
EXPERT TALK
REMOTE SECURITY SOLUTION

REMOTE SECURITY SOLUTION

17.03.2021 | WebEx

COLLABORATION Tools
Home / Office

Calling

Messaging

Meetings

Seamless experiences across app and all your devices

Cisco Webex

HOME OFFICE EQUIPMENT

DESKPHONE

SOFTPHONE

+

HEADSET
STEREO / MONO

+

optional

VIDEOKONFERENZ

WEBEX DESK PORTFOLIO

DESK Camera

DESK *

DESK Limited Edition

DESK PRO

WEBEX DESK KAMERA

- Plug & Play Device. Connection via USB-C or USB-A
- Up to 4K streaming possible
- Integrated AI in the camera
- 2 Omni-directional microphones
- Face detection for perfect perpective
- 10x digital zoom
- Central administration via Webex Control Hub

VERGLEICH

DESK PRO

- 27 Zoll LCD
- **4k** Display
- USB-C & HDMI Anschluss
- Virtuelle Hintergründe
- Gesichts- und Geräuscherkennung
- Whiteboarding

DESK LIMITED EDITION

- 27 Zoll LCD Display
- **1080p** Display
- USB-C & HDMI Anschluss
- Virtuelle Hintergründe
- Gesichts- und Geräuscherkennung
- Whiteboarding
- *kein Laptop charging(USB-C)*
- *kein Directional Audio*
- *kein Stylus Stift*

NTS

HOME OFFICE EQUIPMENT

DESKPHONE

+

HEADSET
STEREO / MONO

+

optional

VIDEOKONFERENZ

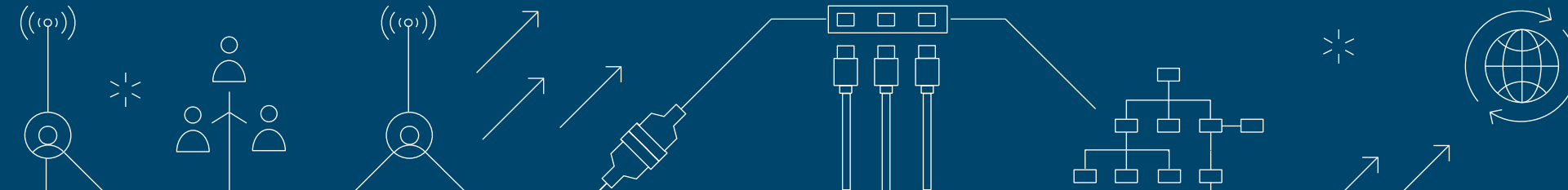
SOFTPHONE

ZU MEINER PERSON

MARTIN STEIBL
Senior Systems Engineer
CCNP R/S, Sec
seit 8 Jahren bei NTS Innsbruck

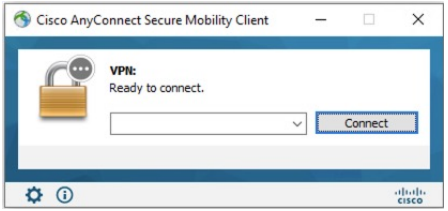
NTS

ANYCONNECT



SOFTWARE

ANYCONNECT



iOS 

VPN SERVER HARDWARE

FPR9300

FPR4100

FPR2100

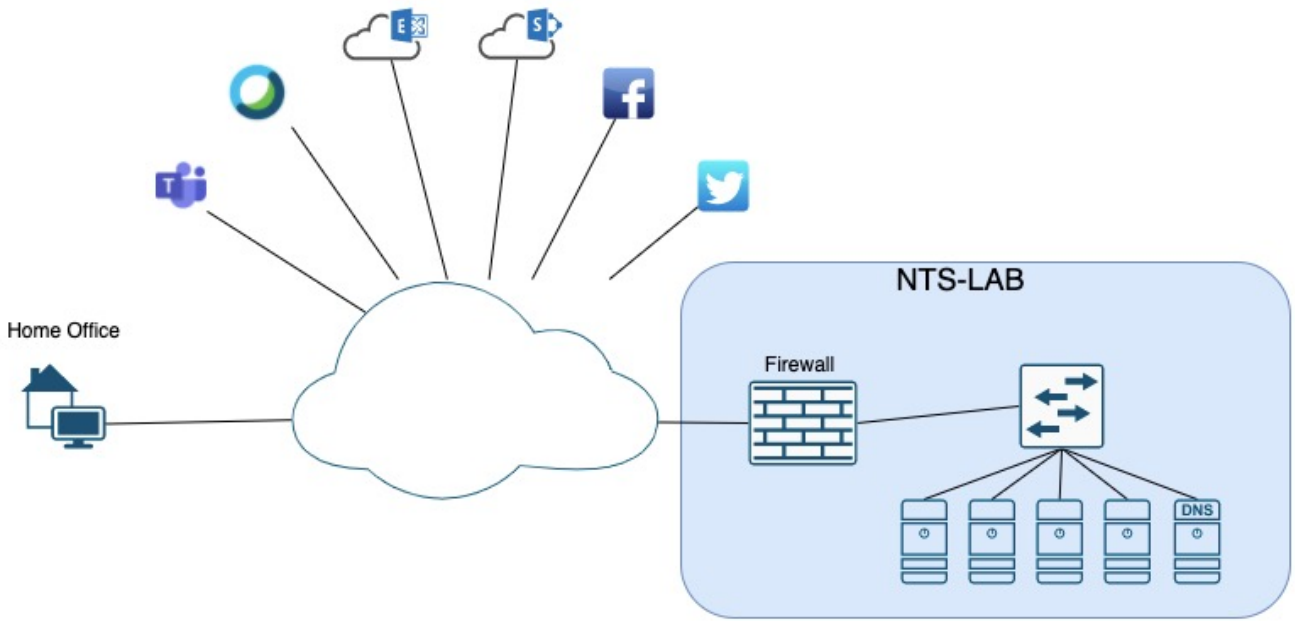
FPR1100

VPN SERVER

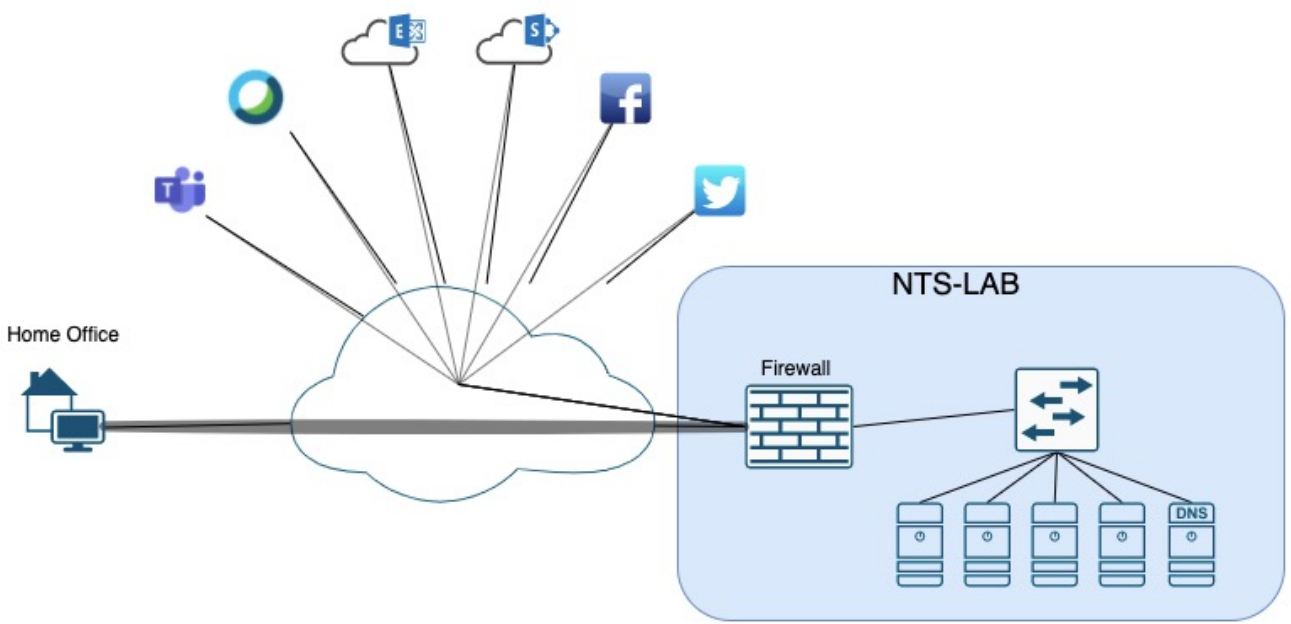
ON PREM

PUBLIC CLOUD

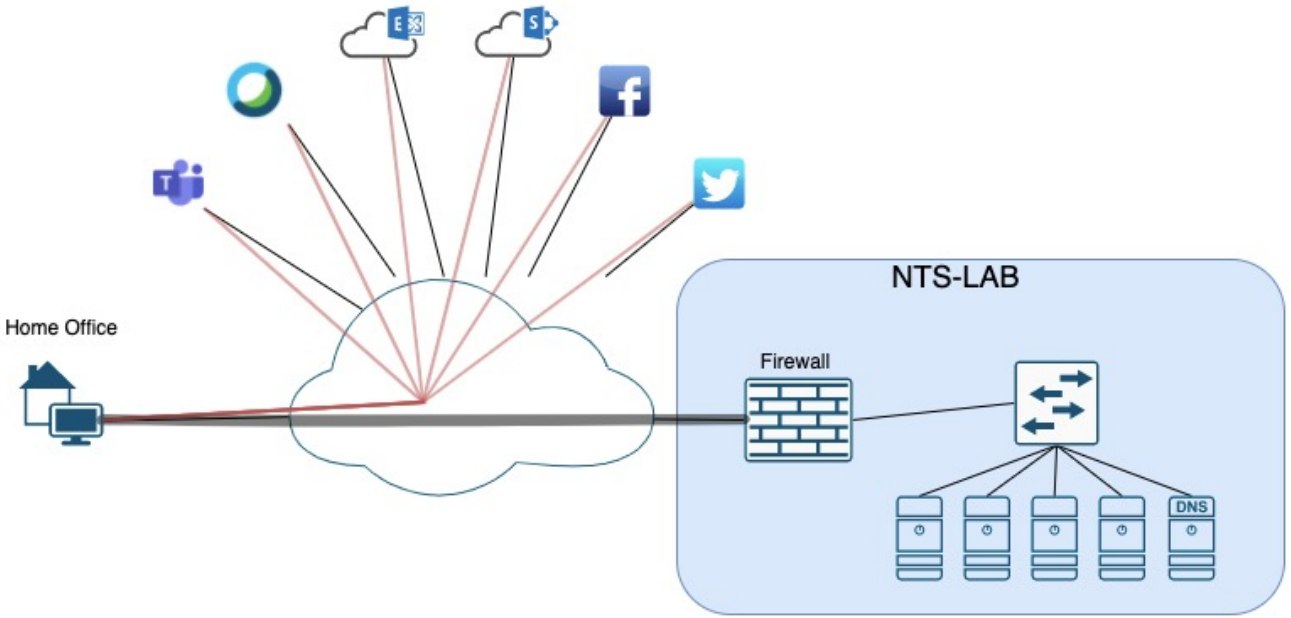
SETUP



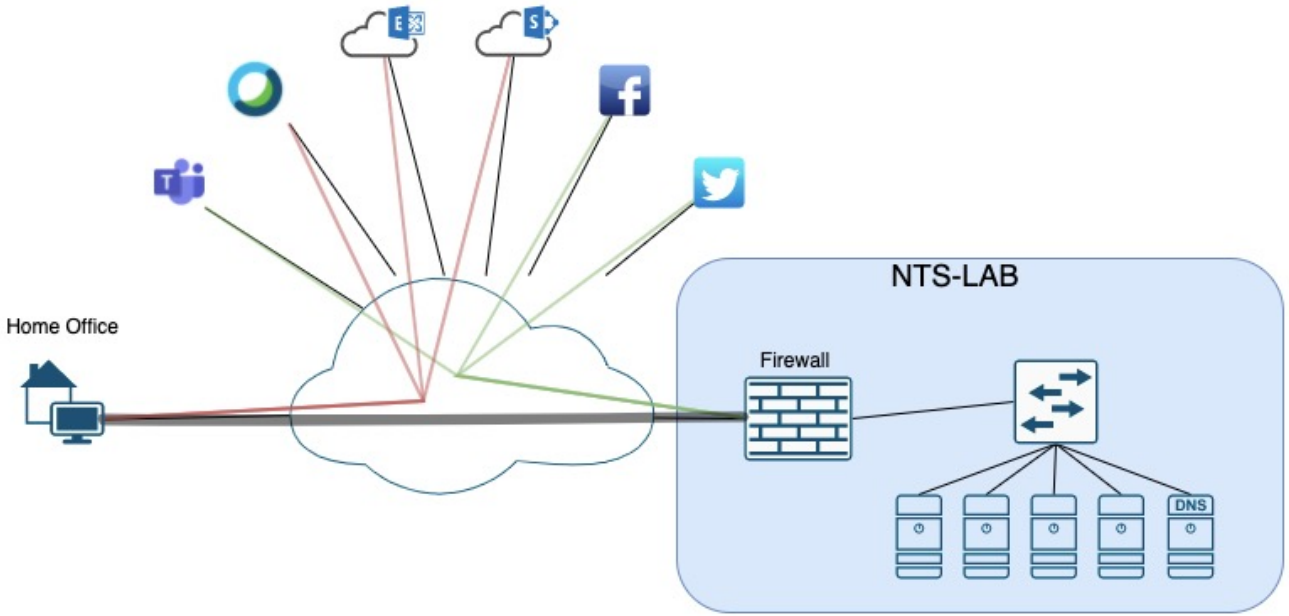
FULL TUNNEL



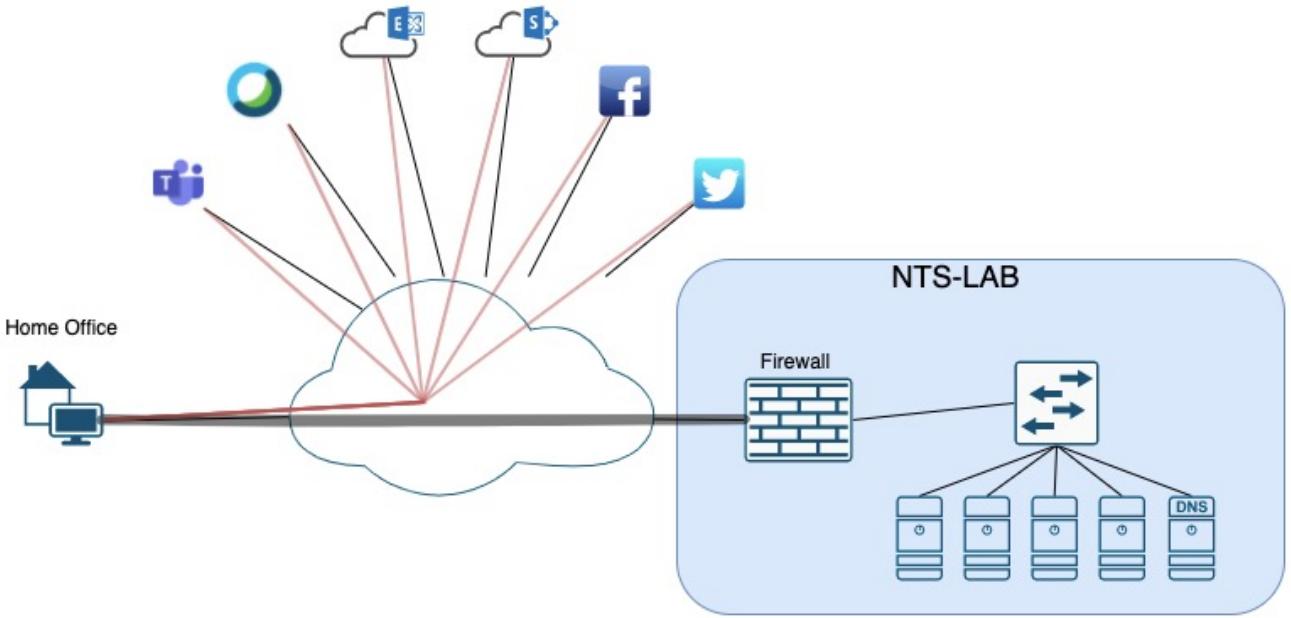
SPLIT TUNNEL



DYNAMIC SPLIT TUNNEL

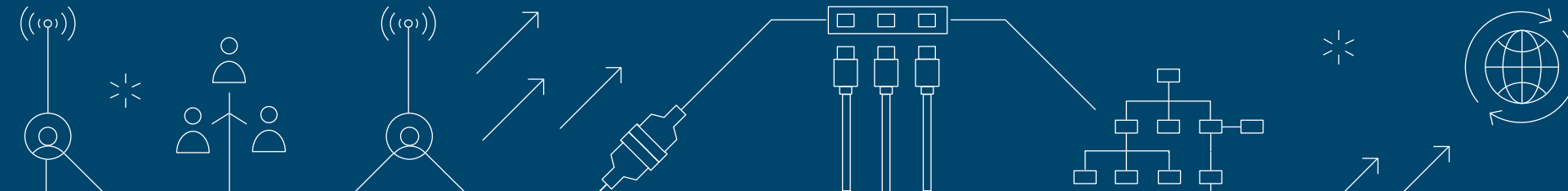


MANAGEMENT TUNNEL

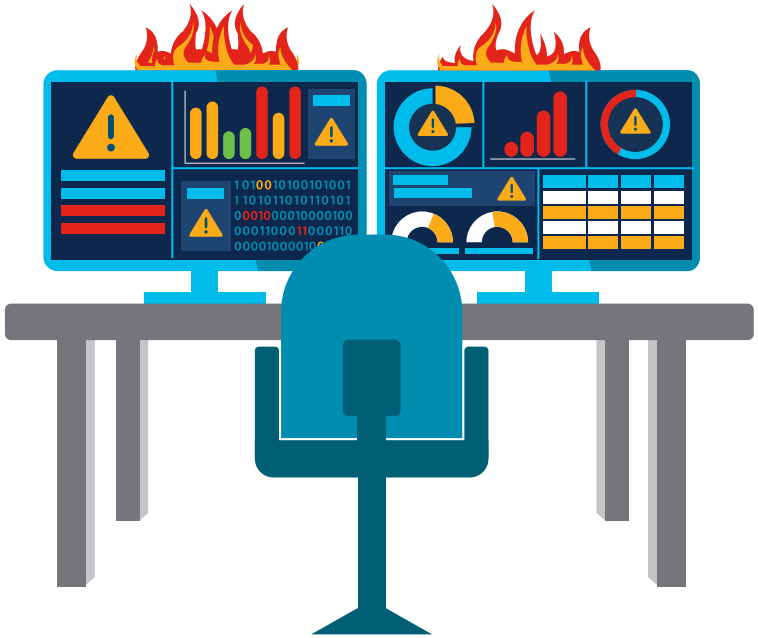


NTS

DEMO

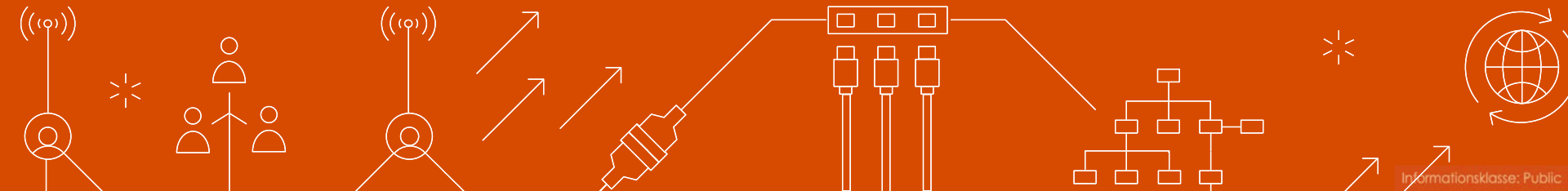


AKTUELLE SITUATION



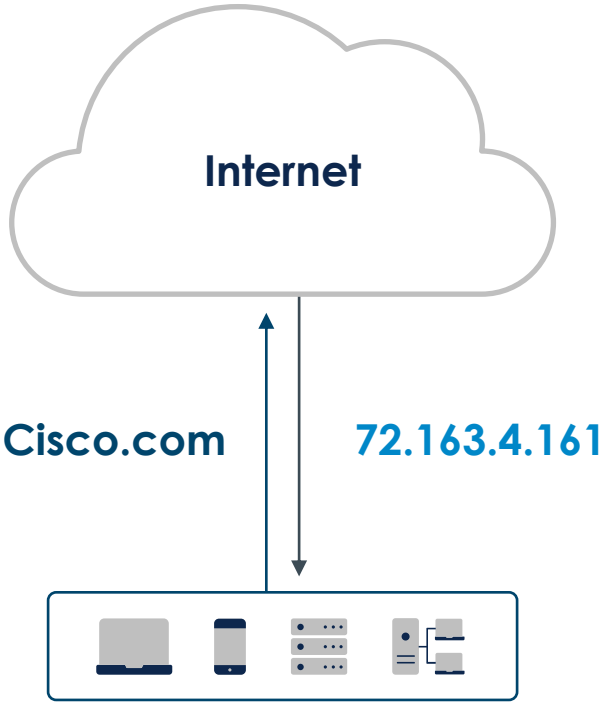
NTS

UMBRELLA



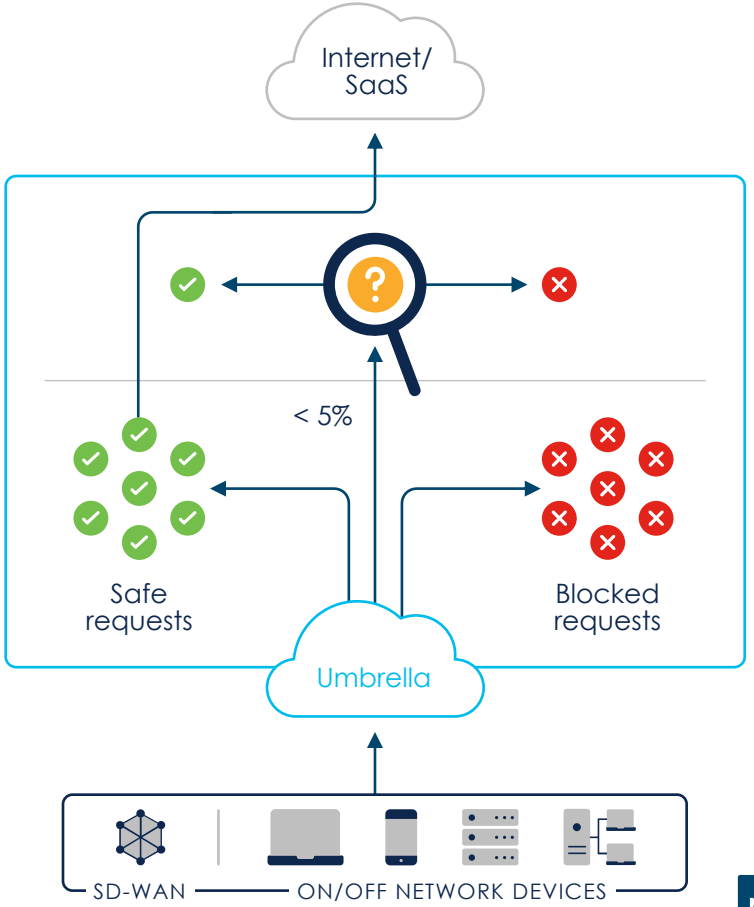
WHY IS DNS USEFUL FOR SECURITY?

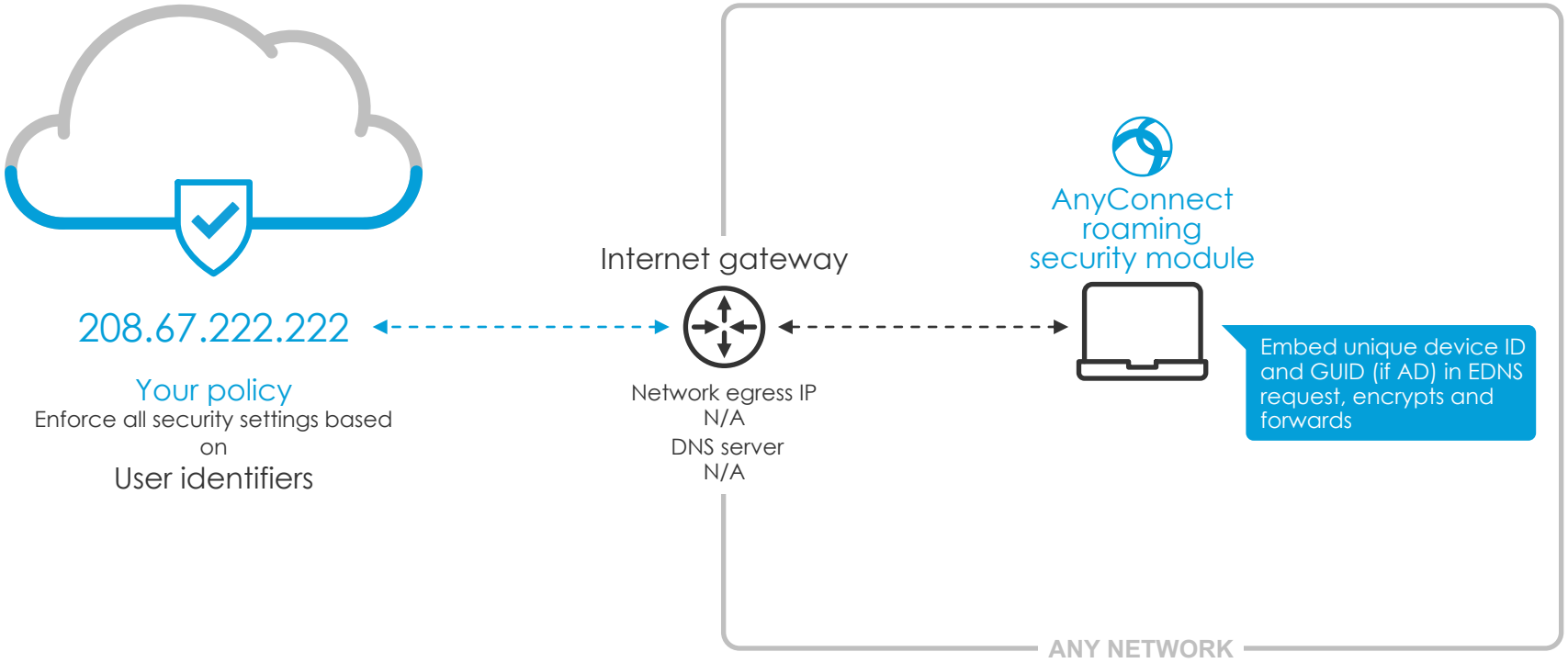
- First step in connecting to the internet
- Precedes file execution and IP connection
- Used by nearly all devices



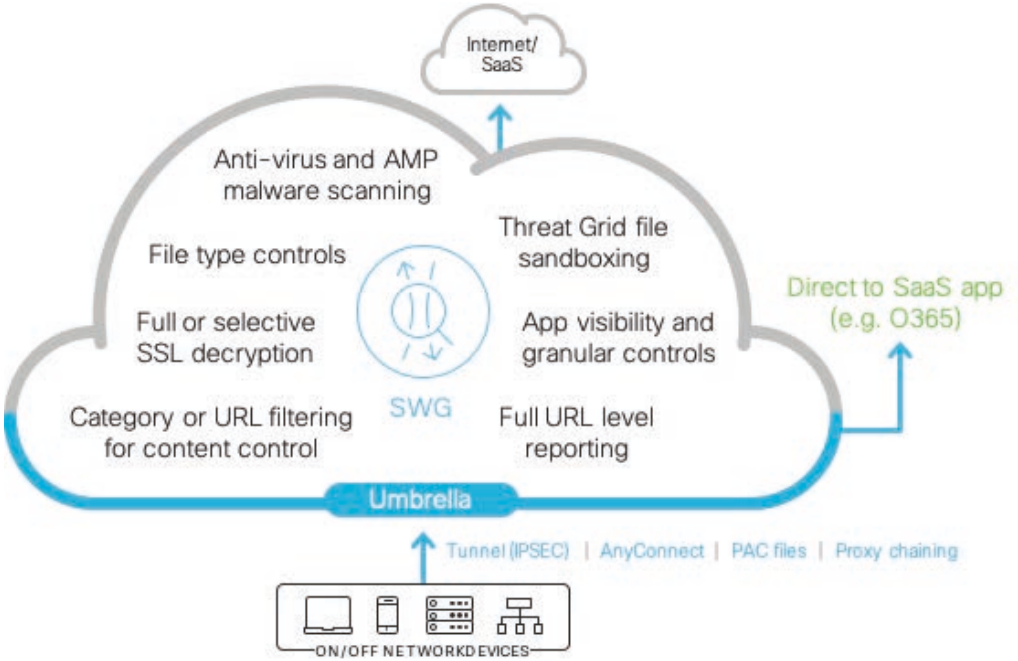
WHY UMBRELLA DNS-LAYER SECURITY

- Block domains associated with malware, phishing, command and control callbacks anywhere
- Stop threats at the earliest point and contain malware if already inside
- Accelerate threat response with an integrated security platform
- Amazing user experience — faster internet access; only proxy risky domains





UMBRELLA SIG CAPABILITIES



BACKED BY CISCO TALOS, UNRIVALED THREAT INTELLIGENCE

- **400+** full-time threat researchers and data scientists
- Analyzing **1.5 million** unique malware samples daily
- Blocking **20 billion threats** daily. More than 20x any other vendor.

We see more so you can block more and respond faster to threats.

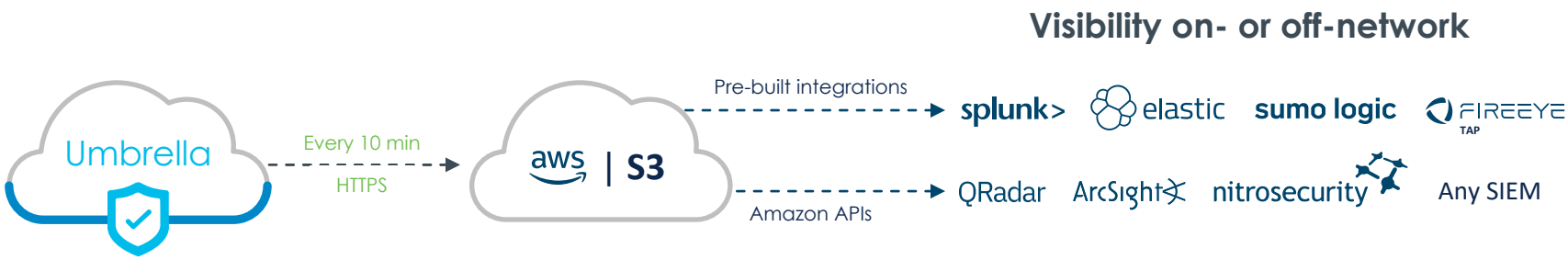
LOG STORAGE WITH AMAZON S3

S3 benefits

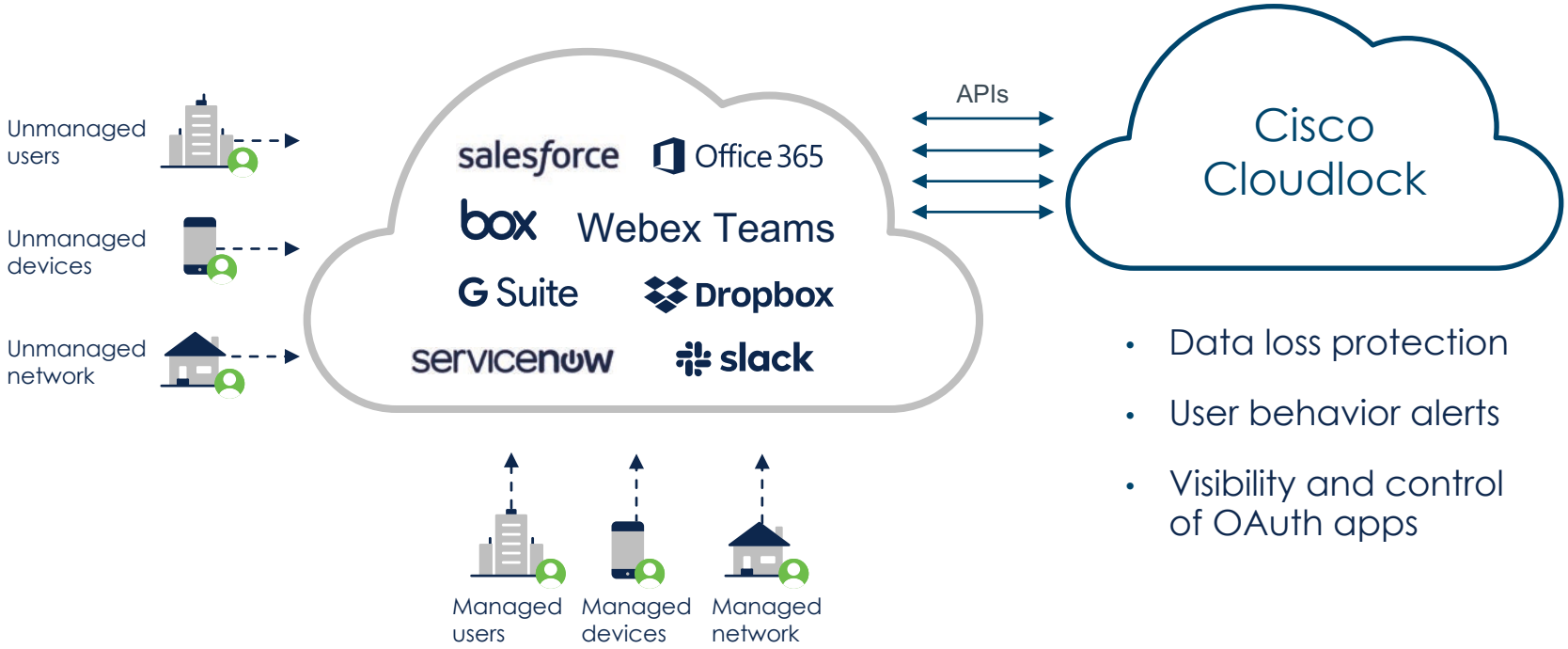
- Triple redundant and encrypted storage
- Pre-built SIEM/log analytic integrations
- Use self-managed or Cisco-managed bucket
- Centrally managed S3 logs

EU data warehouse available

- Ease data security concerns
- Store data in EU facility
- Use multi-org console for different storage settings for different locations

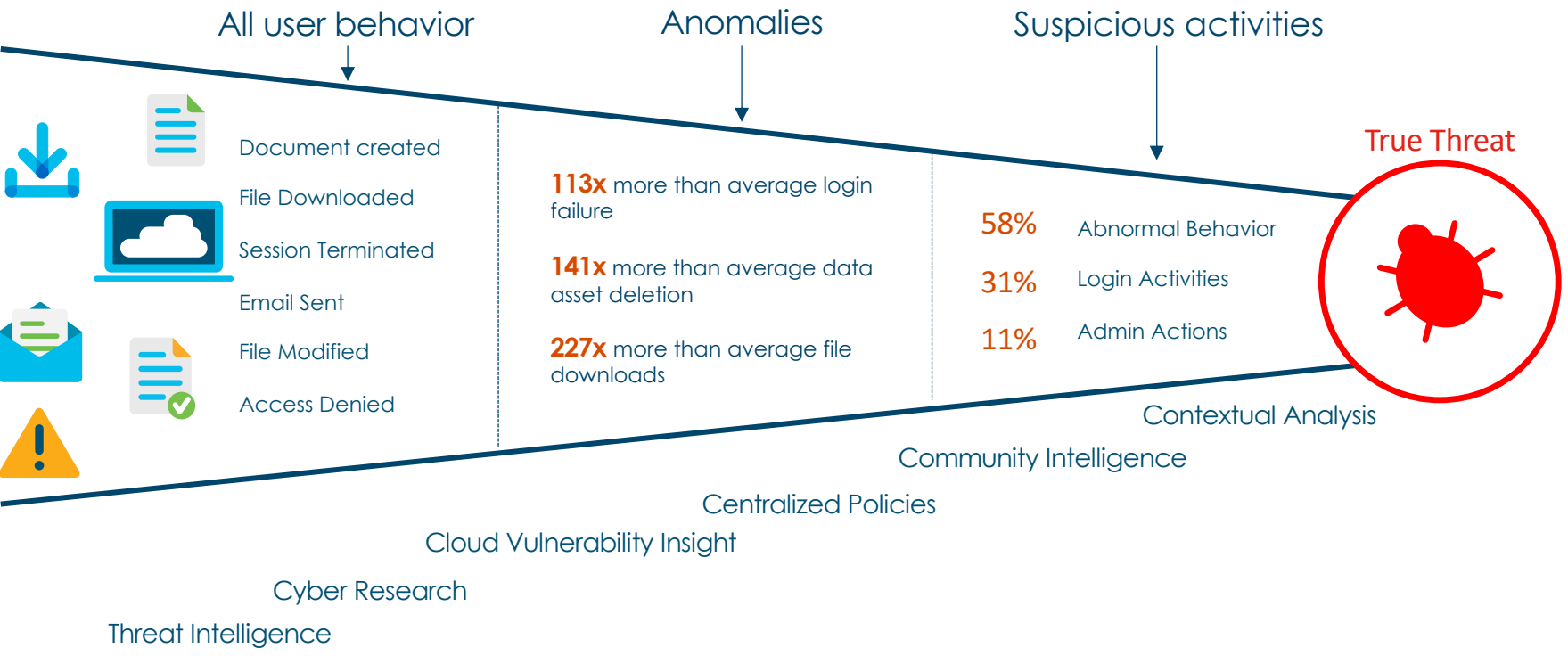


CISCO CLOUDLOCK (API-BASED CASB)



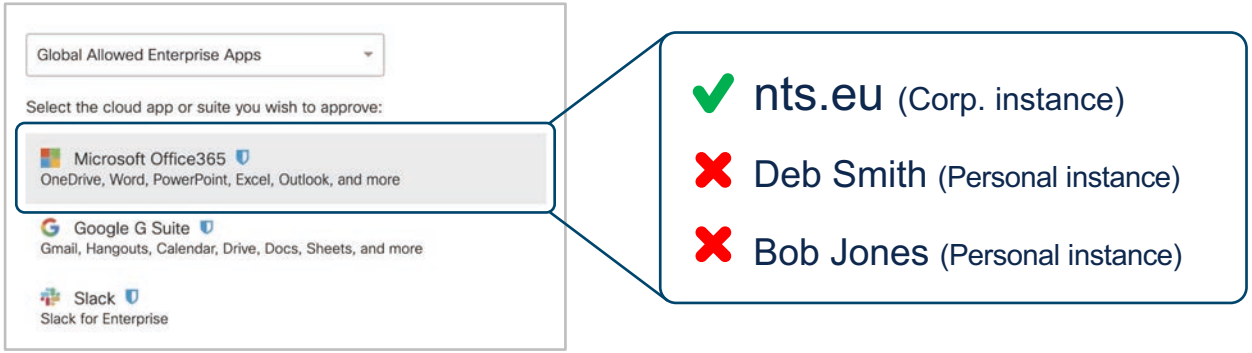
- Data loss protection
- User behavior alerts
- Visibility and control of OAuth apps

THE CLOUD THREAT FUNNEL



TENANT CONTROLS

Select the instance(s) of Core SaaS applications that can be accessed by all users or by specific groups/individuals

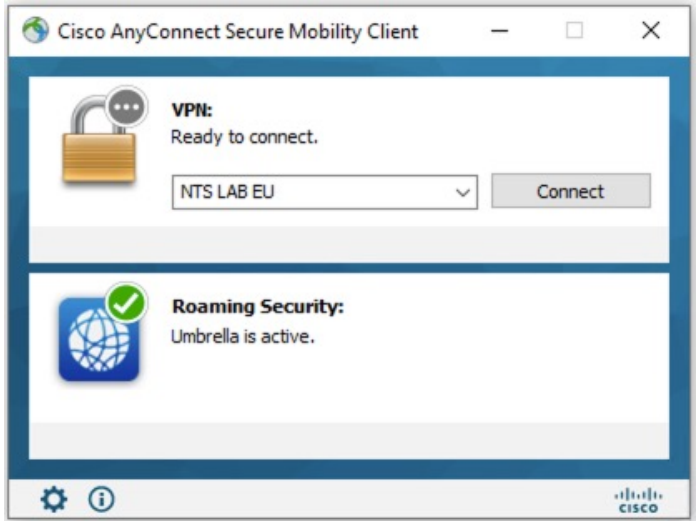


Key Use Cases

Security
Ensure, sensitive data is created and stored in approved instances of cloud apps

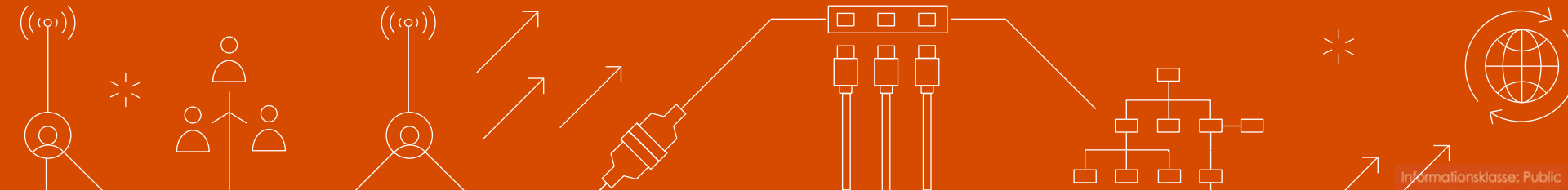
Productivity
Only provide access to corporate instances of core SaaS apps

WIE ROLLT MAN UMBRELLA AUS?



NTS

DEMO



2 Faktor Authentifizierung | McDonald's

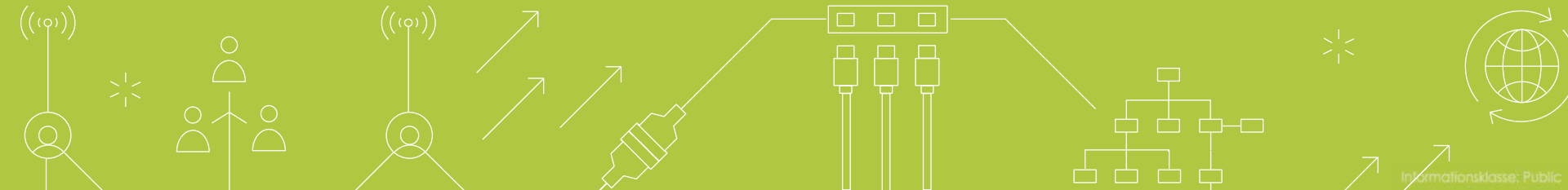
In 3 Schritten zu mehr Sicherheit!

Sichere App – Gesicherte Angebote:

Mit der 2-Faktor-Authentifizierung führen wir ein neues Sicherheitslevel für dich in deiner App ein! Mehr Sicherheit für deine Daten und deine gesammelten Ms.

NTS

DUO



DUO APP SUPPORT

Proprietary Apps (APIs)

C# Java python node Ruby

Microsoft Environments

Forefront Windows Office 365 Microsoft Active Directory Outlook

Cloud Services

Active Directory Federation Services Centrify onelogin okta PingIdentity

Unix Devices (SSH Sessions)

FreeBSD Linux redhat ubuntu

Internal Applications (VPNs)

OPENVPN paloalto Array Check Point Barracuda F5 FORTINET cisco JUNIPER

Cloud Applications

Dropbox salesforce Google Apps workday. amazon web services box Office 365 Cisco webex slack

Web Applications

splunk> Drupal Atlassian Confluence WordPress Atlassian JIRA Shibboleth

SAML 2.0 Applications

Google Apps amazon web services Office 365 salesforce box

NTS

DUO

MFA DEVICES


Wearables


Push


Biometrics


U2F


Phone Call

Soft Token


Hardware Tokens


SMS

NTS

DUO

DEVICE TRUST

Complete Visibility

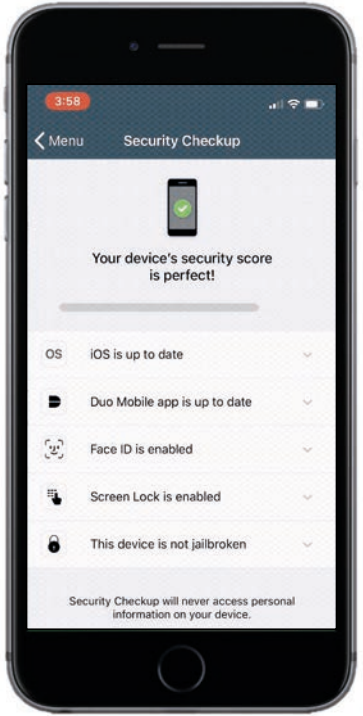
Assess Security Posture

Continuous Inspection

NTS

ASSESS MOBILE DEVICE POSTURE WITHOUT MDM

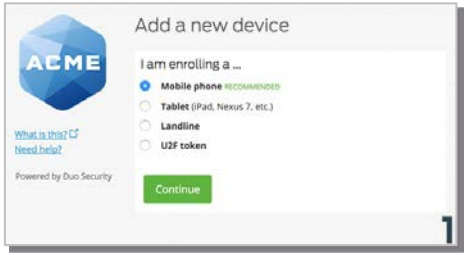
- Check if mobile devices are up-to-date
- Verify encryption and passcode lock
- Check if devices are jailbroken or tampered
- Works for managed and unmanaged mobile devices

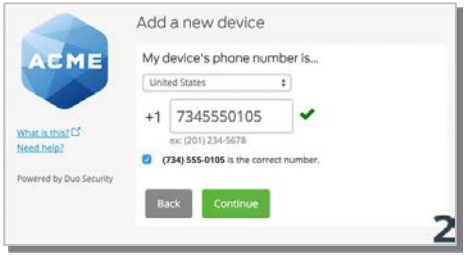


NTS

SELF-ENROLLMENT: EASILY ENROLL USERS IN MINUTES

- Users easily self-enroll in minutes
- Users leverage their own device
- Enroll thousands of users in hours
- Reduce TCO by enabling the user to easily enroll with no help needed





WHAT INFORMATION DOES DUO GATHER?

Mobile Devices

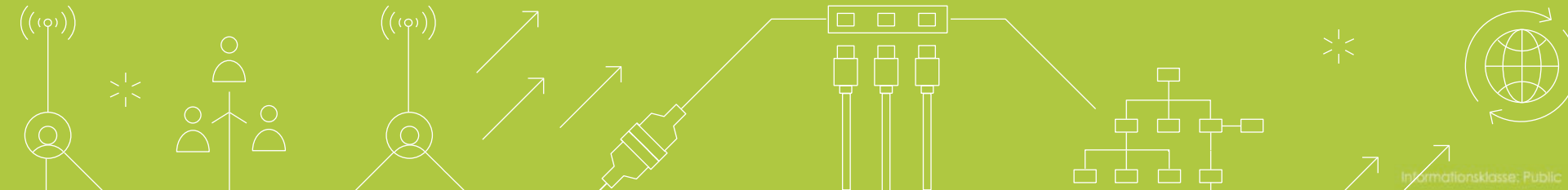
Corp managed asset status
Biometrics (Touch/Face) status
Screen lock status
OS condition (tampered) status
Encryption status
Platform type
Device OS type
Device OS version
Device owner
Duo Mobile version

Laptops / Desktops

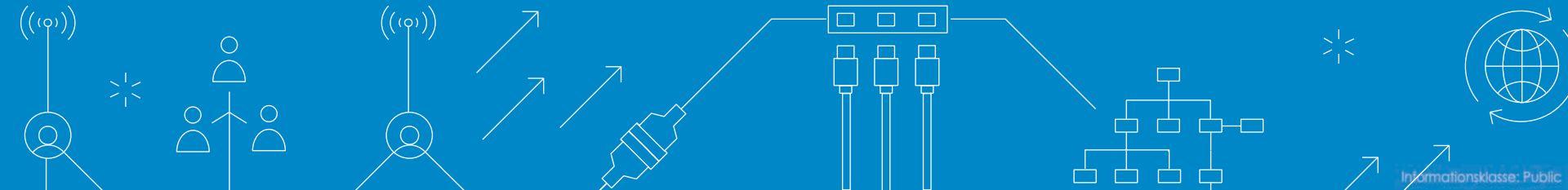
Disk encryption
Firewall enabled
Device password
OS patch level (Win 10)
Third party agents
Corp managed asset status*
OS type & versions
Browser type & versions
Flash & Java plugins versions
OS, browser and plugins status

NTS

DEMO

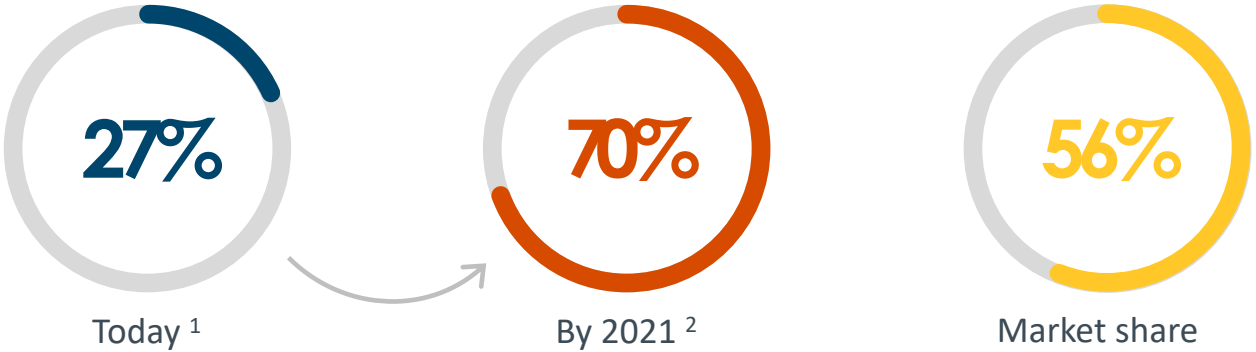


CLOUD MAILBOX DEFENSE



THE GREAT EMAIL MIGRATION

Public Cloud Email Services Adoption by Public and Private Companies



[1] Gartner, Survey Analysis: Google and Microsoft Battle It Out in a Growing Cloud Email Market
[2] Gartner, Market Guide for Email Security

#1

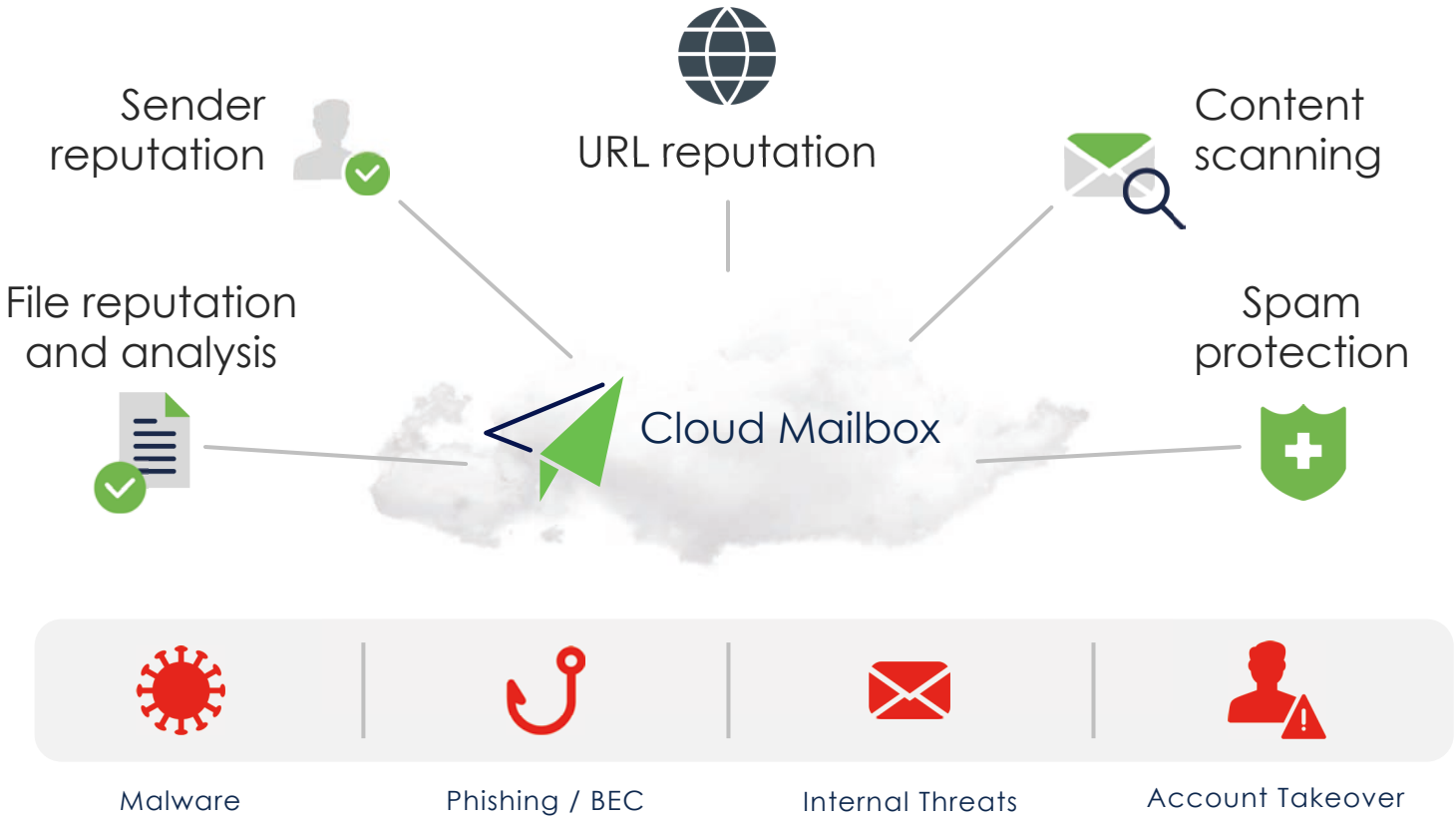
Email: The number one threat vector

$1.2B

in losses to business email compromise in 2018[1]

[1]FBI IDC report 2019.

NTS



CISCO SECURITY INSIDE MICROSOFT'S CLOUD

- ✓ No MX record changes
- ✓ Messages scanned in MS cloud
- ✓ Metadata sent to Cloud Mailbox
- ✓ Attachments stay in MS cloud[1]

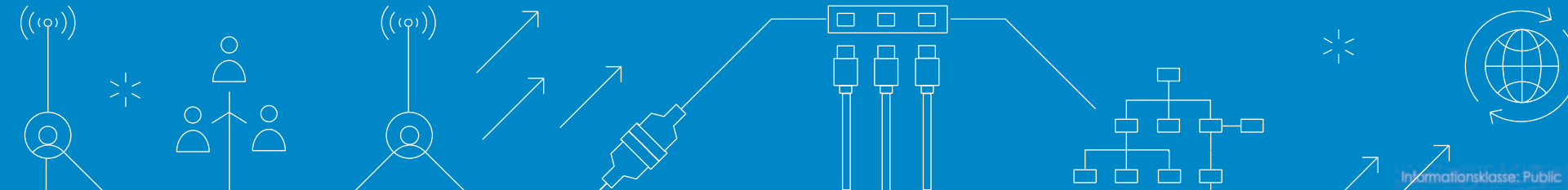
Bringing Cisco threat intelligence as close to the mailbox as possible

[1]Cloud file analysis is optional

NTS

NTS

DEMO



THE BIG THREE

Internet

#1 source of attacks

Email

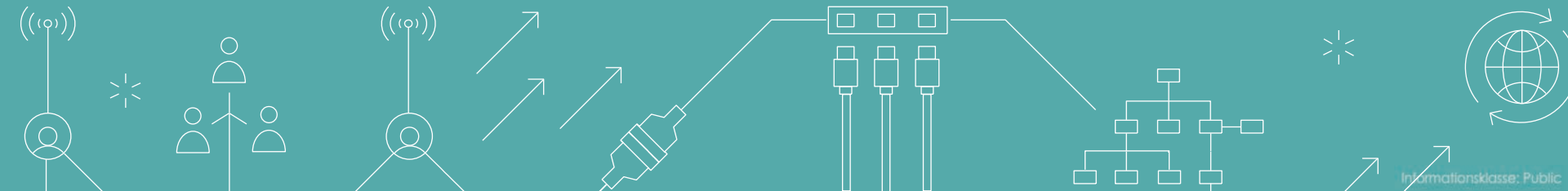
#1 attack vector

Endpoint

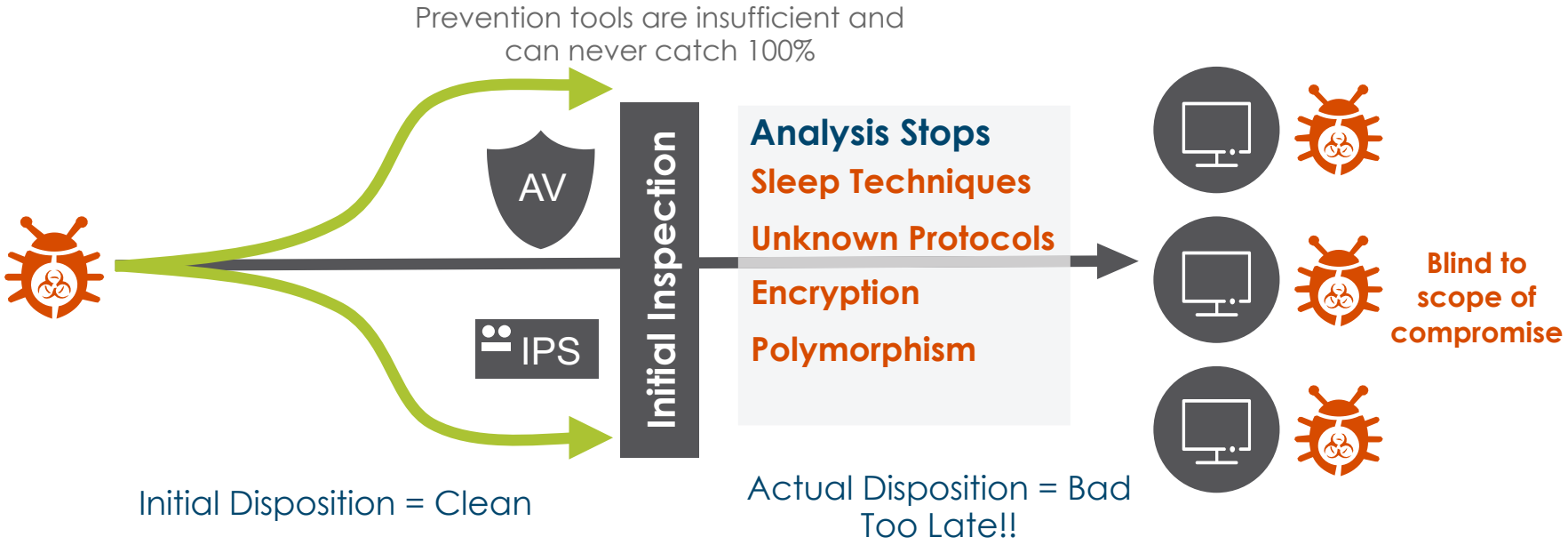
#1 target for attacks

NTS

SECURE ENDPOINT



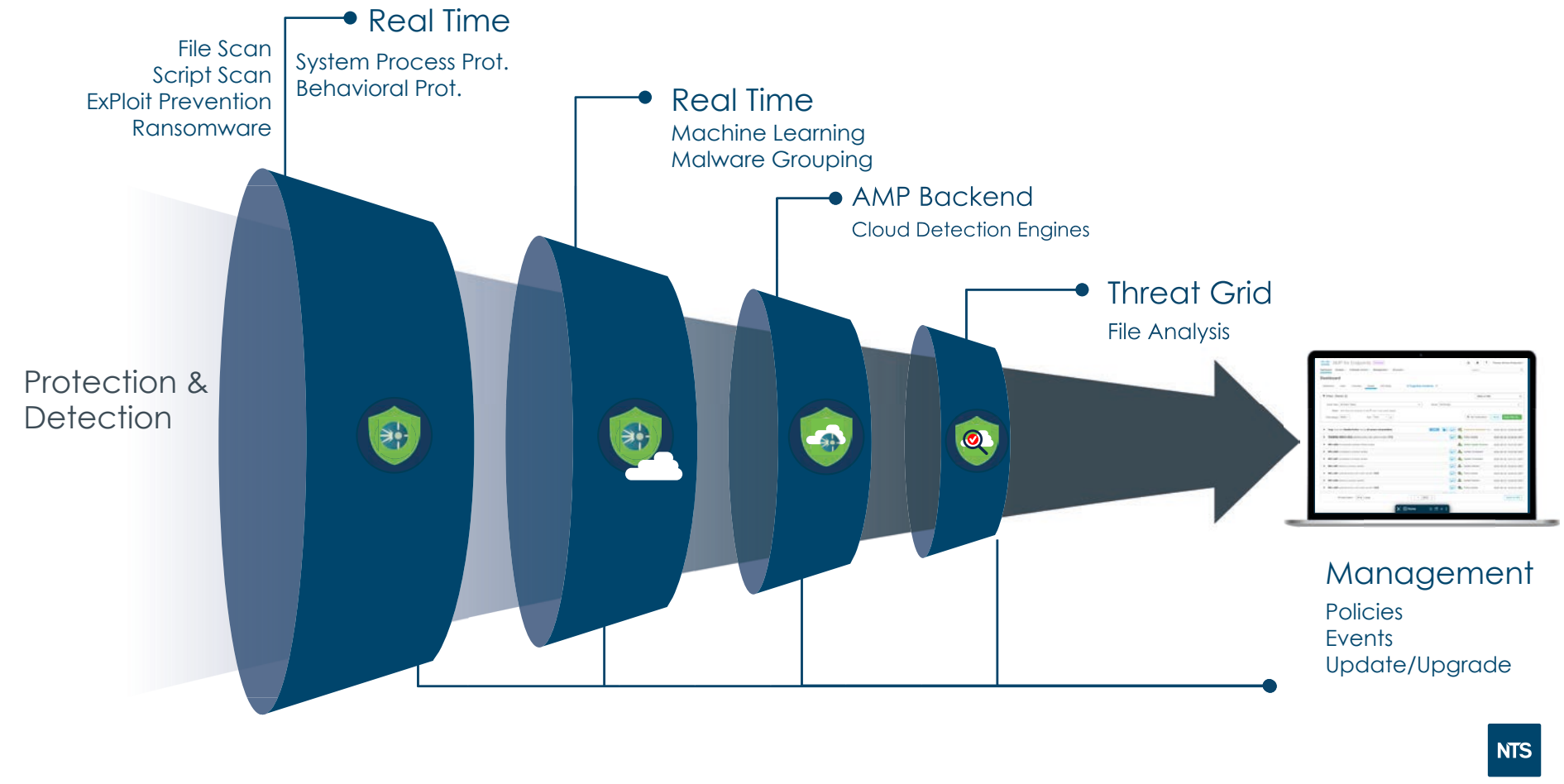
SECURE ENDPOINT



ENDPOINT CHALLENGE

20min with Win10 (Procmon)	Example	Result
• 46M OS operation events • 8.7M file events • 11.5K process events • 114K network events • 35M registry events	• 20K endpoints • Monitoring processes one week • How many are unknown? **1.2M unknown PE files**	• To much data to handle on-premise on the client • Threat landscape too complex to be handled on the endpoint • **Another approach necessary**

NTS



AMP RETROSPECTIVE

- Protection against false-positive/negative
- Block/clean after changing the disposition
- Changing disposition automatically (timeframe)
- Across the Cisco products
  - Email – Office 365 or/and MS Exchange remediation automatically

Retrospective Security Plan B

Unique to AMP - Continuous Analysis & Retrospective Security

HOW CISCO AMP DETECTS MALICIOUS CODE

SHA-256 Matching

Finds the low-hanging fruits

SPERO: Machine Learning

Examines PE headers, looks at DLL imports, compile location and ~400 factors

ETHOS: Fuzzy Fingerprinting

Attempts to pack/unpack/repack to match existing hash

Command Line Capture

Capture command line arguments and use them with Cloud IOCs to discover previously unknown attacks

Threat Grid: Dynamic Analysis (sandboxing)

Runs executable in virtual environment to determine threat score. ~1000 behavior indicators

Built-in AV and rootkit detection engine (TETRA)

Online/Offline full functional antivirus engine to protect against malware files.

Exploit Prevention

Randomize memory structure to protect against memory attacks and file-less malware

System Process Protection

Protects Windows system processes from being compromised through memory injection attacks

Low Prevalence / File Reputation

Analyze 'short-lived' suspects

CTA - Anomalous Web Traffic

Reduce time to detect unknown threats. Gain visibility into devices where agents cannot be installed, such as personal devices, critical server and IoT

Application Vulnerabilities

Highlight risky apps on devices

Cloud IOCs

Behavior-based and artifact analysis to uncover known and unknown malware. ~5.5M recipes

Malicious Activity Protection

Rules engine that looks at behaviors locally on the machine

DFC (Device Flow Correlation)

Device Flow Control (DFC) feature allows you to monitor and block network connections

Cisco TALOS

All malware that's been seen; campaign discovery and research

System Protection (SysPro)

Extends the Self Protect of AMP by protecting system processes from exploitation or process injection so AMP cannot be disabled or removed

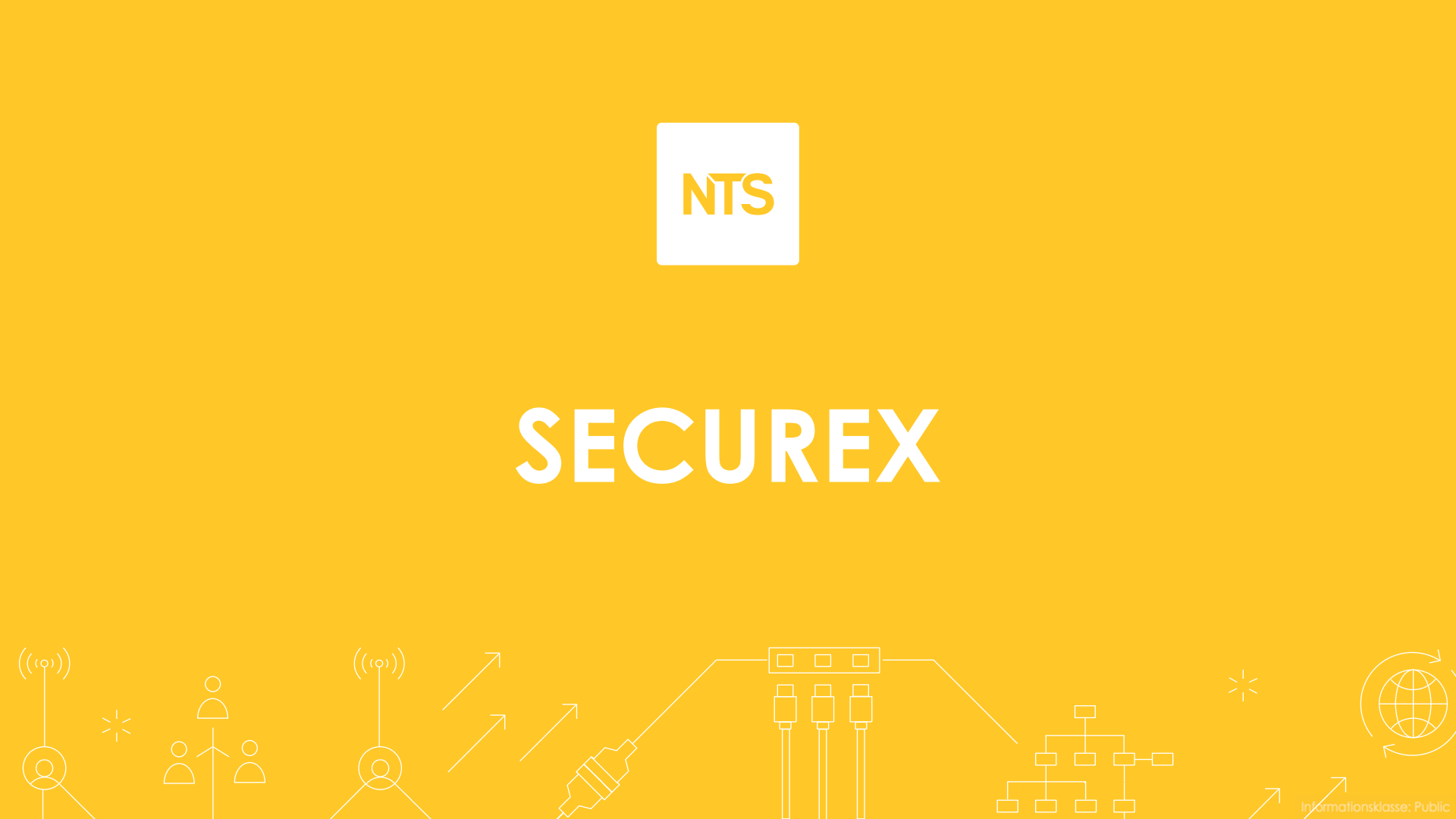
Endpoint Protection

Endpoint Monitoring

**** Services**

NTS

** external Services where the endpoint integrates


NTS
SECUREX
Informationsklasse: Public

SEE MORE, EVERYWHERE YOUR USERS WORK

"With one click in a single console, we can see everything that happened in our environment."

Umbrella

"We can see all internet activity across every device, everywhere."

AMP for Endpoints

"We can see everything happening on every endpoint, even 30 days back."

Email

"We can see exactly how attackers are trying to compromise our users' emails."

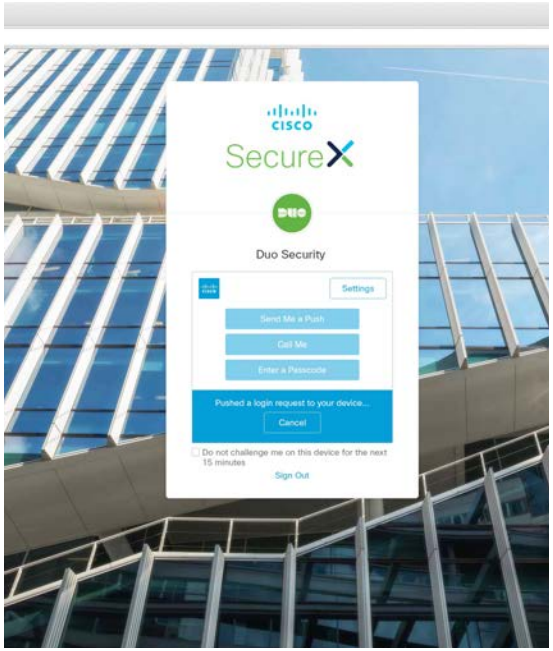
NTS

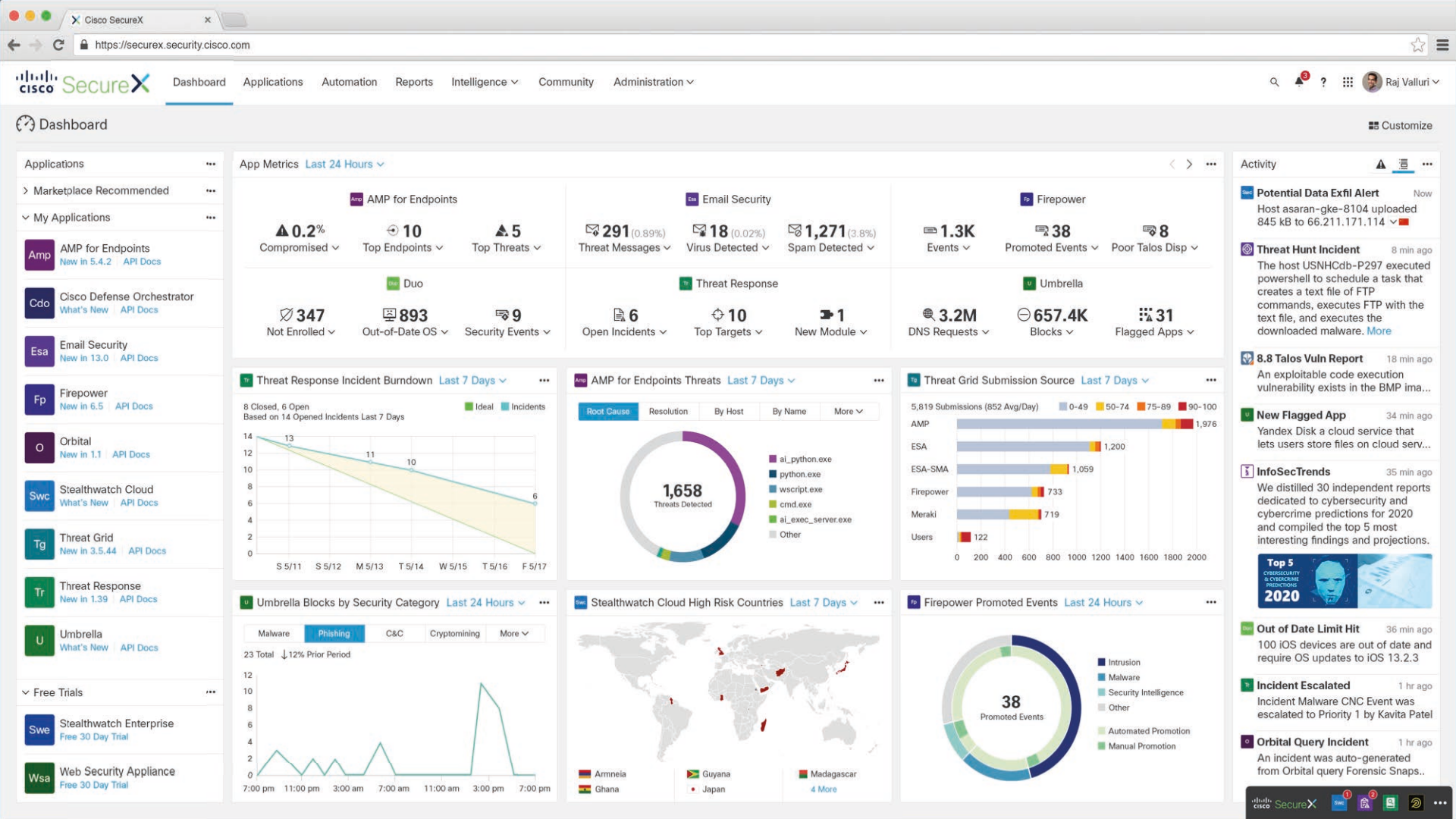
SECUREX COMPONENTS

- **Single Sign-on** for unified experience and simplified authentication
- **Threat response** for fast investigation and remediation
- **Orchestration** to reduce manual tasks
- **Customizable dashboard** to track detailed and important metrics
- **3rd party Integration**

SECUREX SIGN-ON

- Adaptive, layered, and simplified authentication
- Enter a single username and password to access all integrated applications, and maintain context through your workflows
- **Duo's Multi-Factor Authentication (MFA)** integrated secure sign-on feature means one push notification, one tap, instant access.

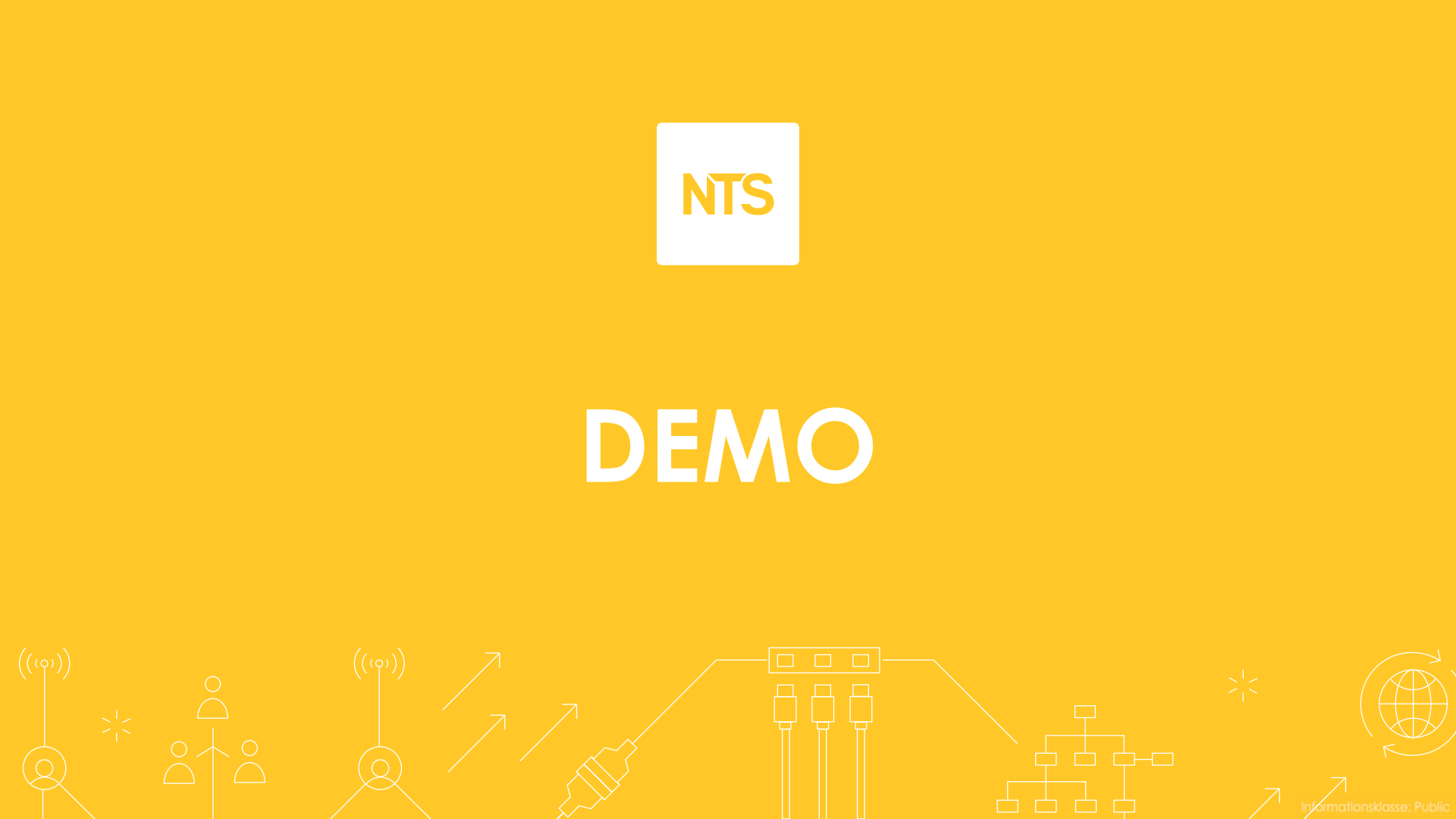



Cisco SecureX
https://securex.security.cisco.com
cisco SecureX
Dashboard
Applications
Automation
Reports
Intelligence
Community
Administration
Raj Valluri
Dashboard
Customize
Applications
Marketplace Recommended
My Applications
Amp
AMP for Endpoints
New in 5.4.2 | API Docs
Cdo
Cisco Defense Orchestrator
What's New | API Docs
Esa
Email Security
New in 13.0 | API Docs
Fp
Firepower
New in 6.5 | API Docs
O
Orbital
New in 1.1 | API Docs
Swc
Stealthwatch Cloud
What's New | API Docs
Tg
Threat Grid
New in 3.5.44 | API Docs
Tr
Threat Response
New in 1.39 | API Docs
U
Umbrella
What's New | API Docs
Free Trials
Swe
Stealthwatch Enterprise
Free 30 Day Trial
Wsa
Web Security Appliance
Free 30 Day Trial
App Metrics
Last 24 Hours
AMP for Endpoints
0.2%
Compromised
10
Top Endpoints
5
Top Threats
Email Security
291 (0.89%)
Threat Messages
18 (0.02%)
Virus Detected
1,271 (3.8%)
Spam Detected
Firepower
1.3K
Events
38
Promoted Events
8
Poor Talos Disp
Duo
347
Not Enrolled
893
Out-of-Date OS
9
Security Events
Threat Response
6
Open Incidents
10
Top Targets
1
New Module
Umbrella
3.2M
DNS Requests
657.4K
Blocks
31
Flagged Apps
Threat Response Incident Burndown
Last 7 Days
8 Closed, 6 Open
Based on 14 Opened Incidents Last 7 Days
Ideal
Incidents
14
12
10
8
6
4
2
0
13
11
10
6
S 5/11
S 5/12
M 5/13
T 5/14
W 5/15
T 5/16
F 5/17
AMP for Endpoints Threats
Last 7 Days
Root Cause
Resolution
By Host
By Name
More
1,658
Threats Detected
ai_python.exe
python.exe
wscript.exe
cmd.exe
ai_exec_server.exe
Other
Threat Grid Submission Source
Last 7 Days
5,819 Submissions (852 Avg/Day)
0-49
50-74
75-89
90-100
AMP
1,976
ESA
1,200
ESA-SMA
1,059
Firepower
733
Meraki
719
Users
122
0
200
400
600
800
1000
1200
1400
1600
1800
2000
Umbrella Blocks by Security Category
Last 24 Hours
Malware
Phishing
C&C
Cryptomining
More
23 Total
12% Prior Period
12
10
8
6
4
2
0
7:00 pm
11:00 pm
3:00 am
7:00 am
11:00 am
3:00 pm
7:00 pm
Stealthwatch Cloud High Risk Countries
Last 7 Days
Armneia
Guyana
Madagascar
Ghana
Japan
4 More
Firepower Promoted Events
Last 24 Hours
38
Promoted Events
Intrusion
Malware
Security Intelligence
Other
Automated Promotion
Manual Promotion
Activity
Potential Data Exfil Alert
Now
Host asaran-gke-8104 uploaded 845 kB to 66.211.171.114
Threat Hunt Incident
8 min ago
The host USNHCdb-P297 executed powershell to schedule a task that creates a text file of FTP commands, executes FTP with the text file, and executes the downloaded malware. More
8.8 Talos Vuln Report
18 min ago
An exploitable code execution vulnerability exists in the BMP ima...
New Flagged App
34 min ago
Yandex Disk a cloud service that lets users store files on cloud serv...
InfoSecTrends
35 min ago
We distilled 30 independent reports dedicated to cybersecurity and cybercrime predictions for 2020 and compiled the top 5 most interesting findings and projections.
Top 5
CYBERSECURITY & CYBERCRIME PREDICTIONS
2020
Out of Date Limit Hit
36 min ago
100 iOS devices are out of date and require OS updates to iOS 13.2.3
Incident Escalated
1 hr ago
Incident Malware CNC Event was escalated to Priority 1 by Kavita Patel
Orbital Query Incident
1 hr ago
An incident was auto-generated from Orbital query Forensic Snaps..
cisco SecureX

PRODUCTS WITH BUILT-IN SECUREX FEATURES NOW

Cisco Security integration \ built-in SecureX feature		Threat response	Orchestration	Dashboard tiles	Ribbon interface	Sign-on
Cisco AMP for Endpoints		✓	✓	✓	✓	✓
↳ Cisco Orbital (advanced search)		✓	✓	✓	✓	✓
↳ Cisco Threat Grid (malware analytics)		✓	✓	✓	✓	
Cisco NGFW (FMC & FDM) [1]		✓	✓ [3]	✓		
↳ Cisco Defense Orchestrator			✓	✓	✓	✓
Cisco Umbrella (cloud security)		✓	✓	✓	✓	✓
Cisco Email Security [2]		✓	✓ [3,4]	✓	✓	Oct '20 [4]
Cisco Web Security Appliance [2]		✓	✓ [3]	✓	Aug '20	
Cisco Stealthwatch (traffic analytics)		✓	✓ [3]	✓	✓	
↳ Cisco Stealthwatch Cloud		July '20	✓	✓	✓	✓
Cisco Tetration (workload protection)			✓ [3,4]	✓	Oct '20	Aug '20
Cisco Duo (multi-factor authentication)			✓	Aug '20		
Cisco Identity Services Engine (network access)			✓ [3]			
Other integrations [5]	Cisco & third-party infrastructure		✓ [3,4]			
	Third-party security	✓	✓ [6]			

1. Uses Cisco Security Services Exchange
2. Can use Cisco Security Management Appliance or direct
3. On-prem deployment needs remote connector, which will be published in Git repository when available.
4. Available for SaaS/cloud product deployment
5. A full list will be published at general availability, and a partial list of threat response integrations is online at cs.co/threatresponseintegrations
6. Some use threat response integration with orchestration




NTS
RELAX,
WE CARE