
AXIANS

axians

Secure Services Edge

van strategie tot succes

GOOD AI

BAD AI

'FraudGPT' Malicious Chatbot Now for Sale on Dark Web

- PoisonGPT
- Chaos GPT
- FreedomGPT
- XXXGPT

$100 for a month access or $5,000 for private setup.

Bad AI in action

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

“(In the) multi-person video conference, it turns out that everyone [he saw] was fake,” senior superintendent Baron Chan Shun-ching told the city’s public broadcaster RTHK.

Forest Blizzard

Forest Blizzard, also known as Fancy Bear, represents one of the most notable examples of AI-generated malware attacks in recent years. This group, linked to Russian state-sponsored hacking activities, has carried out highly targeted phishing campaigns across multiple continents, affecting at least nine countries.

These attacks are characterized by their use of official government-themed lures, which suit Russian geopolitical interests. The group has used advanced AI techniques to create highly convincing phishing emails that impersonate government documents, including both publicly available and internal files.

Once the phishing lures succeed, the attackers deploy custom backdoors like “Masepie” and “Oceanmap.” These tools establish persistence on victim machines, conduct reconnaissance, and exfiltrate sensitive data. Forest Blizzard’s AI capabilities allow them to quickly exploit vulnerabilities, often launching attacks within hours of landing on a victim’s machine.

Hacker Deepfakes Employee's Voice in Phone Call to Breach IT Company

Retool says social engineering, an AI deepfake, and a weakness in Google's Authenticator app helped the hacker breach the company last month.

The breach, which ensnared 27 cloud customers, occurred last month at Retool, a company that helps clients build business software.

The hacker kicked off the intrusion by sending several employees at Retool SMS-based text messages that claimed to come from a member of Retool’s IT team who was reaching out to resolve a payroll issue preventing employees from receiving healthcare coverage. Most Retool employees who received the phishing message refrained from responding, except for one.

The unsuspecting employee clicked a URL in the message, which forwarded them to a fake internet portal to log in. After logging into the portal, which included a multi-factor authentication form, the hacker called the employee while using an AI-powered deepfake.

“The caller claimed to be one of the members of the IT team, and deepfaked our employee’s actual voice,” Retool said in the report. “The voice was familiar with the floor plan of the office, coworkers, and internal processes of the company. Throughout the conversation, the employee grew more and more suspicious, but unfortunately did provide the attacker one additional multi-factor authentication (MFA) code.”

Phishing attacks

Certainly, here's an example of a phishing email:

Subject: Urgent: Verify Your Account Information Now

Dear Valued Customer,

We have detected unusual activity in your account and need to verify your information to ensure the security of your account. To avoid any interruptions to your services, please complete the verification process as soon as possible.

Please follow these steps:

1. **Click the link below** to access the verification page: Verify Your Account
2. **Log in** using your account credentials.
3. **Review and update** your account information as requested.

Failure to complete this process within 24 hours may result in a temporary suspension of your account for security reasons.

We apologize for any inconvenience this may cause and appreciate your prompt attention to this matter.

If you have any questions, please contact our support team by replying to this email.

Thank you for your cooperation.

Old-Fashioned Phishing

- Sloppy grammar, spelling, and layout
- Suspicious addresses
- Generic greetings and addresses
- Suspicious attachments
- Spoofed links
- Requests for personal information

AI en Cybersecurity

De invloed van AI op het Cyber landschap

- **Adapting and customizing in real time**
  - LLM's worden gebruikt om source code aan te passen zodat bijv Yara rules niet geraakt worden
- **Automating attacks**
  - Ook aanvallers proberen zo efficient mogelijk te werken. AI helpt in deze automatisering
- **Precision-targeting weaknesses**
  - AI wordt gebruikt voor verkenning en vulnerability assesment
- **Well-informed follow-on attacks**
  - Multimodal language models (MMLMs) parse videos en photos van gebouwen, apparatuur, en andere publiekelijke informatie


En toch willen we al onze belangrijke data in de cloud zetten

Game Over

Secure Access Service Edge

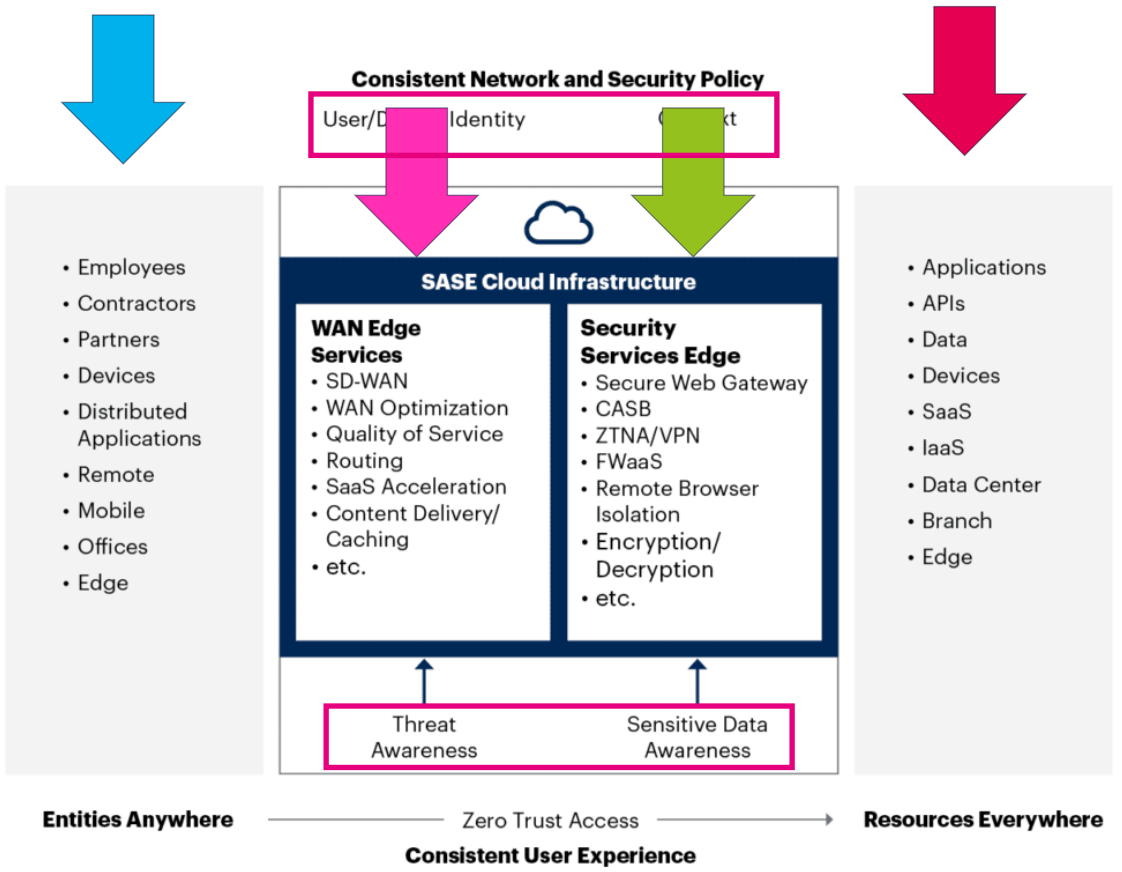
"Een cloud based architectuur waarbij netwerk en security samenkomen"

SASE

- Netwerk en Security samen
- Optie voor netwerk vervanging

SSE

- Security services
- Security transformatie los van het netwerk
- Hoeft niet dezelfde vendor te zijn
- Investering bescherming



Source: Gartner
741491_C

Gartner

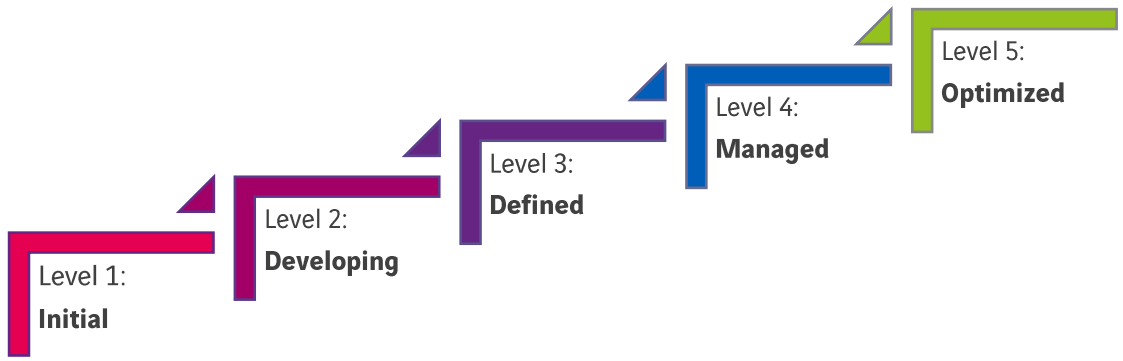
Phase 1- Assessment

Van A naar Beter

- Wat is het doel ? Waarom SSE ?
  - Thuiswerkers, compliancy, security, kosten ?
- Waar staat de data die we moeten beschermen ?
  - Welke controls hebben we al ?
- Waar staan we in een cloud transformatie ?
- Vaststelling van roadmap

Security Maturity Review

- Waar staat uw organisatie NU? (IST)
- Waar willen we heen? (SOLL)
- Roadmap (GAP)



CIS Controls

NIST National Institute of Standards and Technology

Typical (Cloud) Secure Web Gateway

User, Group, OU	Device	URL Category	Activity	Threat	Data	Policy Action
Pat Smith Accounting	Managed	File Sharing or IaaS	Limited to View, Upload	Threat Intel AV Analysis Sandbox	ICAP to DLP	Allow or Block

Rich Policy Context – integrated SSE (CASB + SWG + DLP)

User, Group, OU	Device	SaaS App	App Instance	App Risk Rating	URL Category	Activity Controls	User Risk Rating	Threat	Data	Contextual Policy Action
Pat Smith Accounting Logged in as Psmith @GMAIL.com	Managed Personal	Cloud Storage App Managed Unmanaged	Company Personal	97 Across breadth of 40K Apps Risk Security Privacy Legal Etc.	Cloud Storage 130+ Categories	Depth of controls (dozens) Upload Share Create Edit Post	User Behavior UEBA	Threat Intel AV Analysis Sandbox UEBA	DLP Profiles And Rules	Contextual Allow Block Coach Encrypt Legal Hold Quarantine etc.

Phase 2- Visibility

Wat je niet ziet, kun je niet beveiligen

Applications
79 FOUND

Sort by: **Bytes Uploaded** TAG AS...

APPLICATION	CATEGORY	SANCTIONED	CCI	# USERS	# SESS
Taboola	Marketing	No	61	6	6
Optimizely	Development Tools	No	78	9	9
Salesforce.com	Customer Relationship Mana...	No	89	1	1
WeTransfer	Cloud Storage	No	47	10	10
Microsoft OneDrive	Cloud Storage	No	92	10	10
Amazon IAM	Identity and Access Manage...	No	91	3	3
Amazon S3	Cloud Storage	No	88	4	4
Twitter	Social	No	59	7	7
Microsoft Office 365 Outlook.com	Webmail	No	88	3	3
GlobalSign	Security	No	64	5	5

CCI >
Compare

WeTransfer		Microsoft Office 365 OneDr...	
65		86	
ENTERPRISE	UNSANCTIONED	ENTERPRISE	UNSANCTIONED
USERS	0	USERS	1
# SESSIONS	0	# SESSIONS	4
BYTES DOWNLOADED	0	BYTES DOWNLOADED	83.89M
BYTES UPLOADED	0	BYTES UPLOADED	20.27M

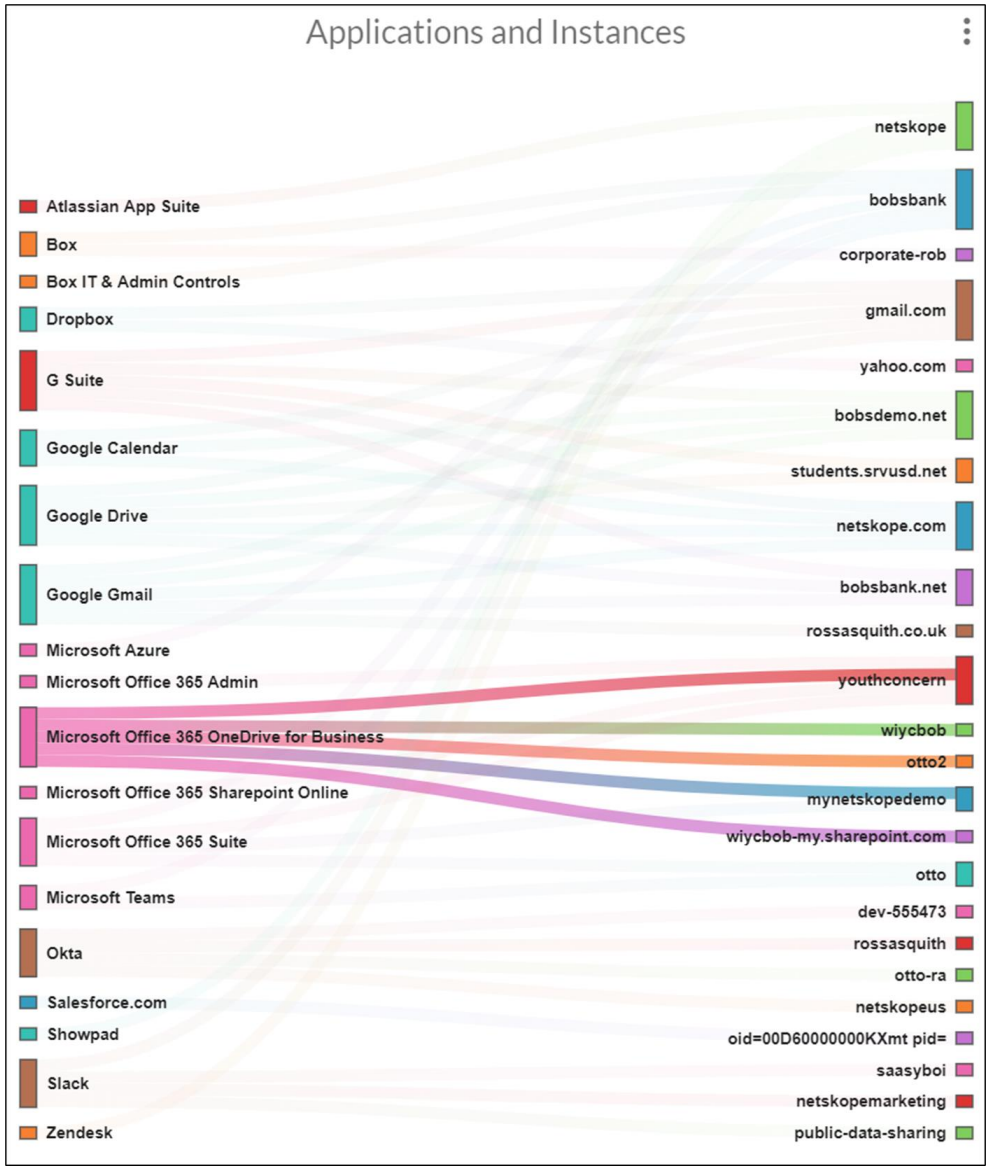
Show All

WETRANSFER	MICROSOFT OFFICE 365 ONEDRIVE FOR BUSINESS
Certifications and Standards	**Certifications and Standards**
What compliance certifications does the app have? • PCIDSS	What compliance certifications does the app have? • FedRAMP • FISMA • HIPAA • HITRUST • NIST / SP800-53 • PCIDSS • Data Privacy Framework
To what data center standards does the app adhere? • ISO27001	To what data center standards does the app adhere? • SOC-1 • SOC-2 • SOC-3 • SAS70/SSAE 16/SSAE 18 • ISO27001 • ISO/IEC 27018 • Cyber Essentials/ Cyber Essentials Plus (UK) • C5 (Germany)
Data Protection	**Data Protection**
Does the app allow customer-managed encryption keys? • No published support	Does the app allow customer-managed encryption keys? • Yes
Does the app enable file sharing? • Yes	Does the app enable file sharing? • Yes
File Sharing Capacity • Greater than 10GB	File Sharing Capacity • Greater than 10GB
Does the app allow anonymous sharing of data?	Does the app allow anonymous sharing of data?

Phase 2- Visibility

Wat je niet ziet, kun je niet beveiligen

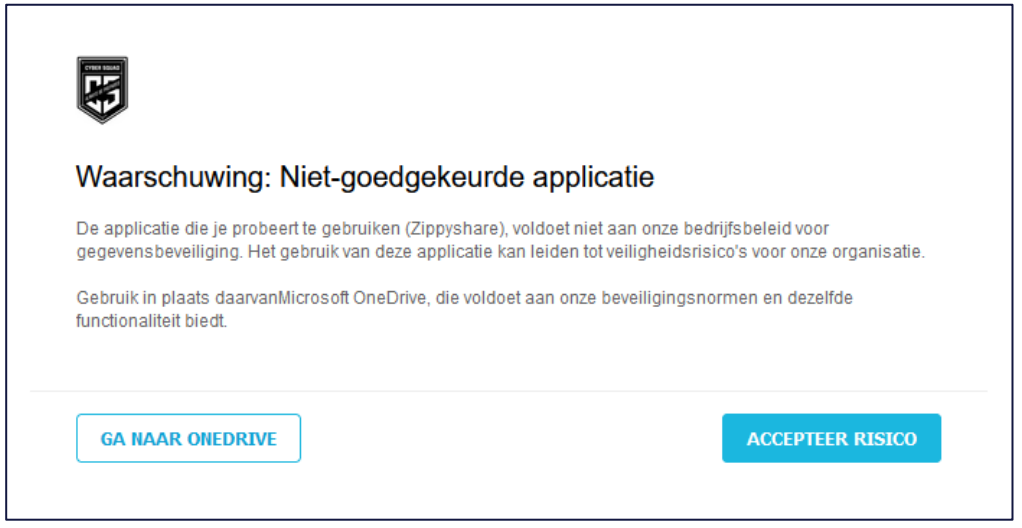
- Welke tenant wordt gebruikt van office ?

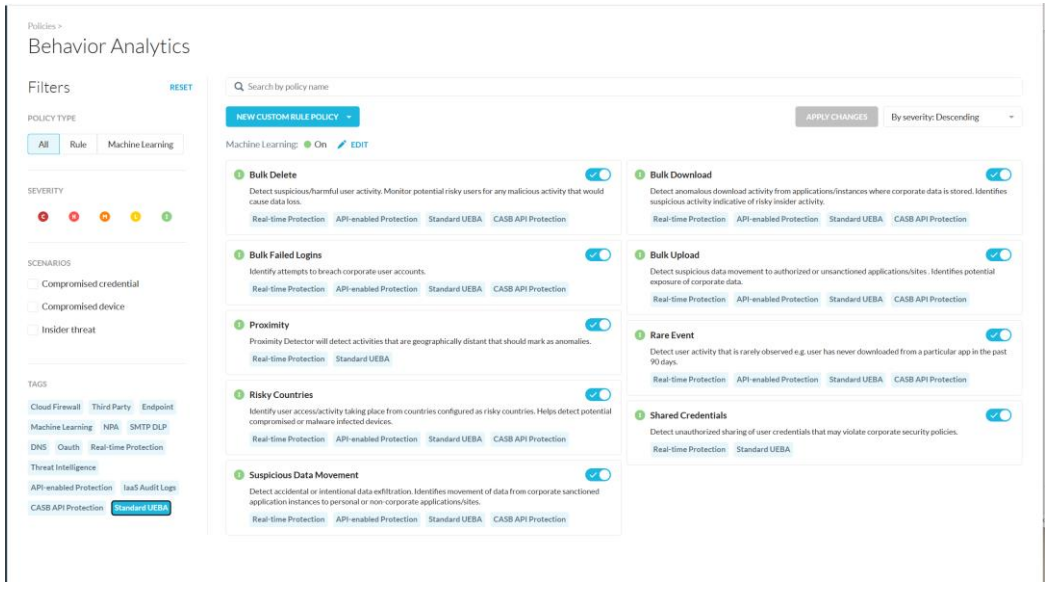


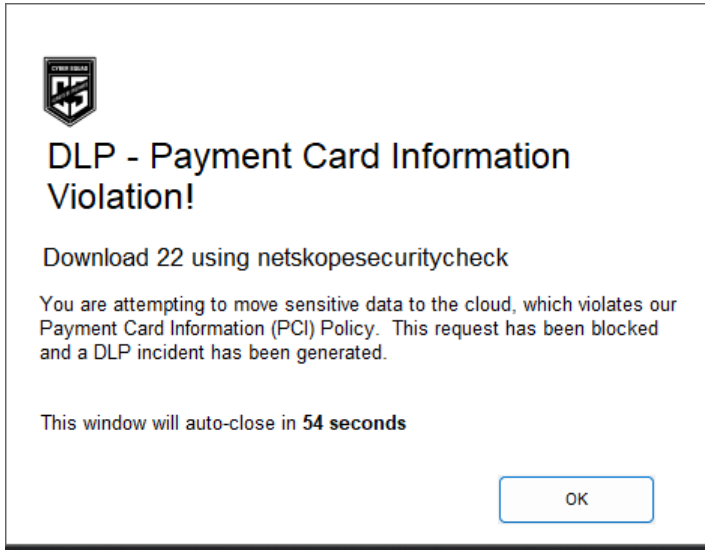
Phase 3- Control

User awareness

- Definitie van policy
  - Saas applicatie / instance basis / Activiteiten
  - DLP definitie (coaching)
  - Sturing van mensen, coaching
- Gedrag analyse



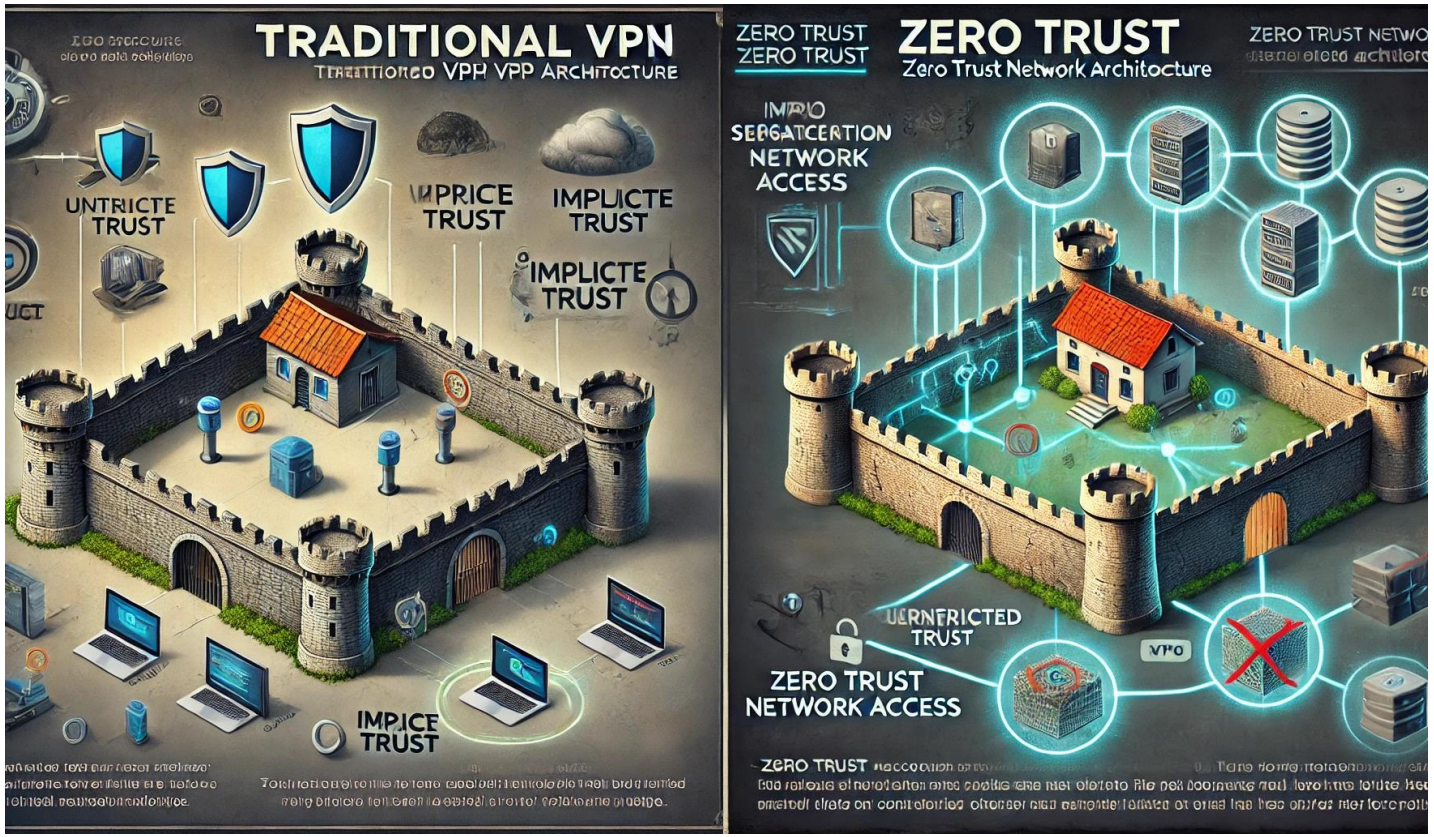




Phase 4 is zero trust

“Vertrouwen is goed, controleren is beter”

- VPN vs Zero trust
  - Concentrator vs Publisher
- Trust
  - Posture
  - Authenticatie
- Applicatie toegang
  - Step up authenticatie



Phase 5 is Consolidatie

Consolidatie van security services

- Focus van on-prem definitief naar cloud
- On premise firewall -> Cloud firewall
  - AWS Direct connect
  - Azure Express route

Take aways

Ervaringen uit de praktijk

- Vergeet SaaS en Cloud Security niet
  - SaaS Security Posture Management (SSPM) en Cloud Security Posture Management (CSPM)
  - SSE focust op wat jouw gebruikers doen… niet op wat externen met malicious intend nu doen richting de SaaS/Cloud omgevingen
- Single-Vendor SASE is een optie, een keuze nu kan voor issues/kosten zorgen wanneer de eisen veranderen in de toekomst.
- Netwerk, Security en Endpoint **visie** moet afgestemd zijn.
- Begeleid gebruikers
  - Verandering van gedrag kost tijd
  - Acceptatie kost tijd

axians

Henri van den Heuvel

Security Solution Architect

https://www.axians.nl/expertises/cyber-security/cyber-squad/