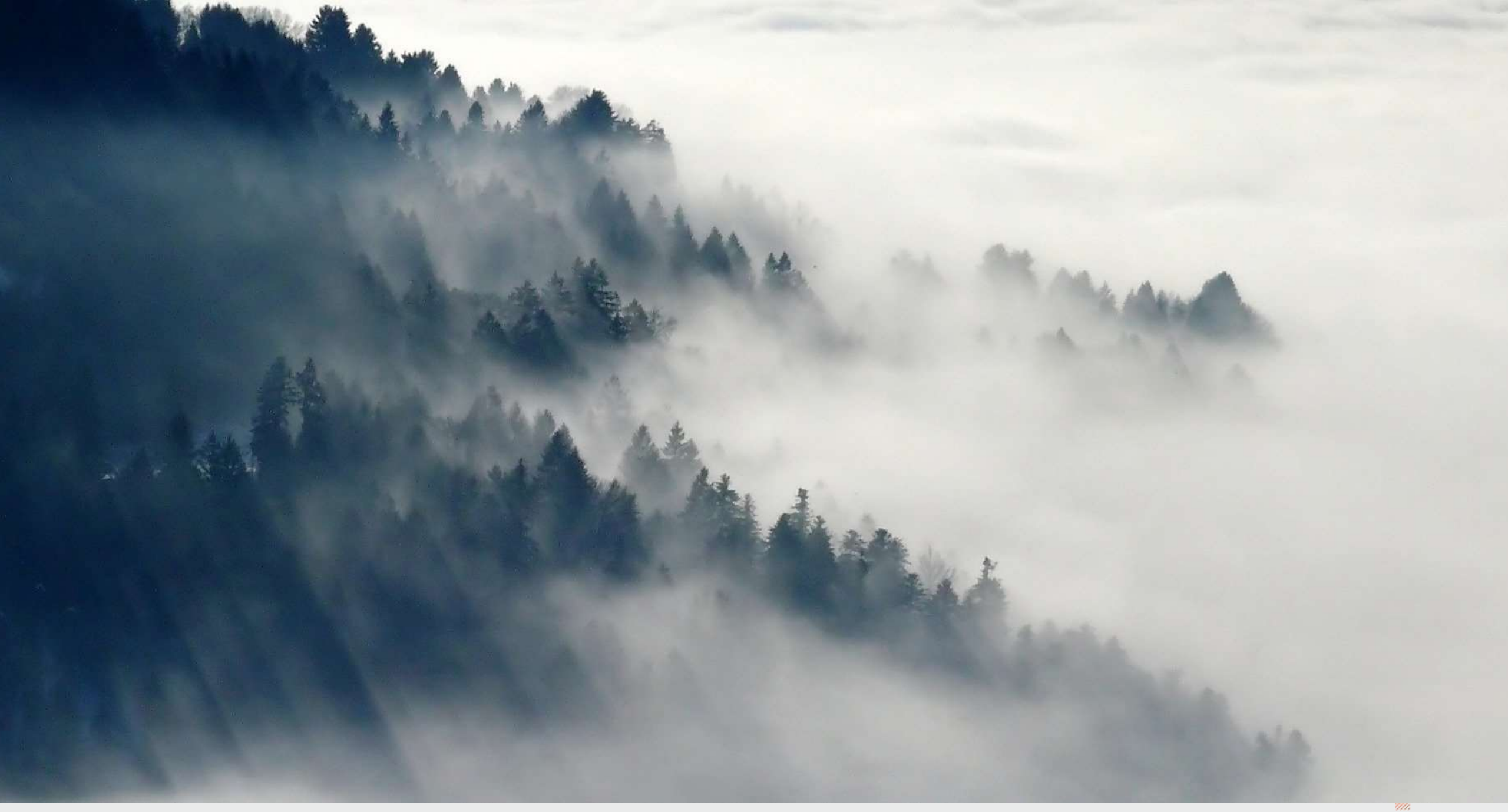
illumio

Warum sich Angreifer in Ihrem Netz so wohl fühlen

Warum Ransomware uns auch in der Zukunft beschäftigen wird

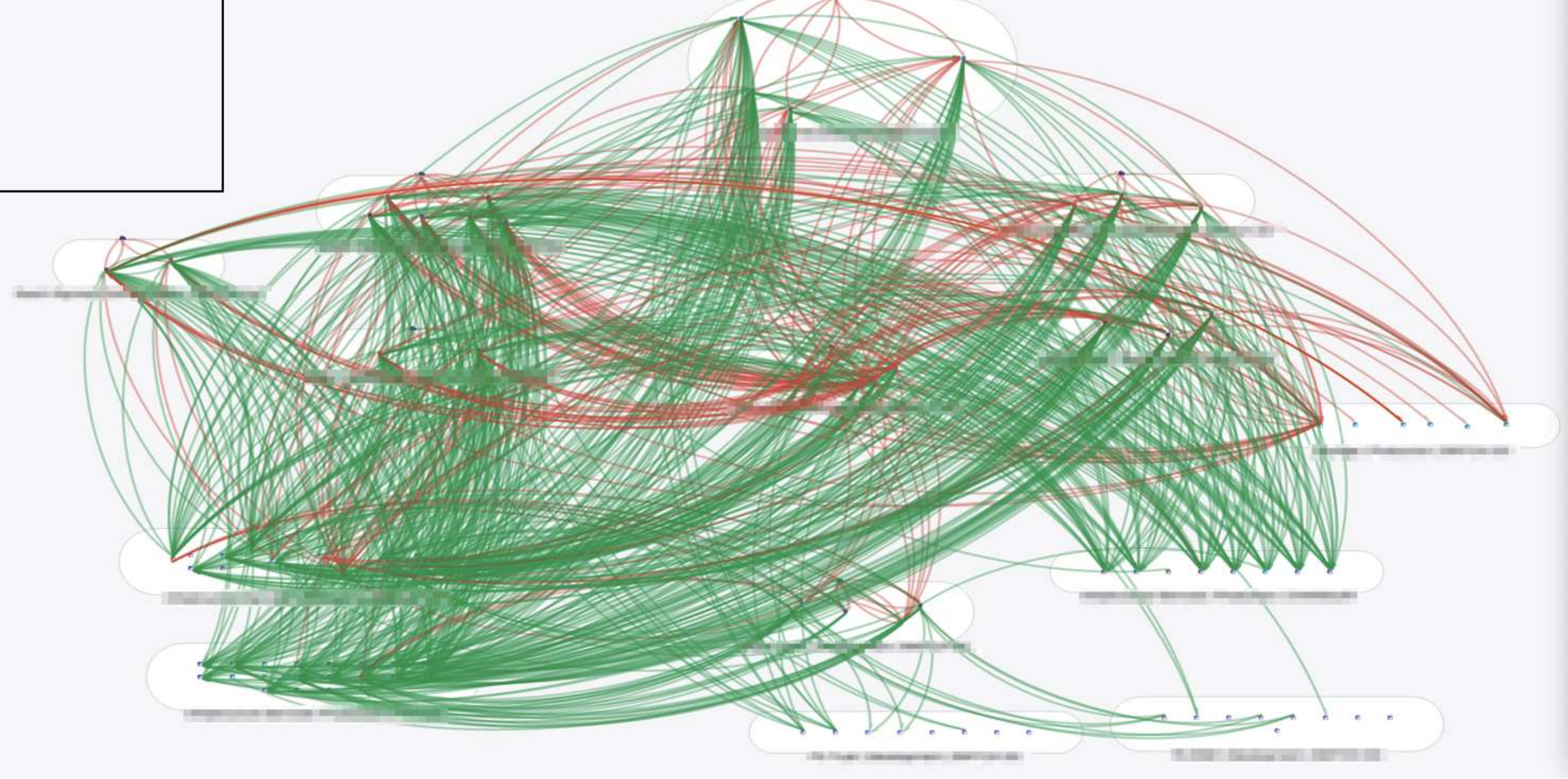
Alexander Goller
Senior Systems Engineer, Illumio

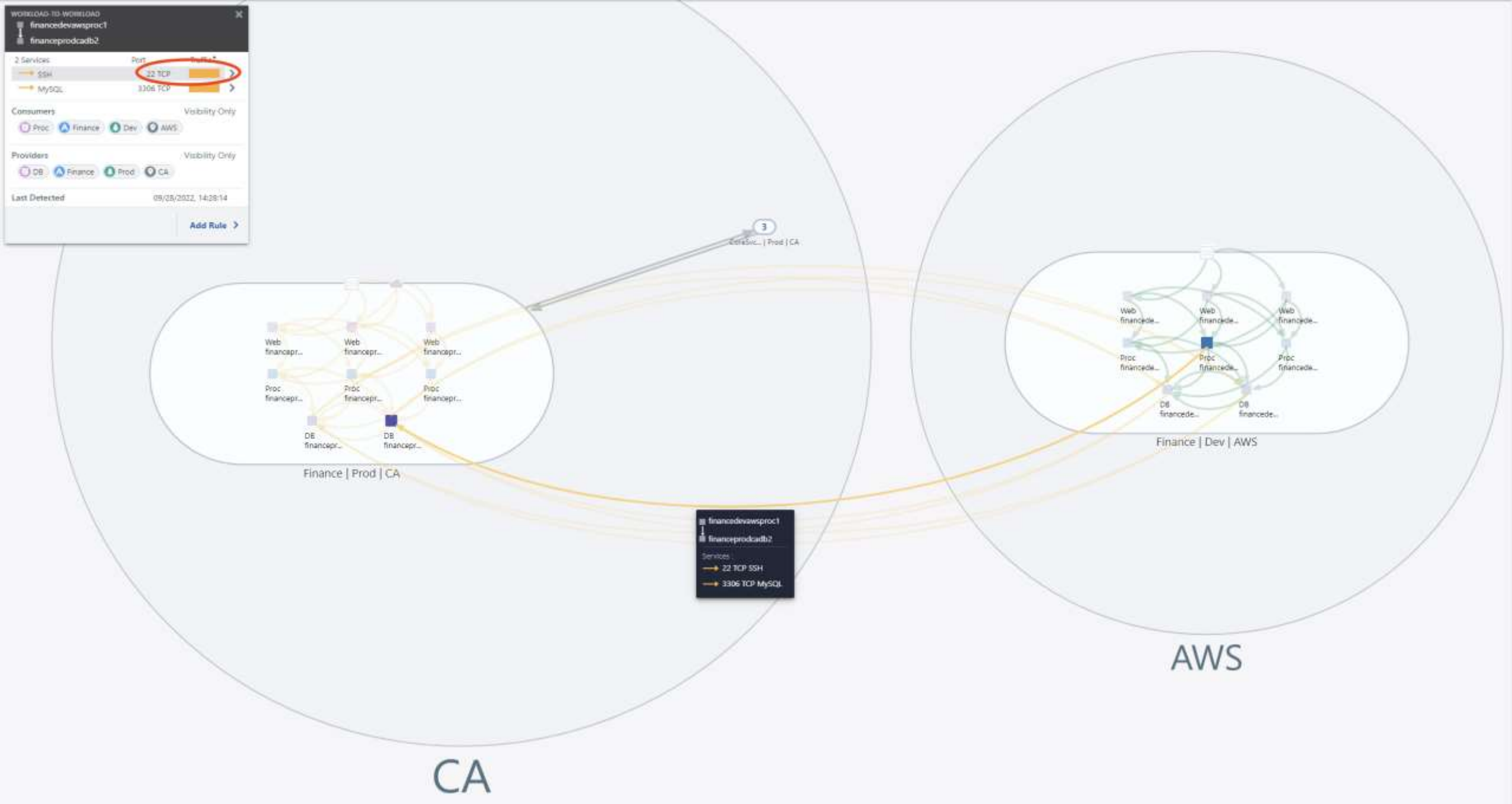
Oktober 2022



Ihr Netz ist eine Black-Box

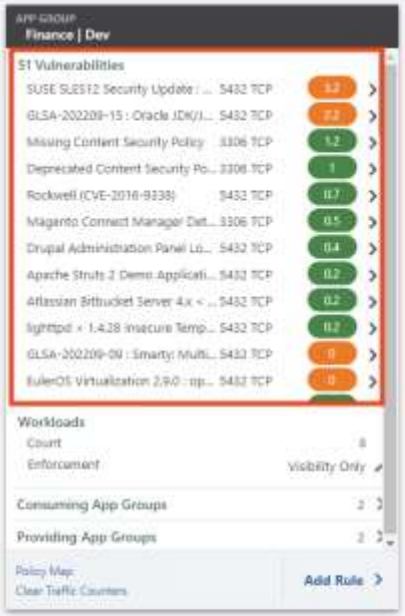
illumio

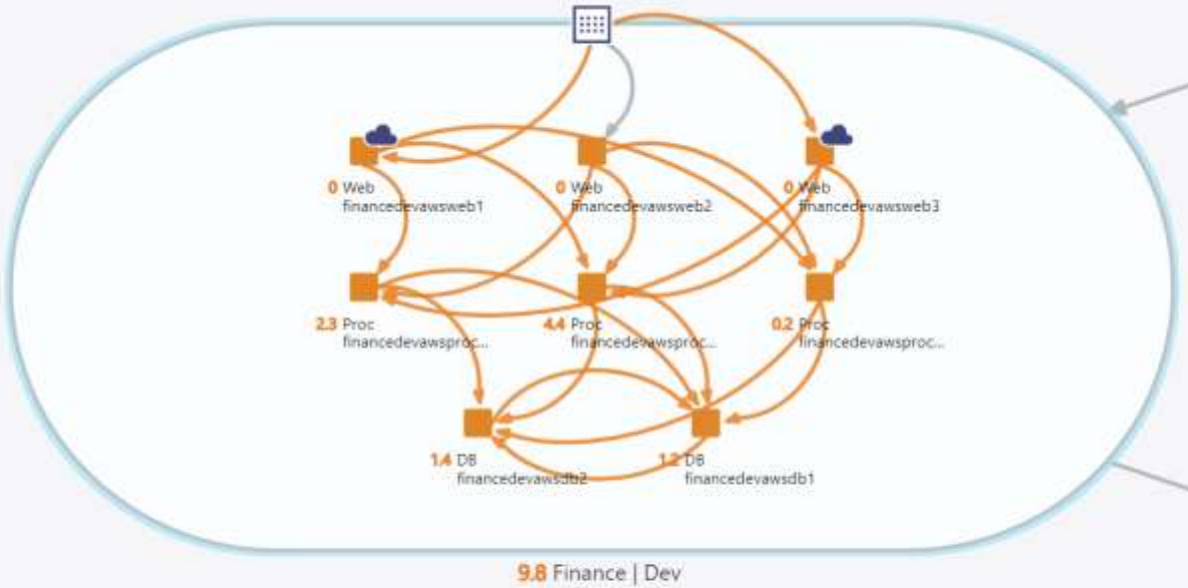



financedevawsproc1
financeprodcadb2
2 Services
Port
SSH
22 TCP
MySQL
3306 TCP
Consumers
Visibility Only
Proc
Finance
Dev
AWS
Providers
Visibility Only
DB
Finance
Prod
CA
Last Detected
09/28/2022, 14:28:14
Add Rule
3
Web
Proc
DB
Finance | Prod | CA
Finance | Dev | AWS
financedevawsproc1
financeprodcadb2
Services
22 TCP SSH
3306 TCP MySQL
CA
AWS

Risiko ist weder sichtbar noch greifbar

illumio


APP GROUP
Finance | Dev
51 Vulnerabilities
Workloads
Count
Enforcement
Visibility Only
Consuming App Groups
Providing App Groups
Policy Map
Clear Traffic Counters
Add Rule


0 Web
financedevawsweb1
0 Web
financedevawsweb2
0 Web
financedevawsweb3
2.3 Proc
financedevawsproc...
4.4 Proc
financedevawsproc...
0.2 Proc
financedevawsproc...
1.4 DB
financedevawsdb2
1.2 DB
financedevawsdb1
9.8 Finance | Dev


2
Consuming
App Groups
View


2
Providing
App Groups
View

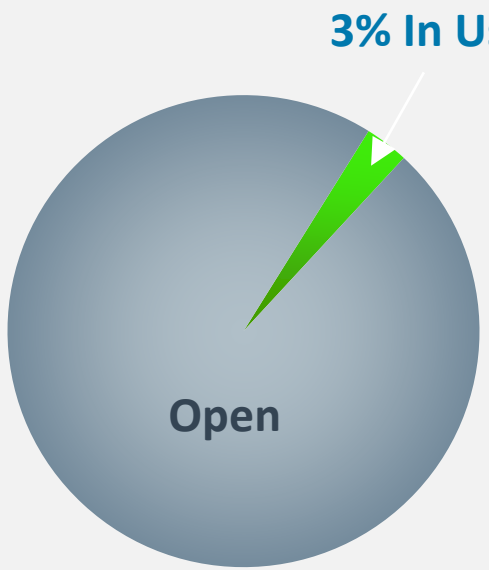
illumio

Netzwerke sind massiv über-konnektiert

107 Workloads

244,050 Potential connections

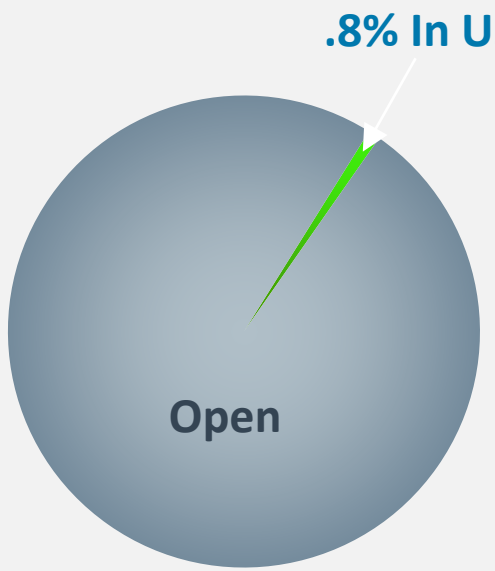
6,663 Connections in use



3,500 Workloads

37,012,842 Potential connections

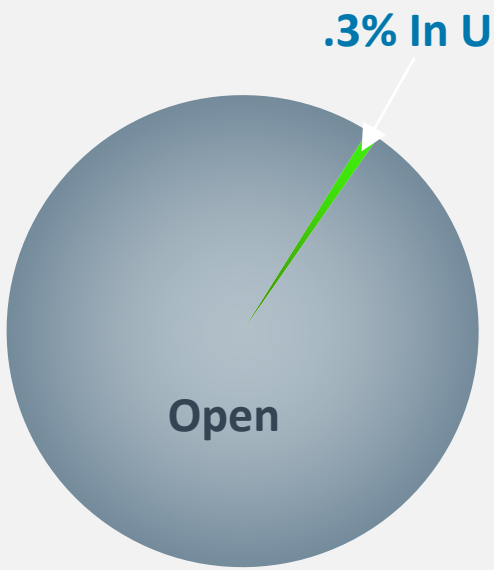
342,549 Connections in use



11,554 Workloads

273,395,075 Potential connections

820,185 Connections in use



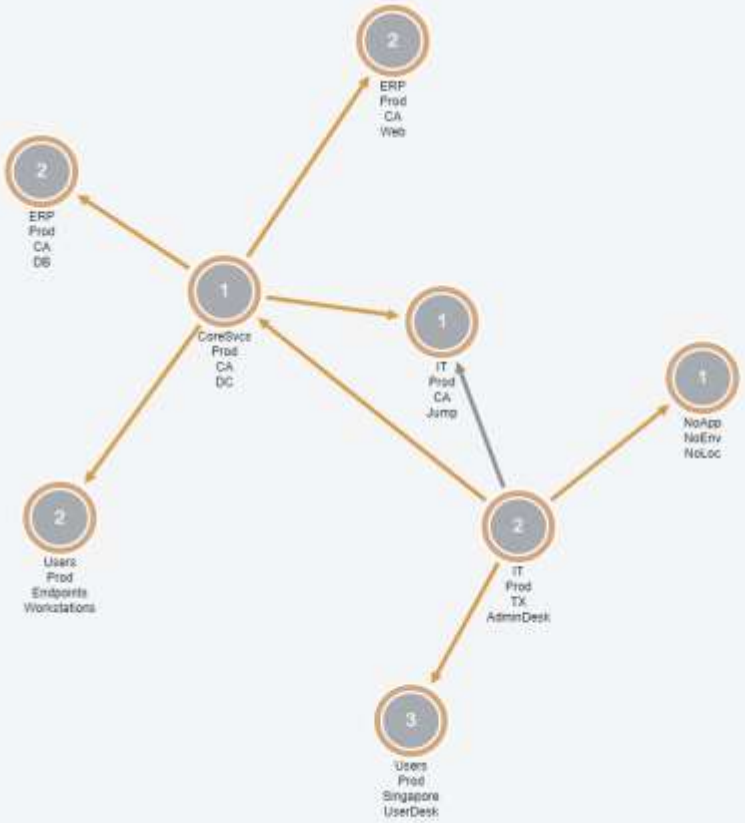
Administrativer Zugang ist von überall erlaubt

Diagnosing the Ransomware Deployment Protocol (RDP)

Remote Desktop Protocol (RDP) is the most popular initial ransomware attack vector and has been for years. For the 2020 Unit 42 Incident Response and Data Breach Report, Unit 42 studied data from over 1,000 incidents and found in 50% of ransomware deployment cases, RDP was the initial attack vector. In the 2021 Cortex Xpanse Attack Surface Threat Report, Cortex Xpanse researchers found that RDP accounted for 30% of total exposures, which more than doubles the next most common exposure.

RDP is a protocol on Microsoft Windows systems that is designed to allow users to remotely connect to and control a remote system. The most common legitimate use is to allow IT support to remotely control a user's system to fix an issue. More recently, RDP has become popular for cloud computing to access virtual machines (VMs) in cloud environments or to remotely manage cloud assets.

It is extremely easy to expose RDP unintentionally by leaving RDP exposed on a forgotten system, cloud instance, device previously protected by network segmentation or by directly connecting to the internet. What's worse is that RDP has become more widespread, more exposed and a more prevalent risk that can lead to attacks – specifically ransomware deployment – loss of data, expensive downtime and remediation efforts, as well as brand damage for organizations.



Summary | Connections

Export

NEW Customize columns | 50 per page | 1 – 4 of 4 Total

Reported Policy Decision	Consumer	Provider Port Process
Potentially Blocked	CoreSvcs Prod CA DC	ERP Prod CA Web 3389 UDP svchost.exe
Potentially Blocked	CoreSvcs Prod CA DC	ERP Prod CA Web 3389 TCP svchost.exe TermService
Potentially Blocked	CoreSvcs Prod CA DC	ERP Prod CA DB 3389 UDP svchost.exe
Potentially Blocked	CoreSvcs Prod CA DC	ERP Prod CA DB 3389 TCP svchost.exe TermService


Kritische Applikationen
sind unzureichend vom
Netz getrennt

Map | Members | Rules | Policy Generator | Vulnerabilities | Explorer

Choose an App Group | Policy Data | Draft View | Filter | Legend

APP GROUP-TO-APP GROUP

Finance | Dev

Finance | Prod

3 Roles

DB	2
Proc	3
Web	3

Workloads

Count	8
Enforcement	Visibility Only

Consuming App Groups 1

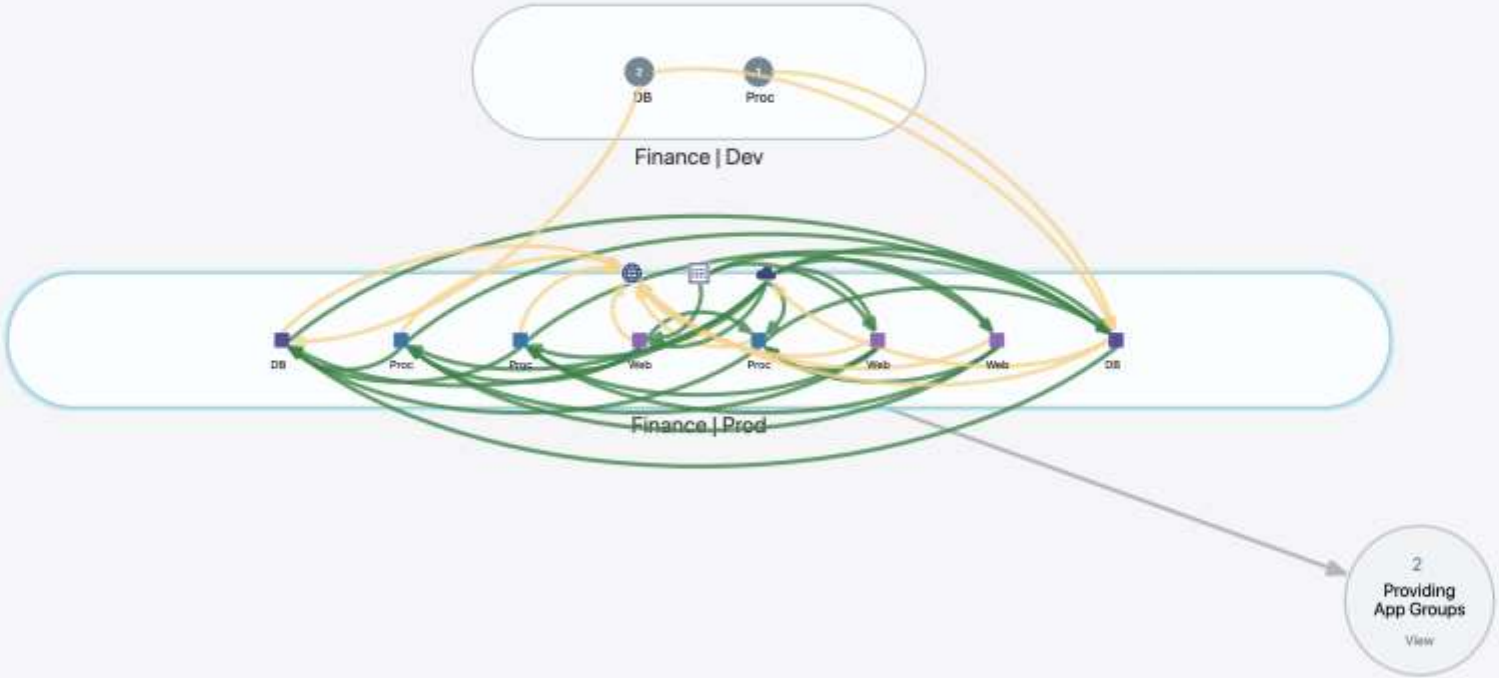
Providing App Groups 2

Vulnerability Map

Collapse Group Roles

More

View Rule



illumio


POLICE

Vorfälle werden gar nicht erst erkannt

Illumio –Stand 7/212 gleich neben dem Forum

Illumio Beer Tasting IT-SA 2022

Ab 17 Uhr 7a/212