white duck

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

CyberSecurity Weißwurstfrühstück, Mai 2025

Microsoft Solutions Partner
Digital & App Innovation
Azure
Specialist
DevOps with GitHub

Microsoft Solutions Partner
Data & AI
Azure
Specialist
Migrate Enterprise Applications to Microsoft Azure

white duck

Wer bin ich?

Nico Meisenzahl
Geschäftsführer | COO

+49 8031 230159-112

nico.meisenzahl@whiteduck.de

@nmeisenzahl

www.linkedin.com/in/nicomeisenzahl

- Cloud Solution Architect
- Azure & Developer Technologies MVP

Ihr Partner für Microsoft Azure & AI

Cloud Native Entwicklung

Konzeption und Entwicklung von nachhaltigen und intelligenten Anwendungen.

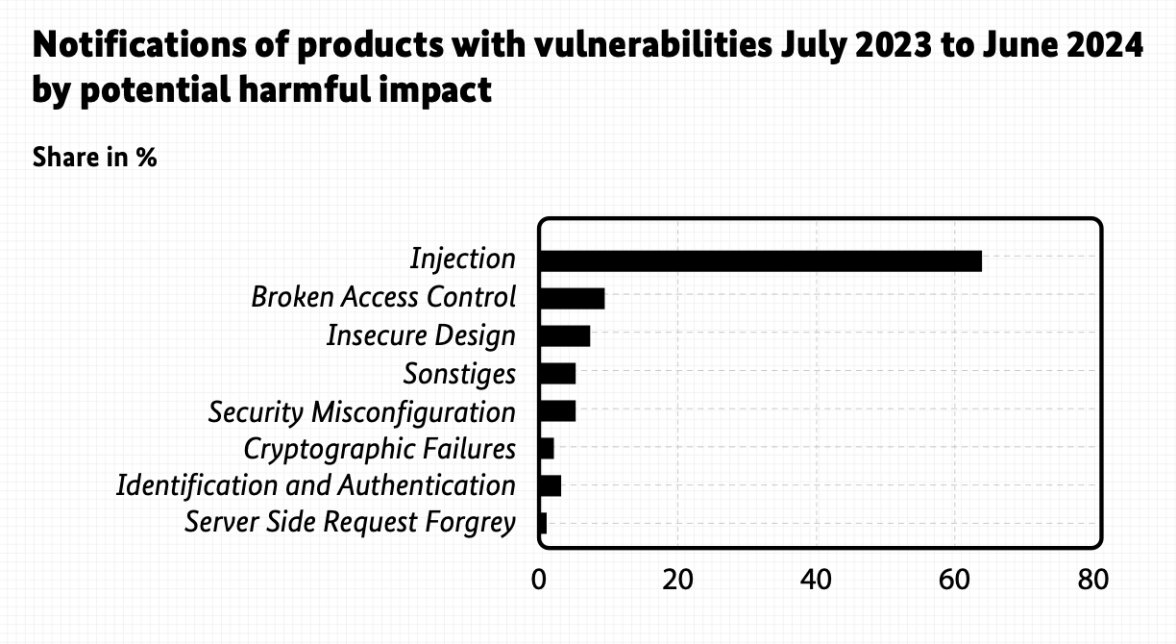
Platform Engineering

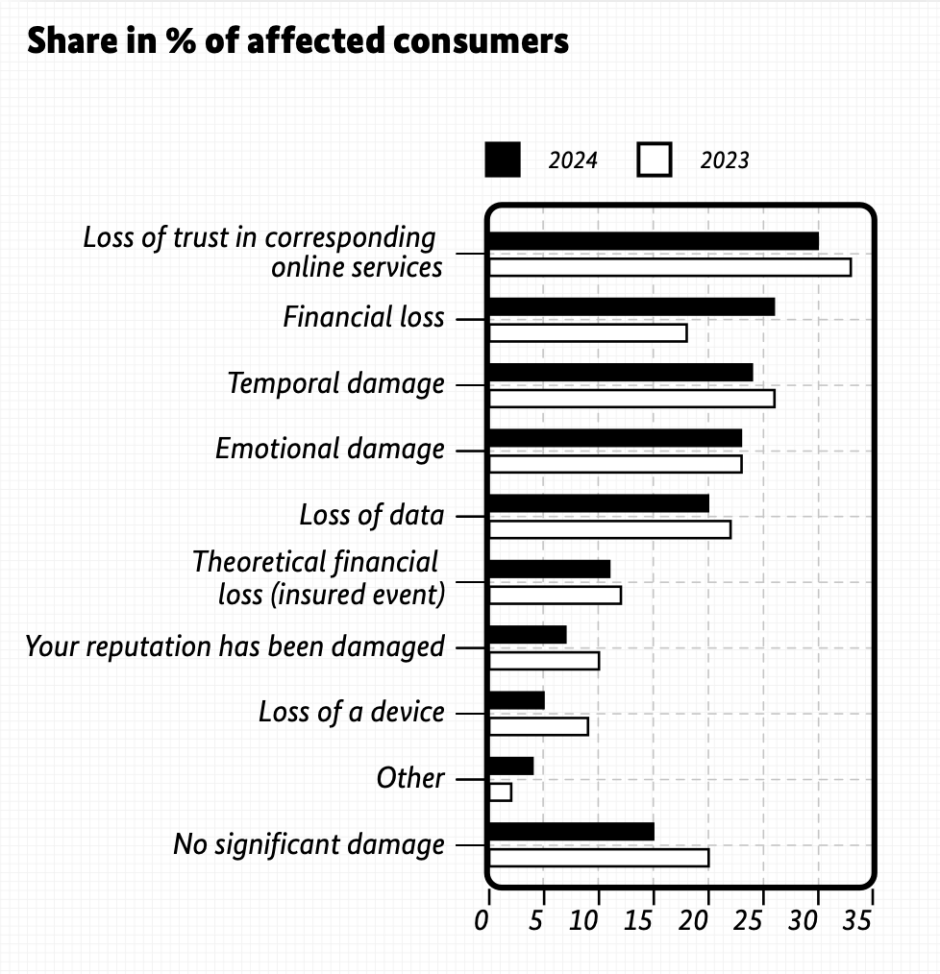
Planung, Implementierung und Betrieb skalierbarer Anwendungsplattformen.

Developer Productivity

Mehr Produktivität und Sicherheit durch KI und agile Prozesse.

State of security in Germany

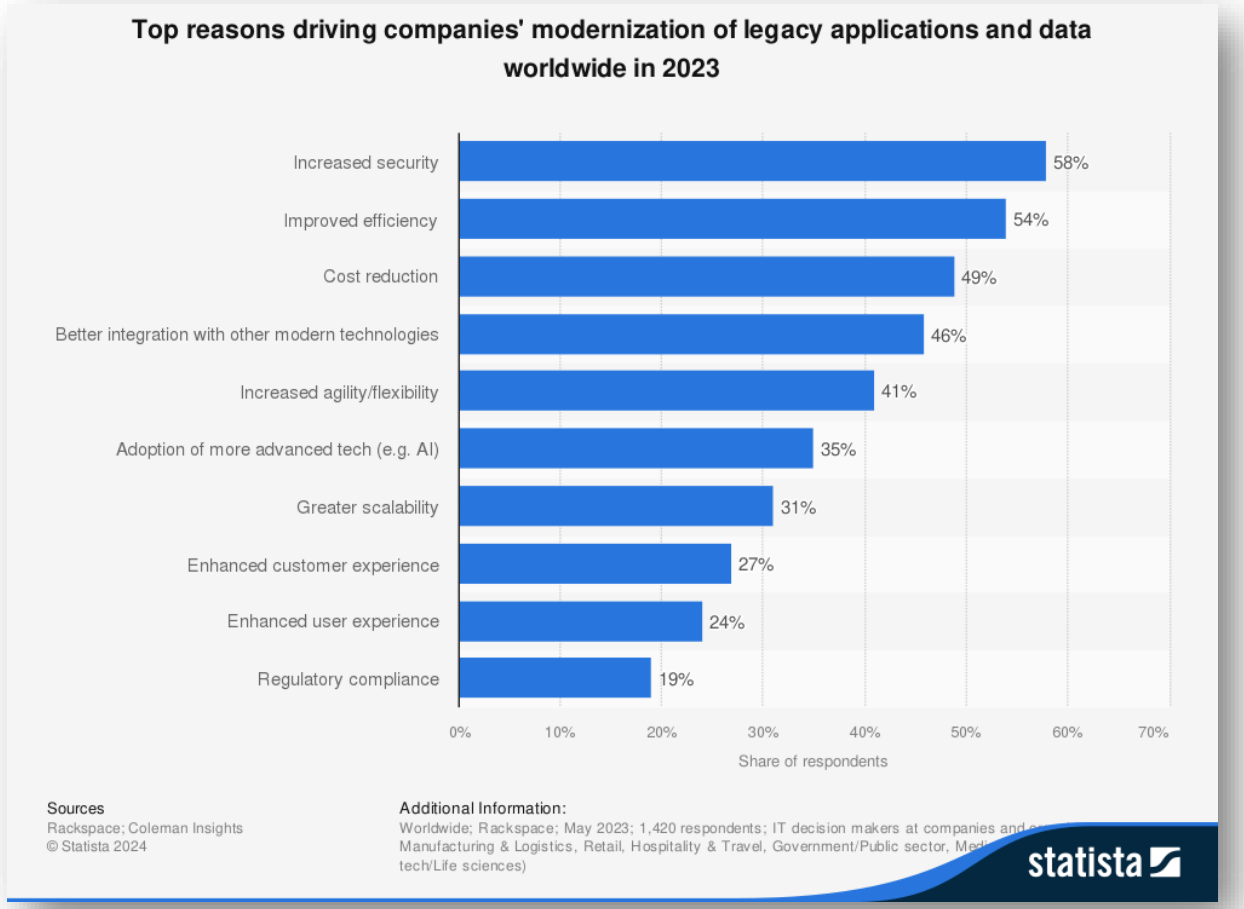




The State of IT Security in Germany 2024 (BSI)

Cloud-native as the fundamental basis

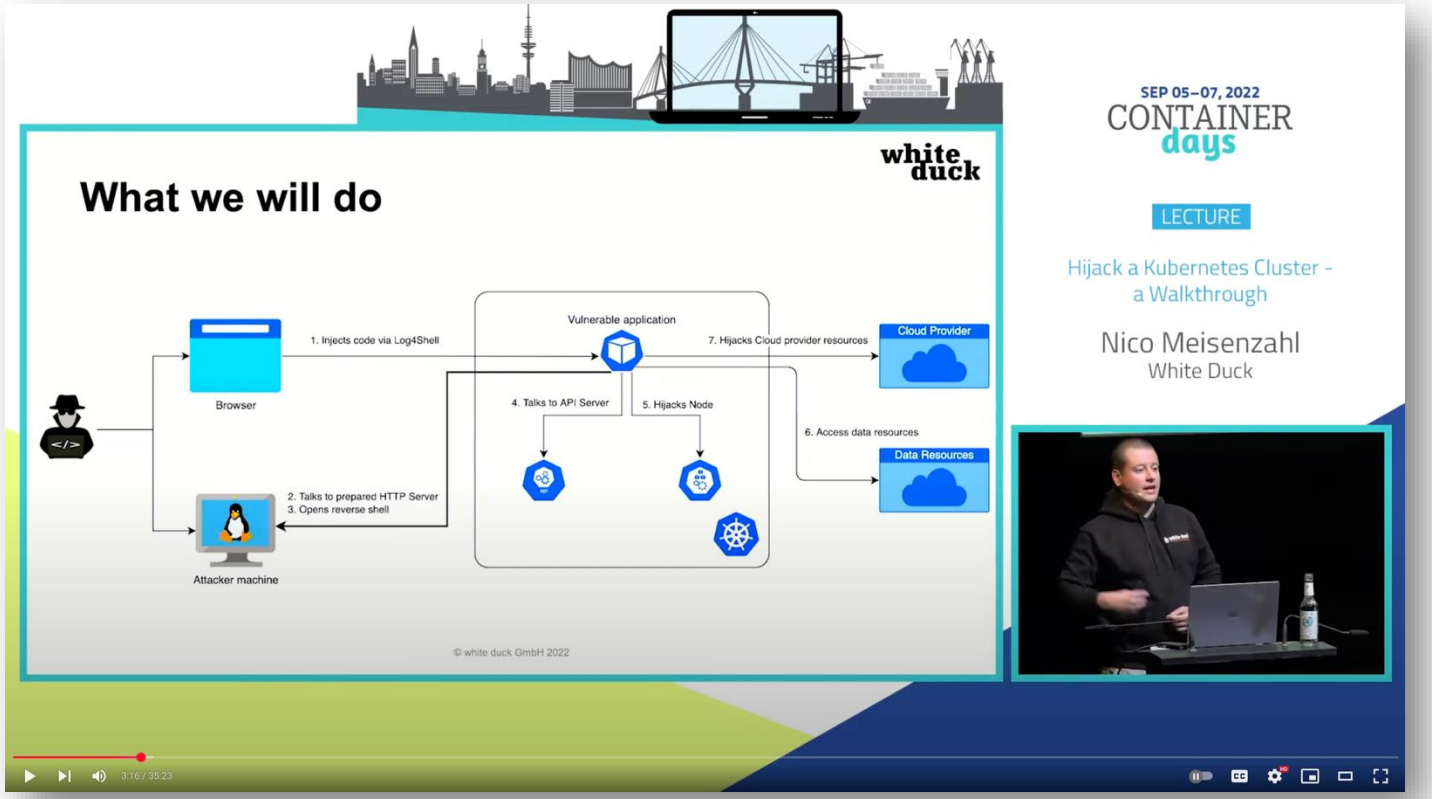
Gartner predicts that **by 2025, more than 95%** of all new digital apps will be delivered on cloud-native platforms, up from 30% in 2021. *



* Gartner, “Your Detailed Guide to the 2024 Gartner Top 10 Strategic Technology Trends”

Example: Log4Shell

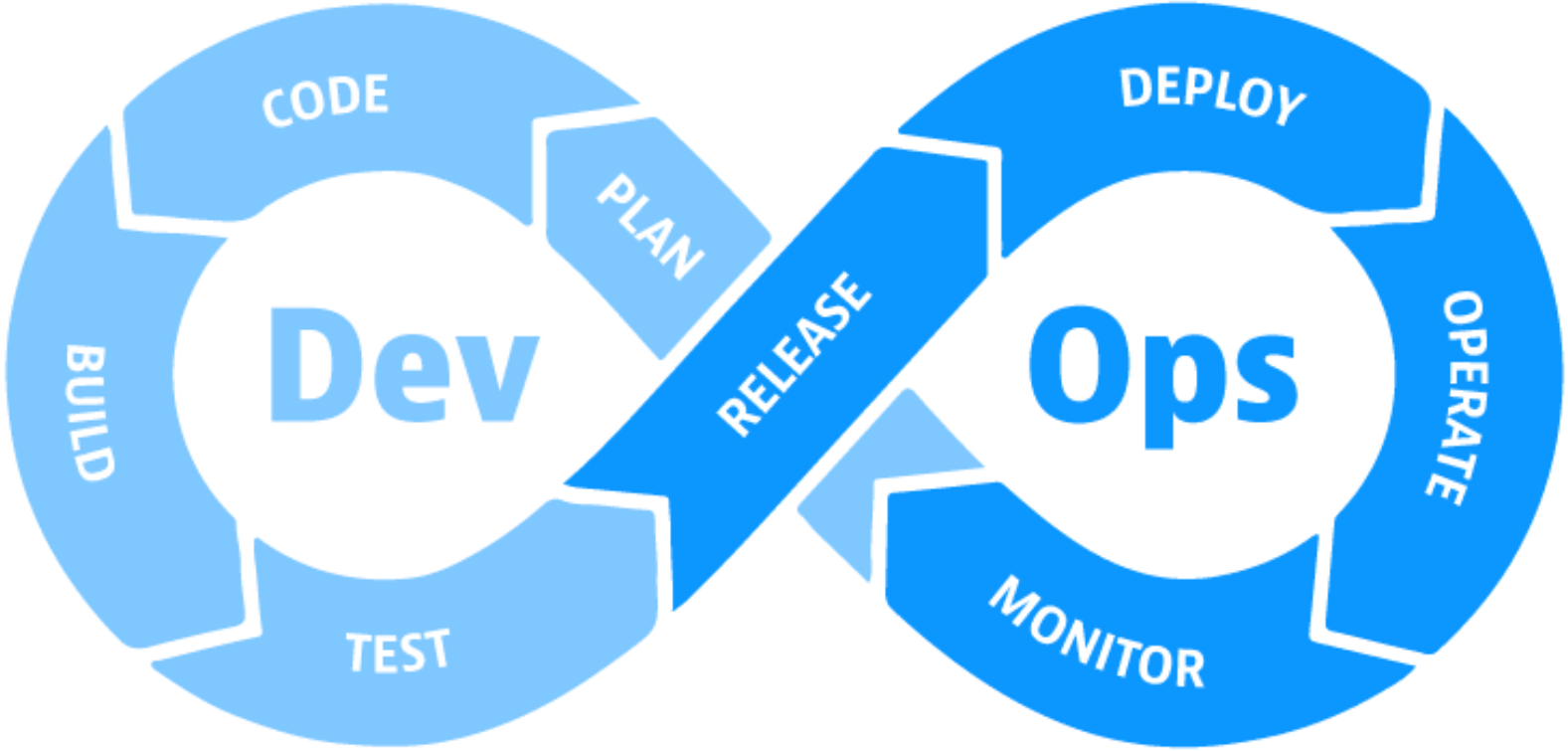
Log4Shell in a shared environment like Kubernetes can lead to gaining access to other applications, data or even unrelated cloud resources!



Hijack a Kubernetes Cluster – a Walkthrough

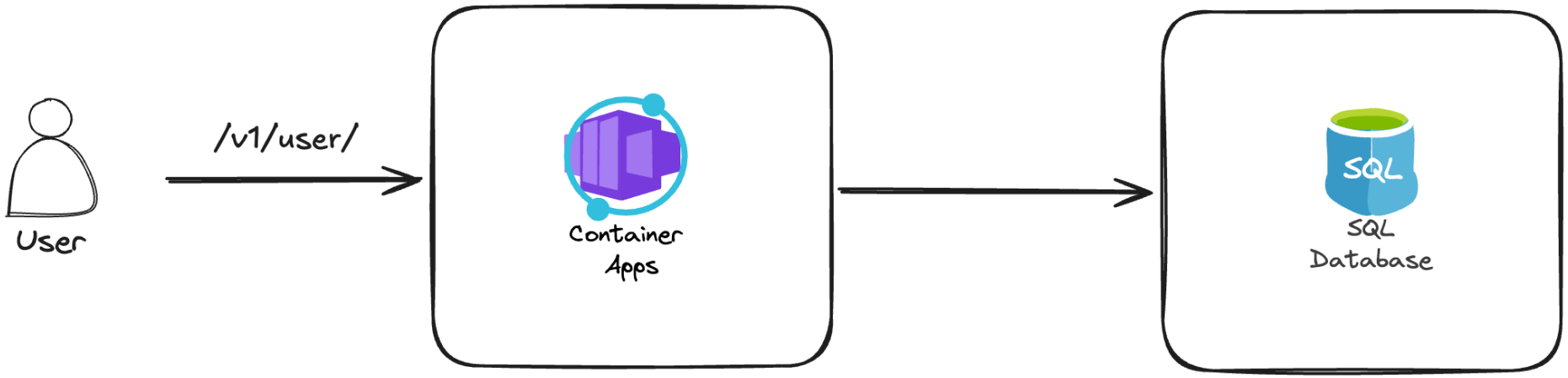
DevSecOps

... is the **integration of security** within the whole DevOps process.



Picture source: https://www.dynatrace.com

Today‘s demo application

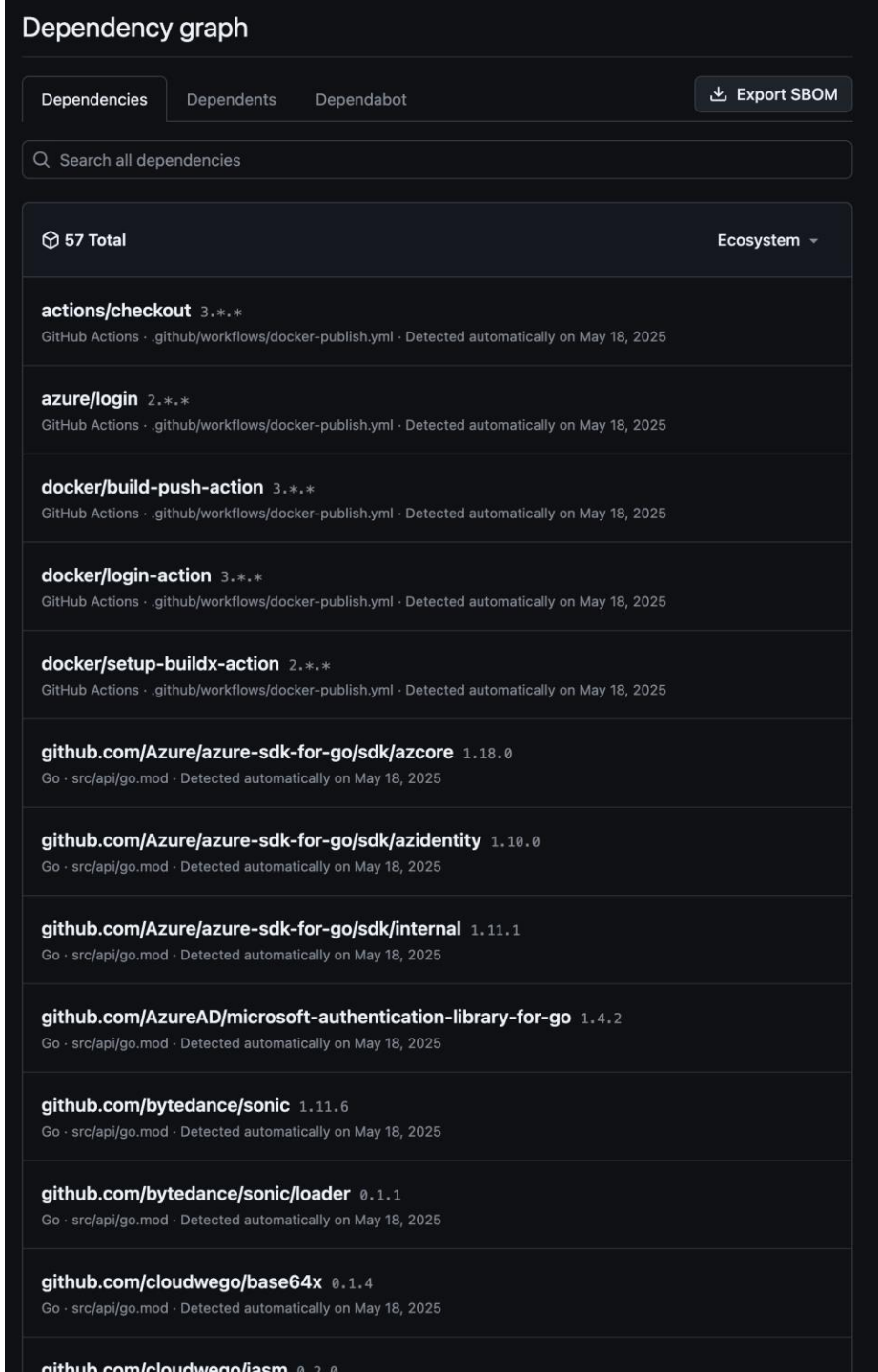


Dependencies

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

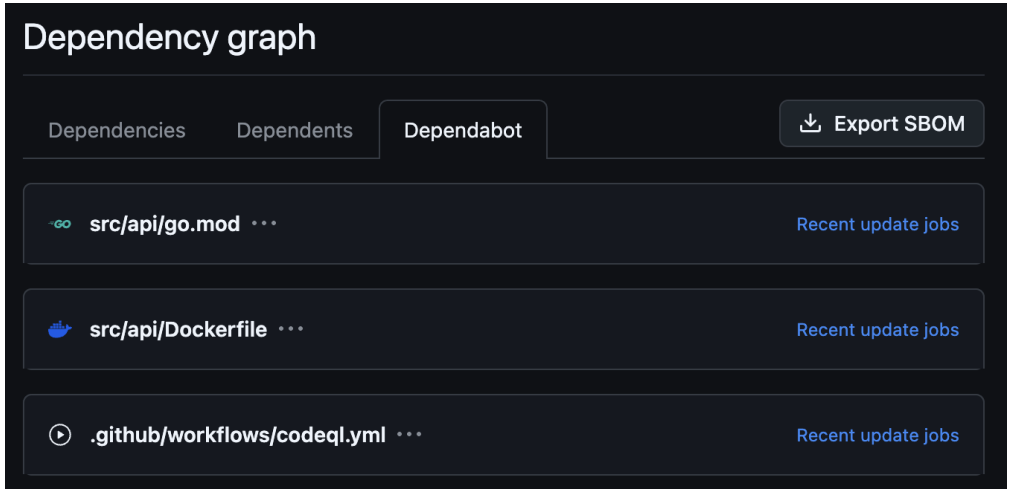
Dependency awareness

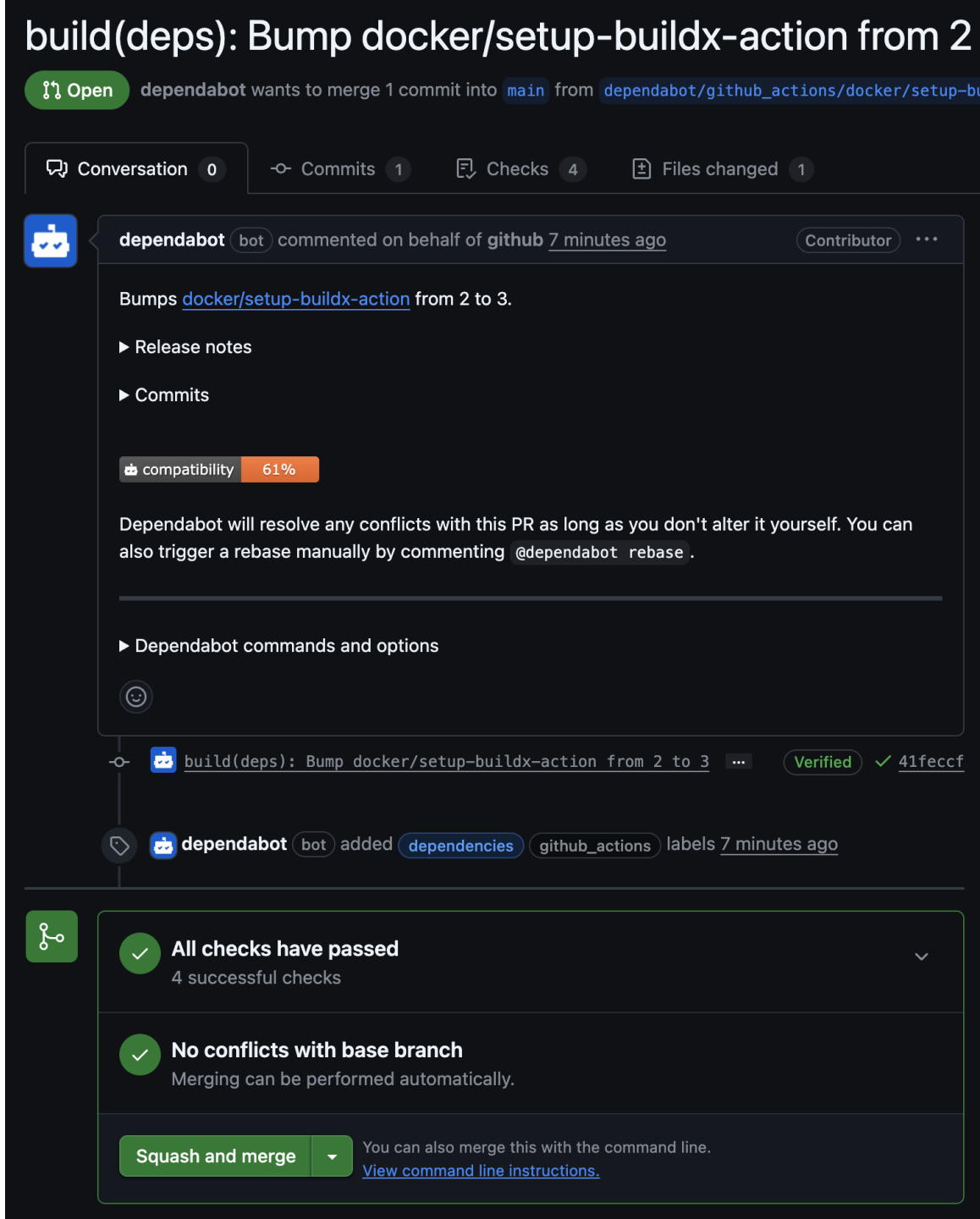
- Software Bill of Materials (SBOM)
  - “List of ingredients” for all your software and dependencies
  - Baseline for vulnerability and licensing scanning
- SBOMs is the baseline for your dependency tracking
  - and therefore, vulnerability scanning
  - but can also track your dependency licenses
- Without it, you don’t have full visibility



Dependency updates

- Dependabot continuously monitoring dependencies
  - It creates pull requests to update outdated or vulnerable packages
- Open source: Renovate
  - https://github.com/renovatebot/renovate

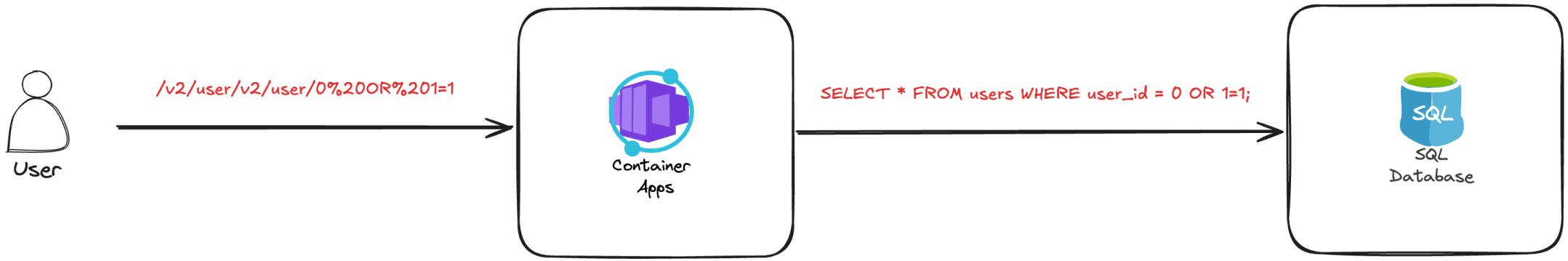




Shift security left

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

Example: SQL-injection

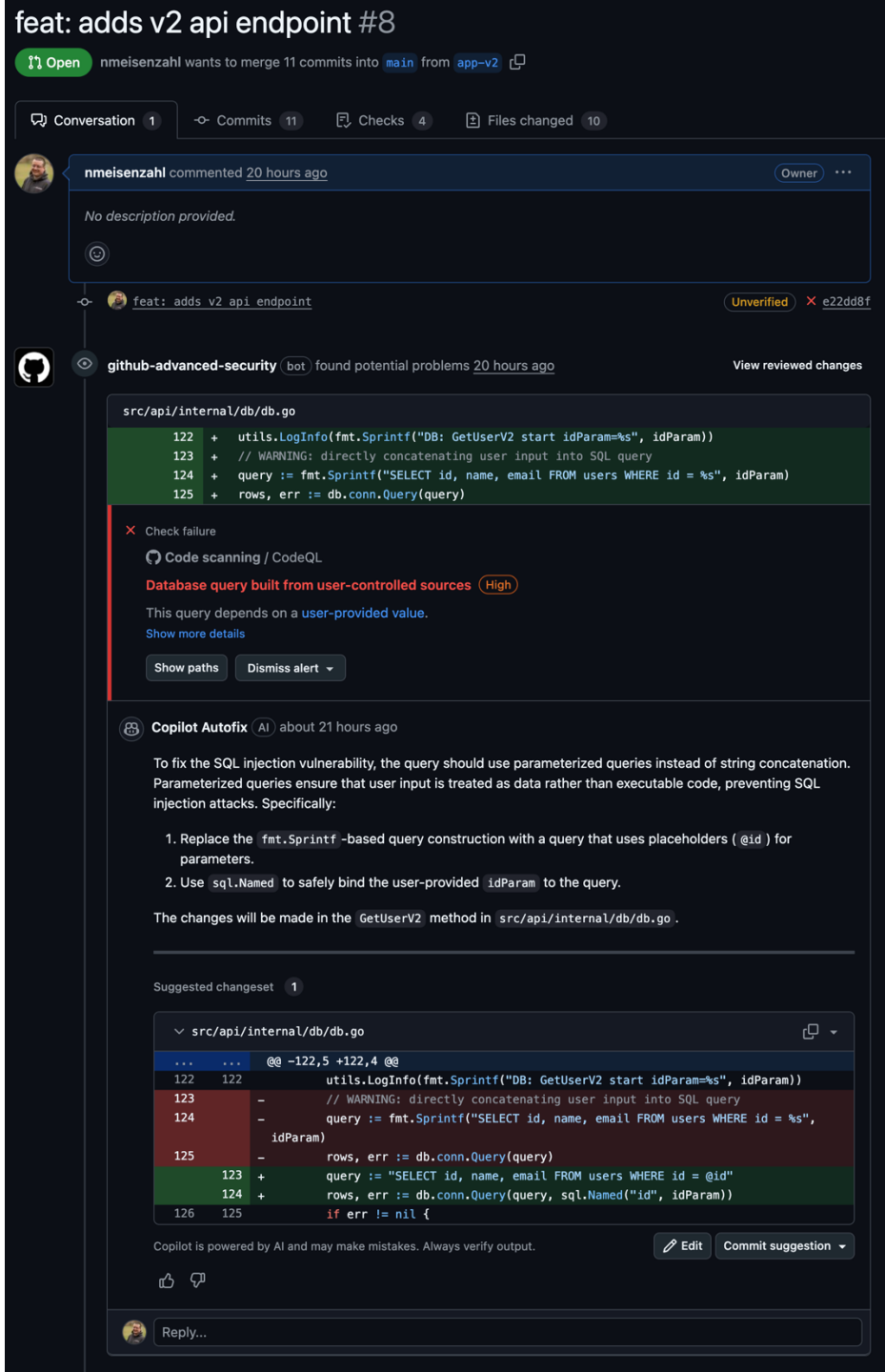


The 1=1 condition always evaluates to TRUE.

As a result, the WHERE clause becomes irrelevant because of the OR condition.

Early awareness with code analysis

- Enforce Static Application Security Testing (SAST) in PRs
  - scans your code to identify potential security vulnerabilities and secrets
- Implement automated Dynamic Application Security Testing (DAST)
  - black-box scanning against a running web application
- GitHub Advanced Security brings a fully-integrated SAST code scanning based on CodeQL
  - based on 2000 open-source policies and 13 years of research



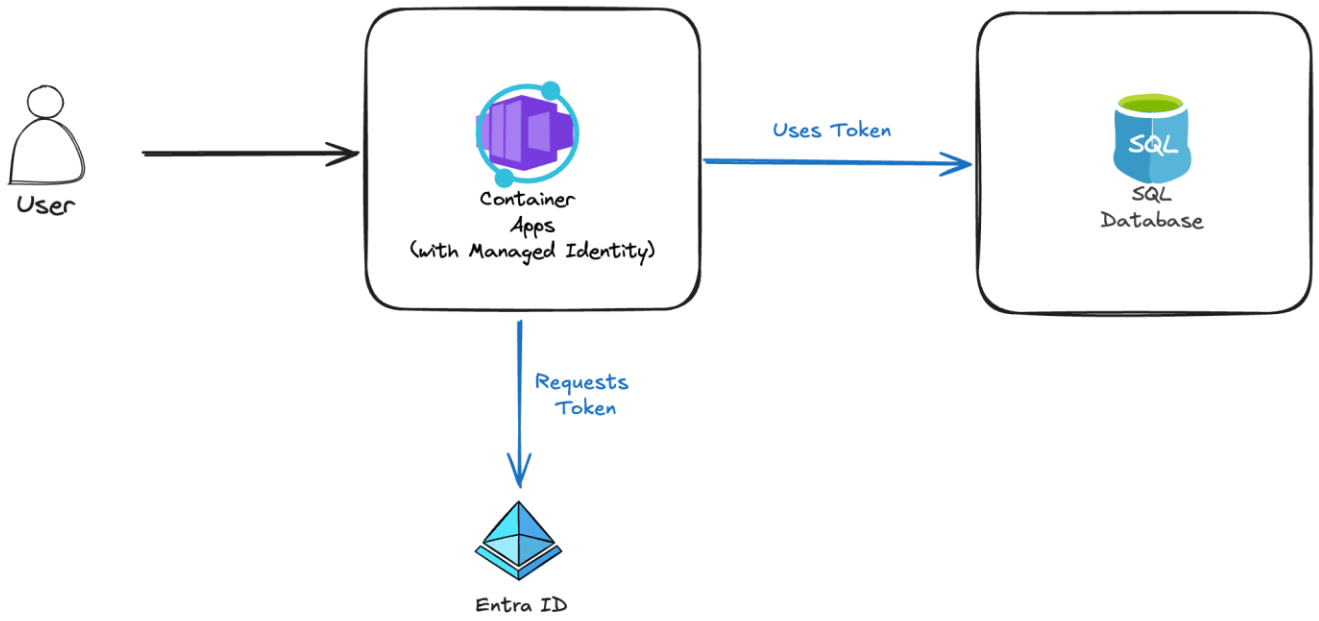
Full flexibility with open source

- Code scanning (SAST) based on your dev stack
  - https://owasp.org/www-community/Source_Code_Analysis_Tools
- Code scanning for DevOps/Platform with trivy & checkov
  - https://trivy.dev
  - https://www.checkov.io
- Dependency tracking (SBOM) and vulnerability scanning with syft & grype
  - https://github.com/anchore/syft
  - https://github.com/anchore/grype

Cloud-native architecture

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

Managed identity for database access

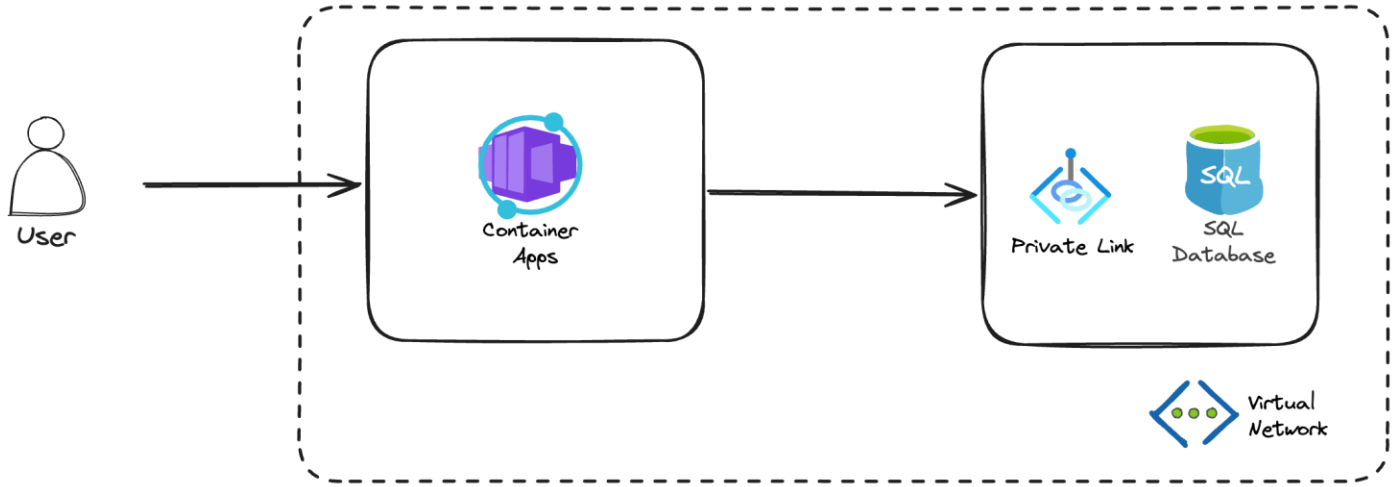



```go
// NewConnection creates a new DB using the provided context and config
func NewConnection(ctx context.Context, cfg *configs.Config) (*DB, error) {
  utils.LogInfo("DB: starting new connection")
  // Use values from external configurations to configure connection properties
  server := cfg.DBServer
  database := cfg.DBDatabase

  // Use Azure's DefaultAzureCredential for authentication
  cred, err := azidentity.NewDefaultAzureCredential(nil)
  if err != nil {
    utils.LogError(err)
    return nil, fmt.Errorf("failed to obtain Azure credential: %v", err)
  }

  // Build base connection string with Active Directory token authentication enforced
  baseConnStr := fmt.Sprintf("server=%s;database=%s;encrypt=true;authentication=ActiveD
  // Token provider using DefaultAzureCredential
  tokenProvider := func() (string, error) {
    tok, err := cred.GetToken(ctx, policy.TokenRequestOptions{
      Scopes: []string{"https://database.windows.net/.default"},
    })
    if err != nil {
      utils.LogError(err)
      return "", fmt.Errorf("failed to refresh Azure token: %v", err)
    }
    return tok.Token, nil
  }
  connector, err := mssql.NewAccessTokenConnector(baseConnStr, tokenProvider)
  if err != nil {
    utils.LogError(err)
    return nil, fmt.Errorf("failed to create token connector: %v", err)
  }
  conn := sql.OpenDB(connector)
```

Authentication between Azure resources

- Relying on connection strings isn't the best idea
  - Long living secrets without rotation
  - Connections string needs to be stored and injected
- Managed Identity (Workload Identity) solves this issue
  - It is essentially a managed service principal living in your Entra ID
  - Relies on certificate-based with expiration of 90 days and rollover every 45 days
- There is a system-assigned and user-assigned option
- Abstracted via Azure SDK Azure.Identity library *“DefaultAzureCredential”*
  - Supports all credential types which is helpful for developer inner loop

Private Link for database access




```
// Private Endpoint for SQL Server to allow private connectivity
You, 22 hours ago | 1 author (You)
resource "azurerm_private_endpoint" "sql_pe" {
  name                = "${var.prefix}-sql-pe"
  resource_group_name = azurerm_resource_group.rg.name
  location            = azurerm_resource_group.rg.location
  subnet_id           = azurerm_subnet.pe_subnet.id

  You, 22 hours ago | 1 author (You)
  private_service_connection {
    name                           = "sql-psc"
    private_connection_resource_id = azurerm_mssql_server.sql.id
    subresource_names              = ["sqlServer"]
    is_manual_connection           = false
  }
}

// Private DNS Zone for SQL Private Endpoint resolution
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_zone" "sql_zone" {
  name                = "privatelink.database.windows.net"
  resource_group_name = azurerm_resource_group.rg.name
}

// Link the Private DNS Zone to the VNet
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_zone_virtual_network_link" "dns_link" {
  name                  = "link-to-vnet"
  resource_group_name   = azurerm_resource_group.rg.name
  private_dns_zone_name = azurerm_private_dns_zone.sql_zone.name
  virtual_network_id    = azurerm_virtual_network.vnet.id
}

// A record for SQL Private Endpoint to resolve server privately
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_a_record" "sql_pe_record" {
  name                = azurerm_mssql_server.sql.name
  zone_name           = azurerm_private_dns_zone.sql_zone.name
  resource_group_name = azurerm_resource_group.rg.name
  ttl                 = 300
  records             = [azurerm_private_endpoint.sql_pe.private_service_connection[0].private_ip_address]
}
```

Enables the private access of Azure services in a vNet

- Public endpoints must be locked down separately!
- Increases security and performance

Federated Credentials for GitHub Action authentication

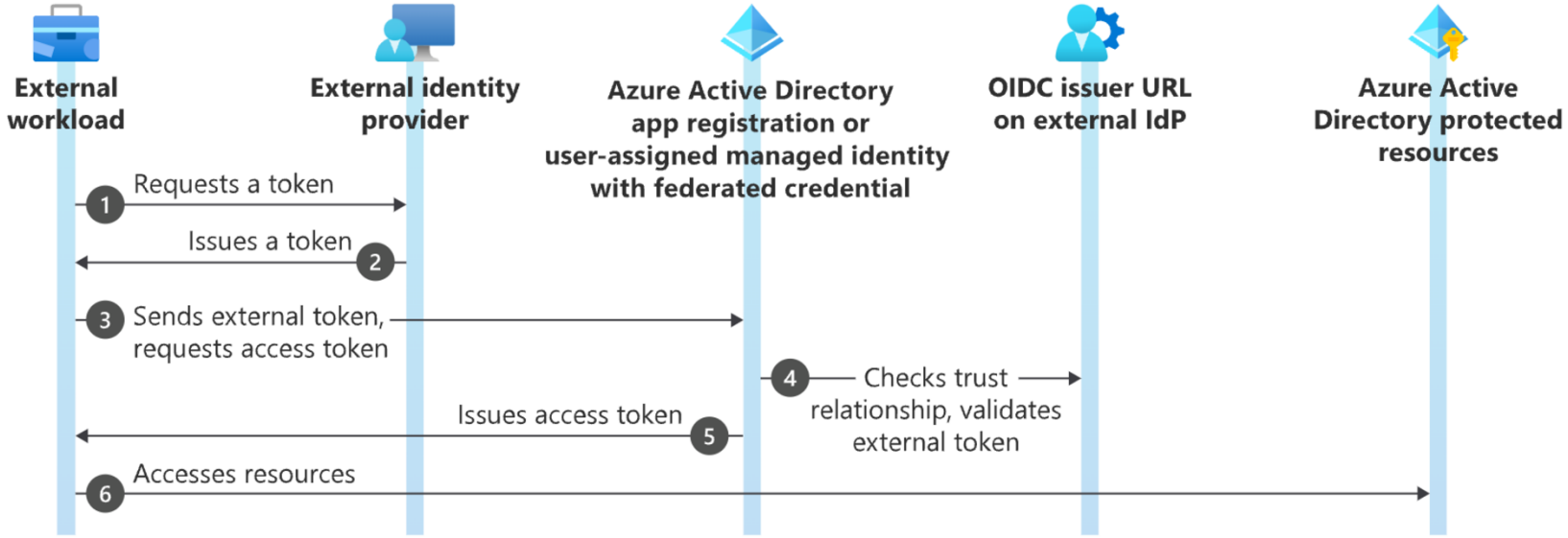
Azure Login using OIDC 5s

```
▼Run azure/login@v2
  with:
    client-id: ***
    tenant-id: ***
    subscription-id: ***
    enable-AzPSSession: false
    environment: azurecloud
    allow-no-subscriptions: false
    audience: api://AzureADTokenExchange
    auth-type: SERVICE_PRINCIPAL
  env:
    CONTAINER_APP_NAME: devsecops-app
    RESOURCE_GROUP: devsecops-rg
Running Azure CLI Login.
/usr/bin/az cloud set -n azurecloud
Done setting cloud: "azurecloud"
Federated token details:
 issuer - https://token.actions.githubusercontent.com
 subject claim - repo:nmeisenzahl/devsecops-25:ref:refs/heads/main
 audience - api://AzureADTokenExchange
 job_workflow_ref - nmeisenzahl/devsecops-25/.github/workflows/docker-publish.yml@refs/heads/main
Attempting Azure CLI login by using OIDC...
Subscription is set successfully.
Azure CLI login succeeds by using OIDC.
```

```
// User-assigned identity for GitHub Actions with federated credentials
You, 2 days ago | 1 author (You)
resource "azurerm_user_assigned_identity" "github_actions" {
  name                = "${var.prefix}-uai-gh"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
}

// Federated Identity Credential for GitHub Actions
You, 16 hours ago | 1 author (You)
resource "azurerm_federated_identity_credential" "github_actions" {
  name                = "${var.prefix}-fedcrd-gh"
  resource_group_name = azurerm_resource_group.rg.name
  parent_id           = azurerm_user_assigned_identity.github_actions.id
  audience            = ["api://AzureADTokenExchange"]
  issuer              = "https://token.actions.githubusercontent.com"
  subject             = var.oidc_subject // repo:nmeisenzahl/devsecops-25:ref:refs/heads/main
}

// Role Assignment for GitHub Actions identity in Resource Group
You, 2 days ago | 1 author (You)
resource "azurerm_role_assignment" "github_actions" {
  scope                = azurerm_resource_group.rg.id
  role_definition_name = "Contributor"
  principal_id         = azurerm_user_assigned_identity.github_actions.principal_id
}

// Managed identity for Application Gateway to access Key Vault
You, 17 hours ago | 1 author (You)
resource "azurerm_user_assigned_identity" "appgw_identity" {
  name                = "${var.prefix}-uai-agw"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
}
```

Securely authenticate with Azure services

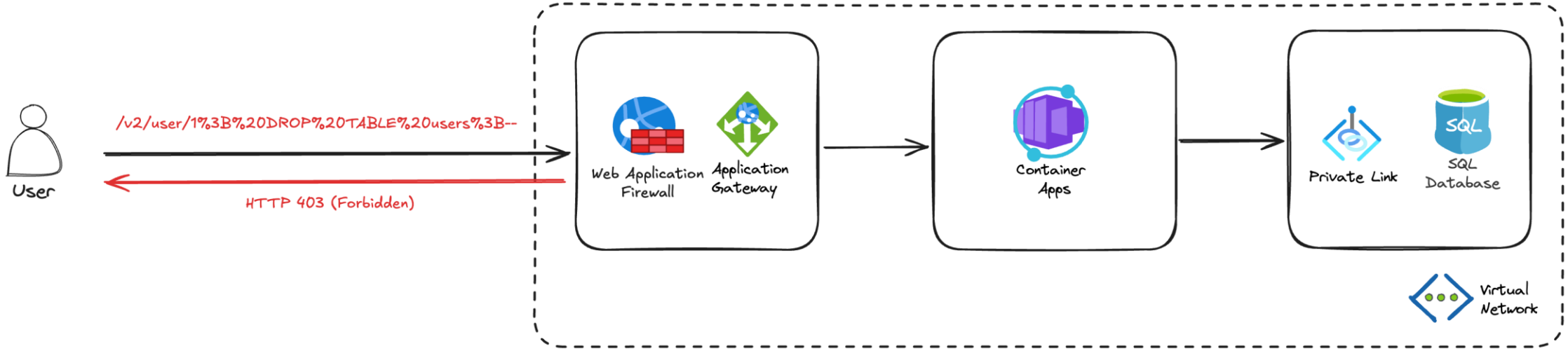
- Entra ID Federated Credential can be used to authenticate with Azure services from third-party
  - Azure DevOps, GitHub Actions, GitLab, and other CI/CD solutions
  - Workload Identity with Azure Kubernetes Service
  - Basically, everything supporting OIDC (includes other cloud provider)



Runtime security

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

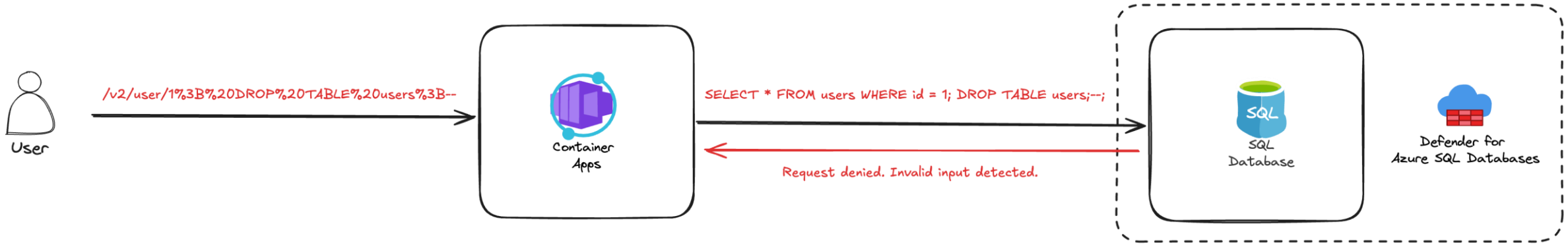
Securely exposing the API



Azure Web Application Firewall (WAF)

- A Web Application Firewall operates on Layer-7 (HTTP) and therefore helps with
  - Threat Detection for web-based attacks such as SQL injection, cross-site scripting (XSS), and other malicious payloads
  - Zero-Day Protection for newly discovered and unpatched vulnerabilities
  - Mitigate Layer-7 DDoS attack & Bot protection
- Managed Rule sets
  - “Core rule set” based on OWASP (Open Web Application Security Project) CRS
  - “Default rule set” based on OWASP and tuned by Microsoft Threat Intelligence team
- Custom rules based on your needs

SQL runtime security

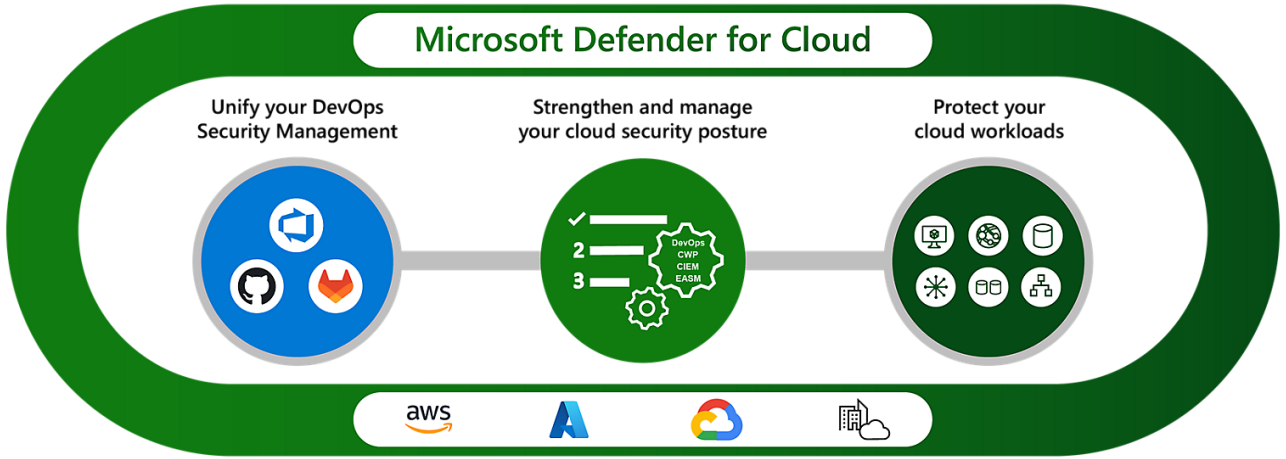


Defender for Azure SQL Databases monitors threats such as:

- Detects vulnerabilities caused by faulty SQL statements (SQL injection)
- Anomalous access patterns: Flags unusual activity like multiple failed sign-ins and brute force attacks

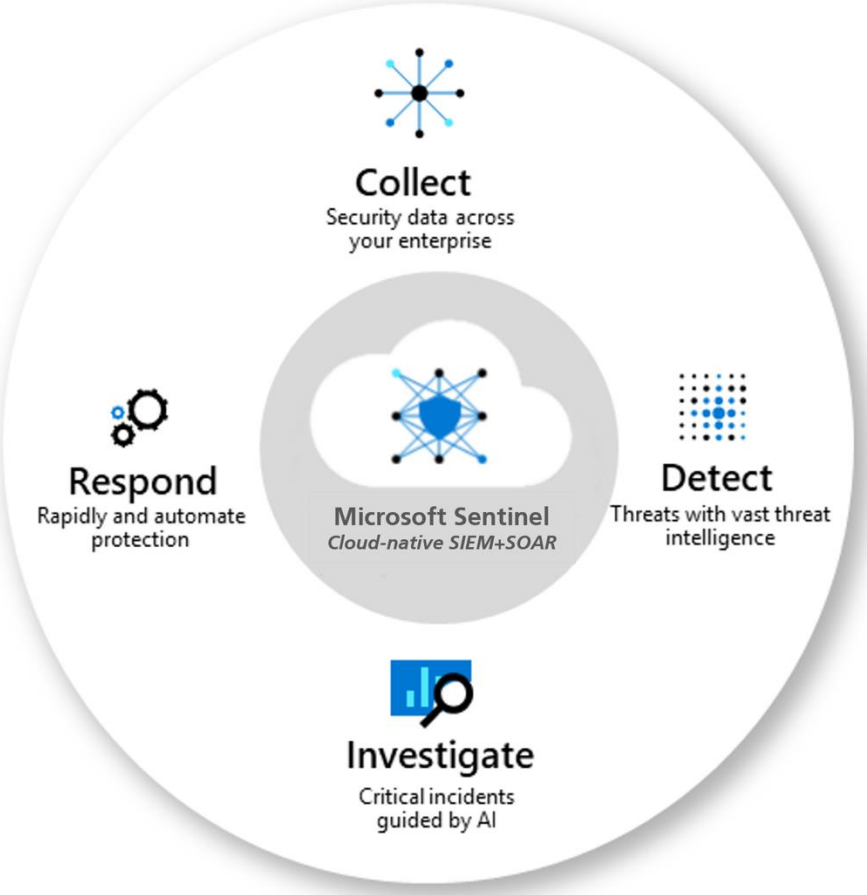
Microsoft Defender for Cloud

- A cloud-native application protection platform (CNAPP) that secures applications from cyber threats. It includes:
  - Unifies security management across code
  - Identifies preventative actions to avoid breaches (Cloud Security Posture Management)
  - Provides protection for Azure IaaS and PaaS (Cloud Workload Protection Platform)
- Provides a holistic view across multiple clouds and environments



Microsoft Sentinel

- Provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise
- Is a cloud-native security information and event management (SIEM) with SOAR (security orchestration, automation, and response) capabilities
- Integrates with the whole Microsoft stack as well as others



How to get started?

- Think big, but start small – then review and iterate
- Enable your team for security awareness
- Abstract security into your CI process and enforce PR reviews
- Implement a zero-trust architecture
- Abstract security into a platform to scale

Unsere Solution Assessments

Ganzheitliche Analyse von Softwarelösungen und Cloud-Plattformen.

Unsere ersten Schritte bei neuen Kunden oder Projekten

- ✓ Einführung/Überblick und Anforderungserfassung
- ✓ Pain-Point-Analyse und Quick-Win-Implementierung
- ✓ Definition Ihrer Roadmap und weitere Zusammenarbeit

Cloud-native Entwicklung mit KI

DevOps & Developer Productivity

Platform Engineering & Kubernetes

Nachhaltige Anwendungsentwicklung

Softwarehersteller & SaaS Anbieter

DevSecOps & Security

Gibt es Fragen?

Nico Meisenzahl

Geschäftsführer | COO

+49 8031 230159-112

nico.meisenzahl@whiteduck.de

@nmeisenzahl

www.linkedin.com/in/nicomeisenzahl

white duck

Vielen Dank!