of customer systems. No need for customers Network/Server/Backup teams (and their consultants) to get alerted/up and running again
- Customer provides (BreakGlass)Admin credentials

glueck kanja

The AD cleaning details

APT Playbook

Secrets

Certificates

Group Policies

Other attacker persistence

Toolchain

Forensic scanner tool

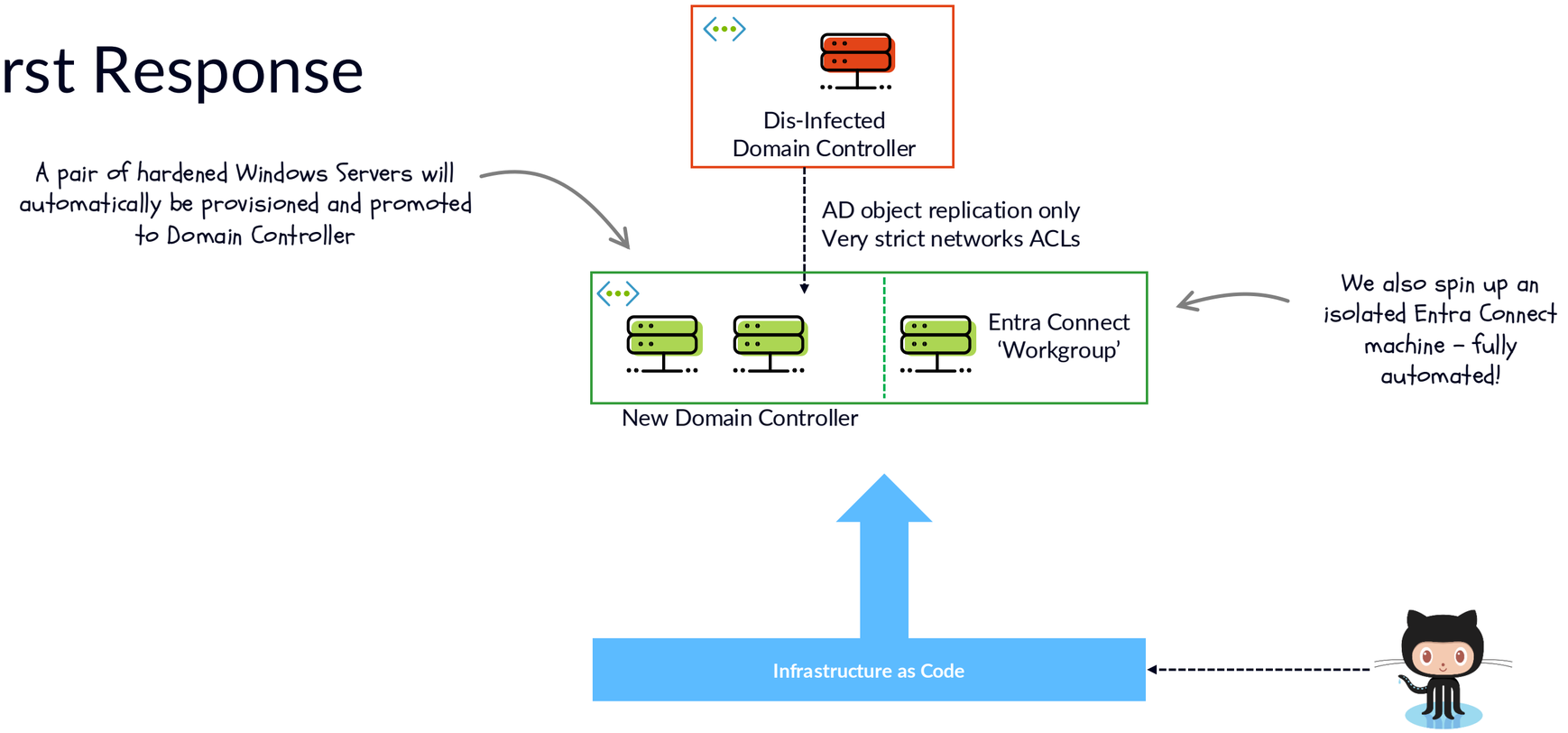
Antivirus and Behavior scanning

AD config/hardening scan

- Generic FullForest Recovery first (seize FSMO, remove all other DCs, ...)
- Renew all credentials
- Use tools for Forensic, AV, Hardening
- Check modified configs for persistence

glueck kanja

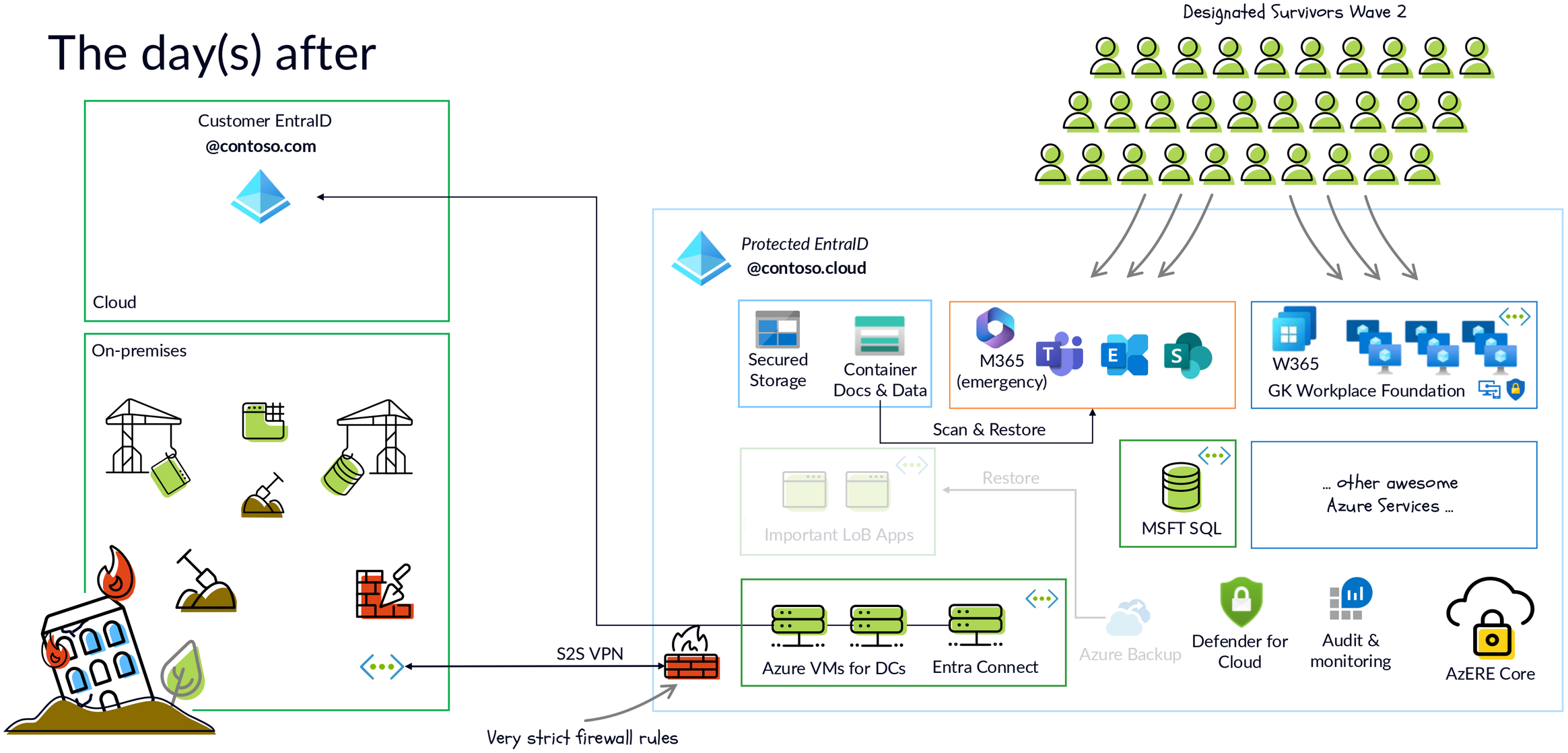
First Response



- A second resource group is created to hold cleaned resources for the rebuild process.
- Two new Windows Servers are created and automatically prepared to get promoted for the ADDS role
- A third server in a dedicated subnet is created and prepared for a fresh Entra Connect instance.
- After successful DC promotion the „disinfected“ Domain Controller will be deleted.

glueck kanja

The day(s) after



glueck kanja

Dandy Bräunlich

— **Bereichsleitung IT der igefa**

— dandy.braeunlich@igefa.de

… / dandybraeunlich

glueck kanja

Thank you!

“Prediction is very difficult, especially if it's about the future.”

– Nils Bohr, Nobel Prize in Physics

With

glueck kanja