

ntop and Checkmk. A dream team for network monitoring. ntopConf '23

checkmk.com

Total service problems

Percentage of total service problems

Top alerters (last 7 days)

Problems	Host
667	ap-ms-04
668	ap-ms-01
668	ap-ms-03

Who I am



Martin Hirschvogel
VP Product

Since 2018

VP Product, Checkmk

2017 - 2018

Chief of Staff, Teamviewer

2014 - 2016

Consultant,
The Boston Consulting Group

Love to build
products ...

... and break
things

Agenda

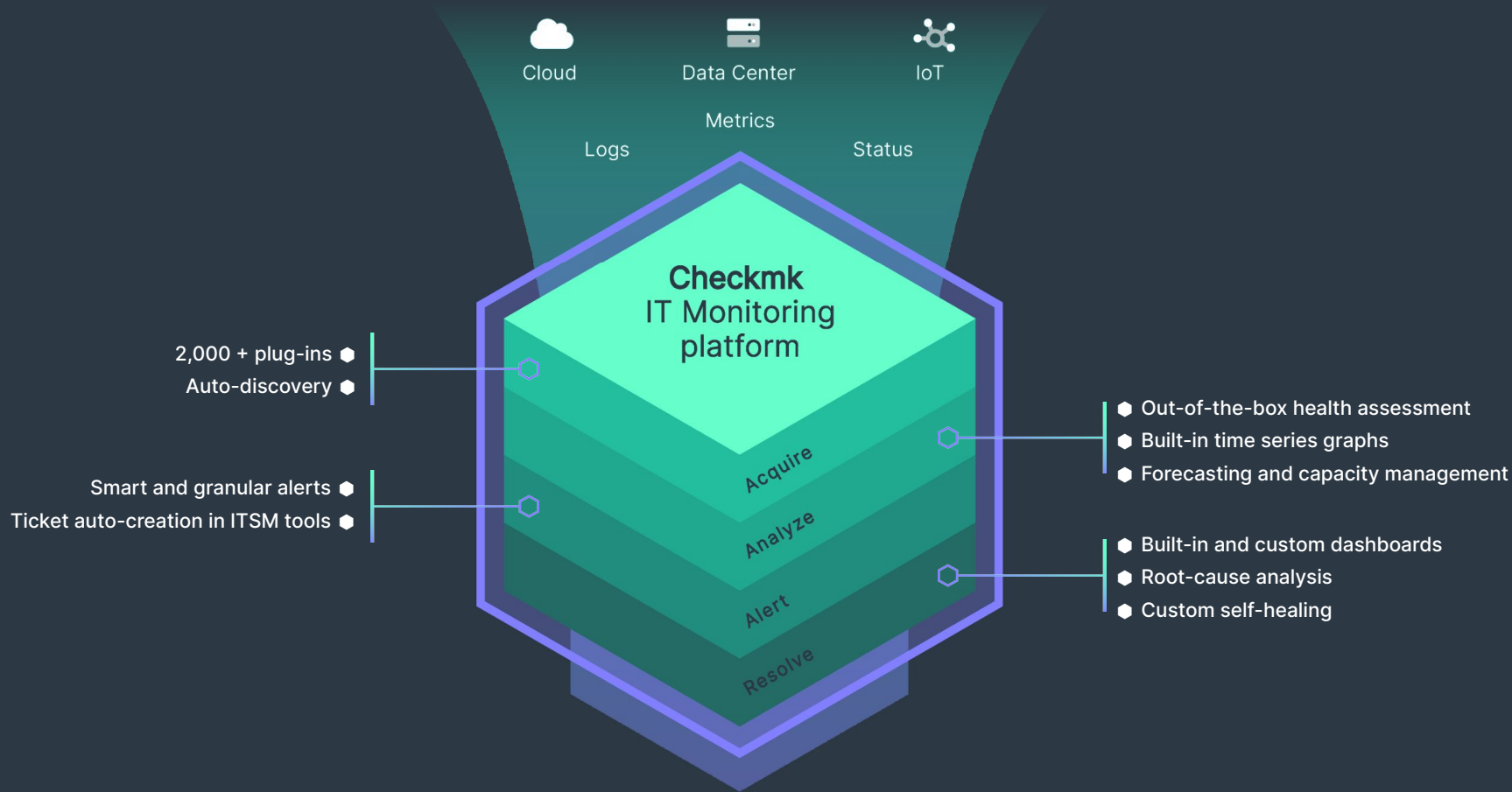


01 Introduction Checkmk

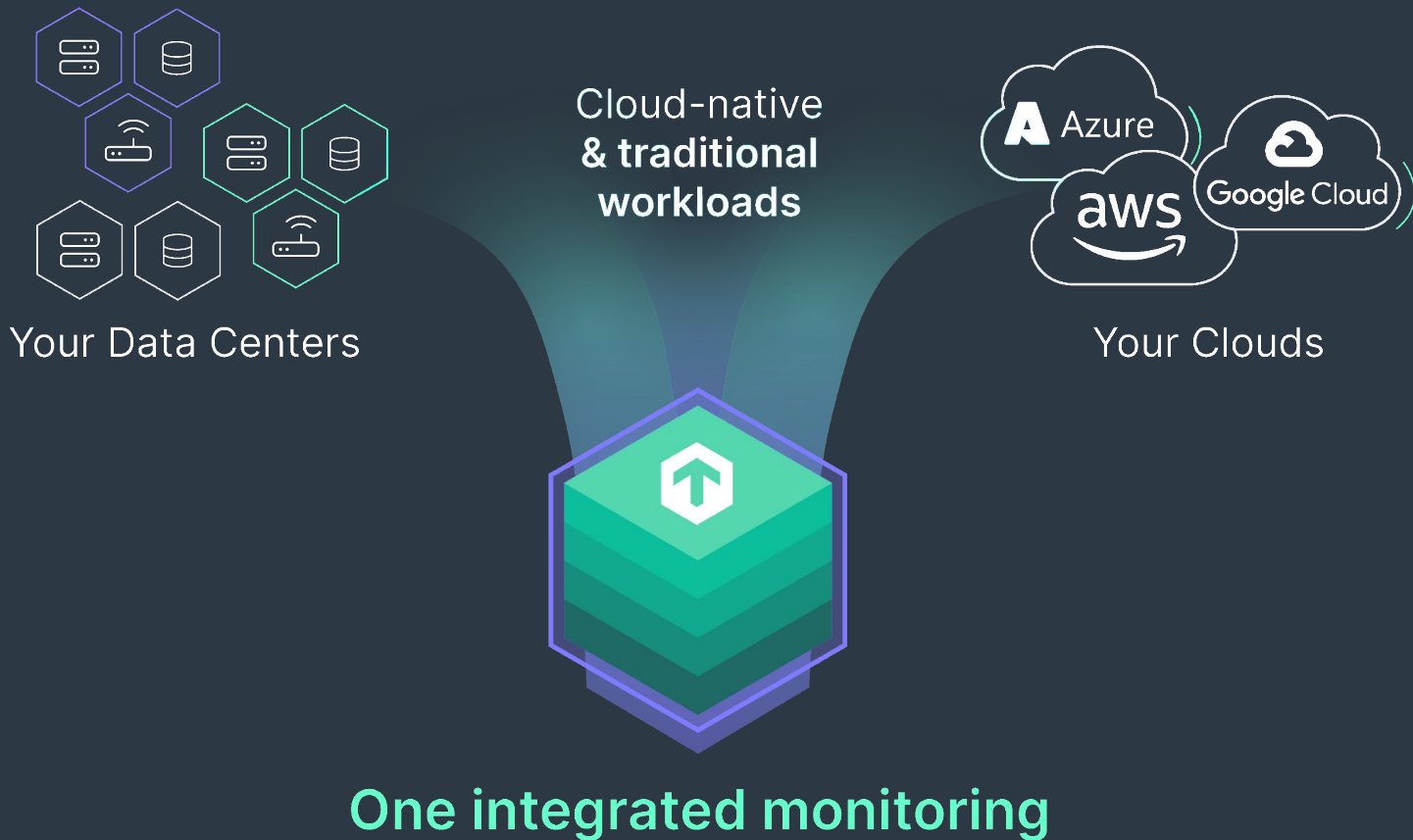
02 Checkmk + ntop

03 Learnings from building a ntop integration

Fast track your time-to-resolution

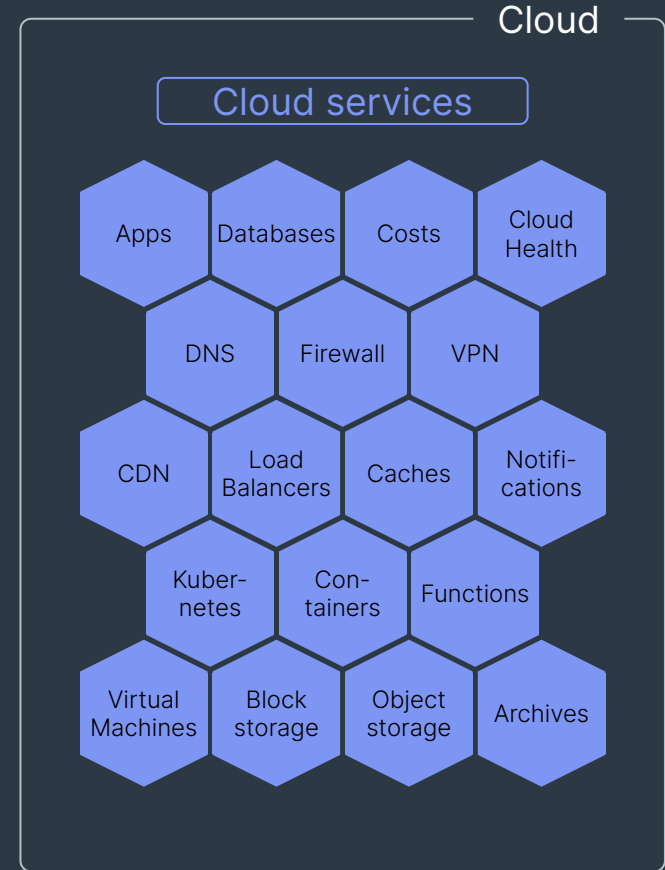
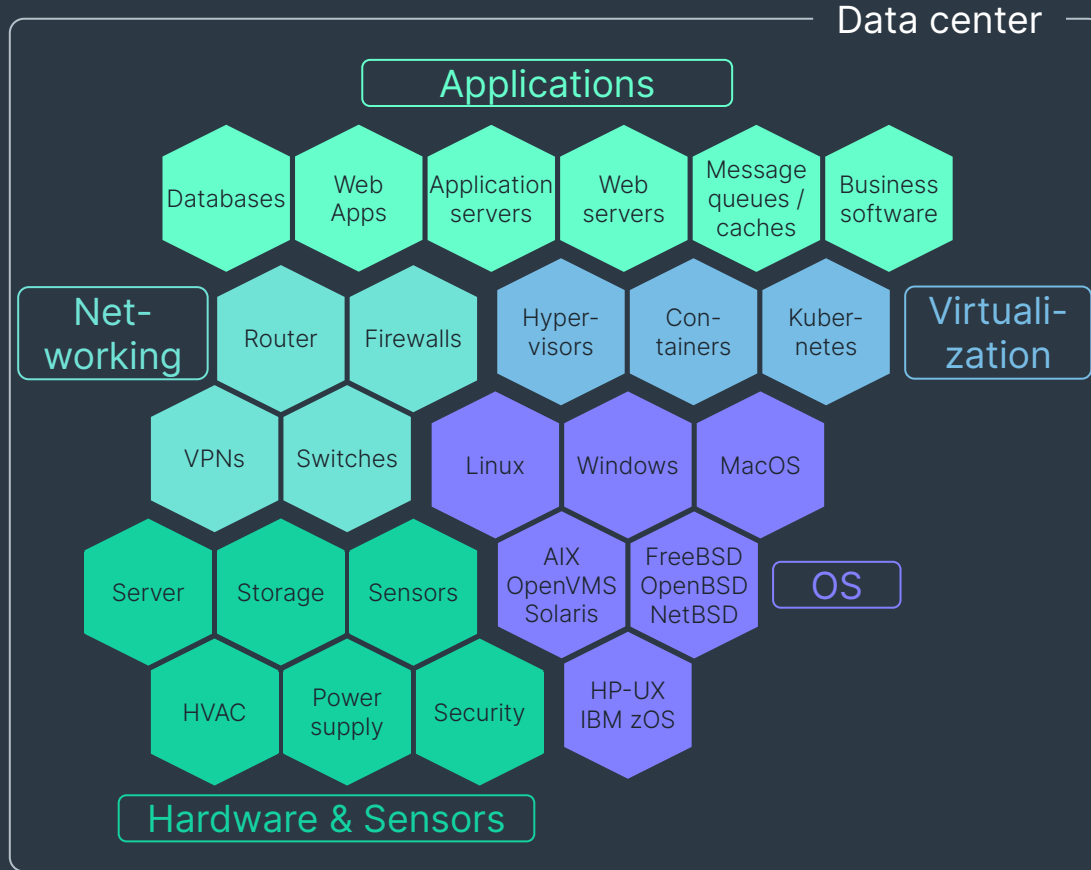


Our mission: bringing visibility into your hybrid IT





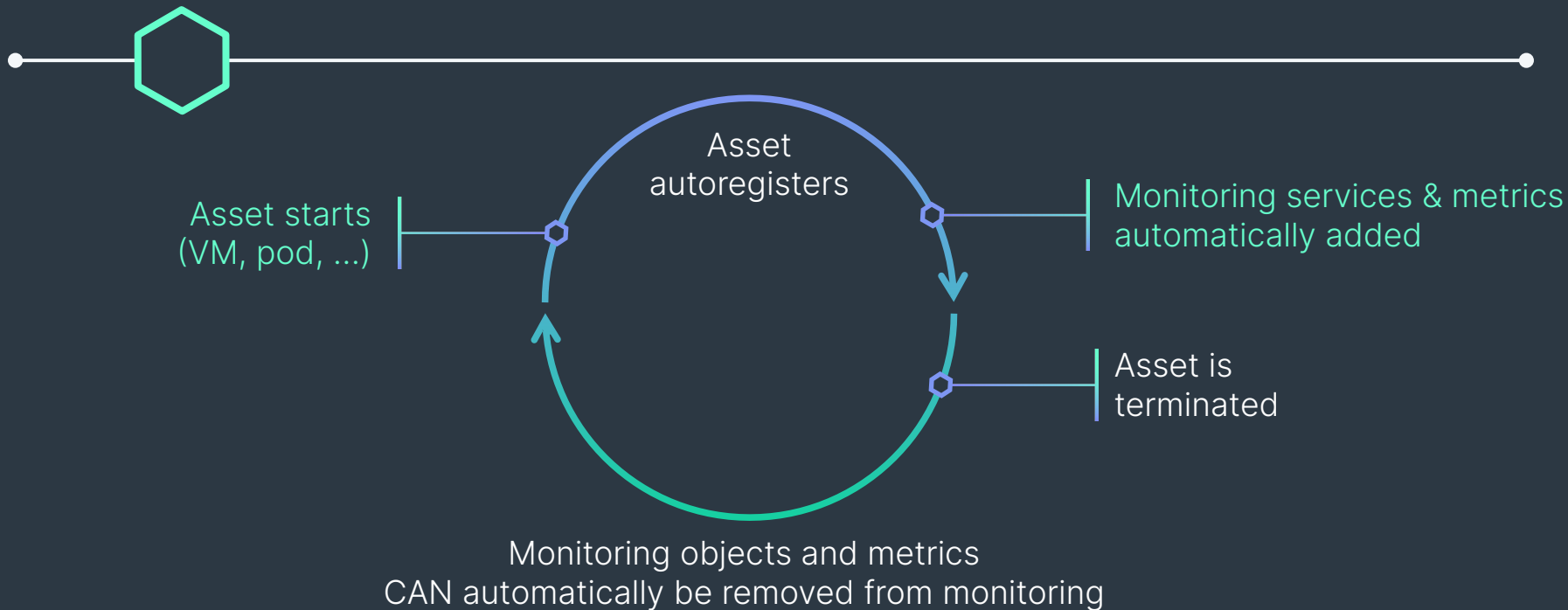
Monitor everything: 2,000+ well-maintained plug-ins





Highly automated to monitor at scale

Auto-register
workloads





Highly automated to monitor at scale

Auto-register
workloads

Auto-discover
services



State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK	☰ 📁	[agent] Success, [piggyback] Success (but no data found for this host), execution time 1.2 sec	2023-05-08 07:17:22	6.74 s	1.16 s
OK	Check_MK Agent	☰	Version: 2.1.0p25, OS: linux, TLS is not activated on monitored host (see details), Agent plugins: 0, Local checks: 0	2023-05-08 07:17:22	6.74 s	
OK	Check_MK Discovery	☰	Services: all up to date, Host labels: all up to date	2023-05-08 07:28:00	96 m	
OK	Check_MK HW/SW Inventory	☰	Found 91 inventory entries, Found 17 status entries	2023-05-08 07:34:08	213 m	
OK	CPU load	☰ 📁	15 min load: 0.35, 15 min load per core: 0.09 (4 cores)	2023-05-15 13:02:40	6.75 s	0.53
OK	CPU utilization	☰ 📁	Total CPU: 12.40%	2023-08-09 06:58:24	6.75 s	12.4%
OK	Disk IO SUMMARY	☰ 📁	Read: 0.00 B/s, Write: 49.2 kB/s, Latency: 940 microseconds	2023-05-08 07:17:22	6.75 s	0.00 B/s / 48.00 KiB/s
OK	Filesystem /	☰ 📁	Used: 37.00% - 71.6 GiB of 194 GiB, trend per 1 day 0 hours: +861 MiB, trend per 1 day 0 hours: +0.43%, Time left until disk full: 145 days 1 hour	2023-05-09 08:29:16	6.75 s	37.0%
OK	Filesystem /boot/efi	☰ 📁	Used: 5.78% - 6.04 MiB of 104 MiB, trend per 1 day 0 hours: +0 B, trend per 1 day 0 hours: +0%	2023-05-08 07:17:22	6.75 s	5.78%
OK	Filesystem /opt/omd/sites/monitoring/tmp	☰ 📁	Used: 0.33% - 12.8 MiB of 3.82 GiB, trend per 1 day 0 hours: +1.62 GiB, trend per 1 day 0 hours: +42.34%, Time left until disk full: 2 days 8 hours	2023-05-08 07:17:22	6.75 s	0.33%
OK	HTTPS Certificate	☰	OK - Certificate 'monitoring.3.7.nip.io' will expire on Thu Oct 5 17:47:02 2023 +0000.	2023-05-17 08:52:56	21.8 s	
OK	Interface 2	☰ 📁	[eth0], (up), MAC: 02:D8:7A:8B:1E:04, Speed: unknown, In: 203 kB/s, Out: 112 kB/s	2023-05-08 07:17:22	6.75 s	1.63 Mbit/s / 898 kbit/s
OK	Kernel Performance	☰ 📁	Process Creations: 5.58/s, Context Switches: 1397.35/s, Major Page Faults: 0.02/s, Page Swap in: 0.00/s, Page Swap Out: 0.00/s	2023-05-08 07:17:22	6.75 s	0.02/s
OK	Memory	☰ 📁	Total virtual memory: 24.16% - 2.81 GiB of 11.6 GiB, 9 additional details available	2023-05-17 08:54:21	6.76 s	36.79%

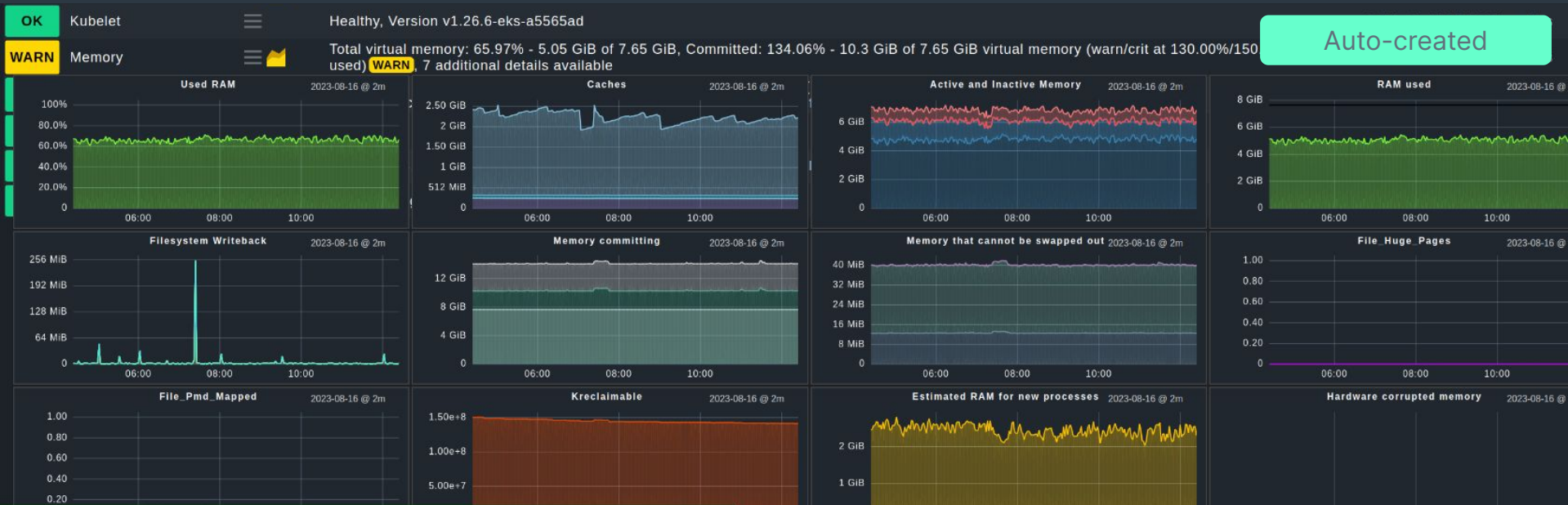
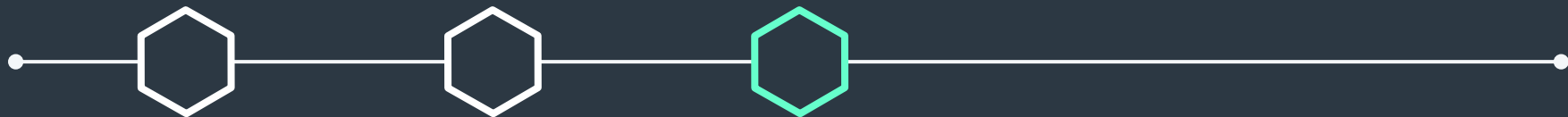


Highly automated to monitor at scale

Auto-register
workloads

Auto-discover
services

Metrics
dashboards





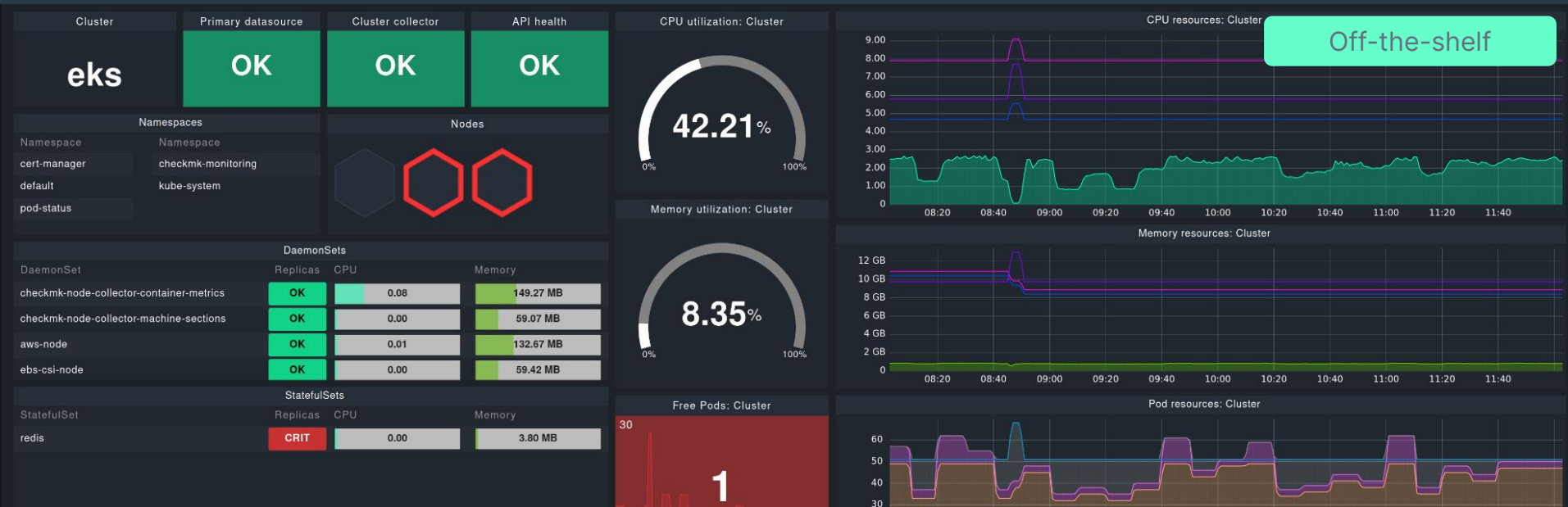
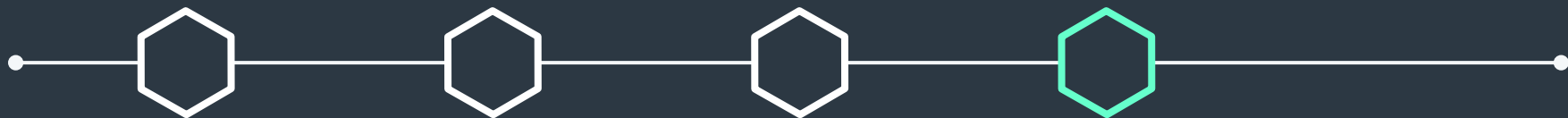
Highly automated to monitor at scale

Auto-register
workloads

Auto-discover
services

Metrics
dashboards

Application
dashboards



Highly automated to monitor at scale



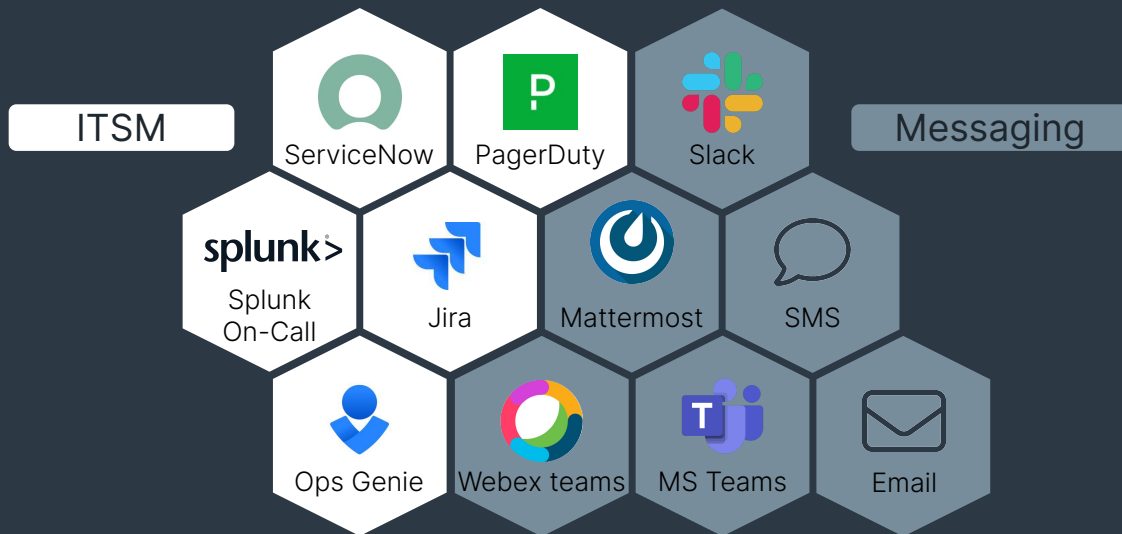
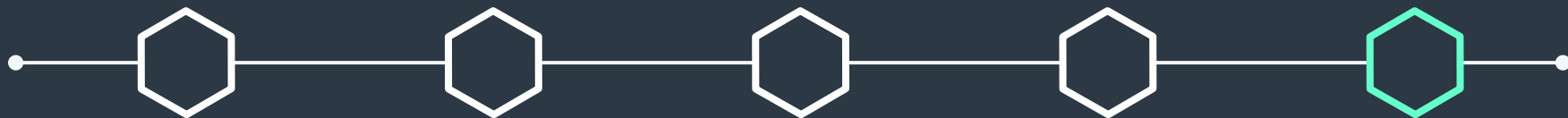
Auto-register
workloads

Auto-discover
services

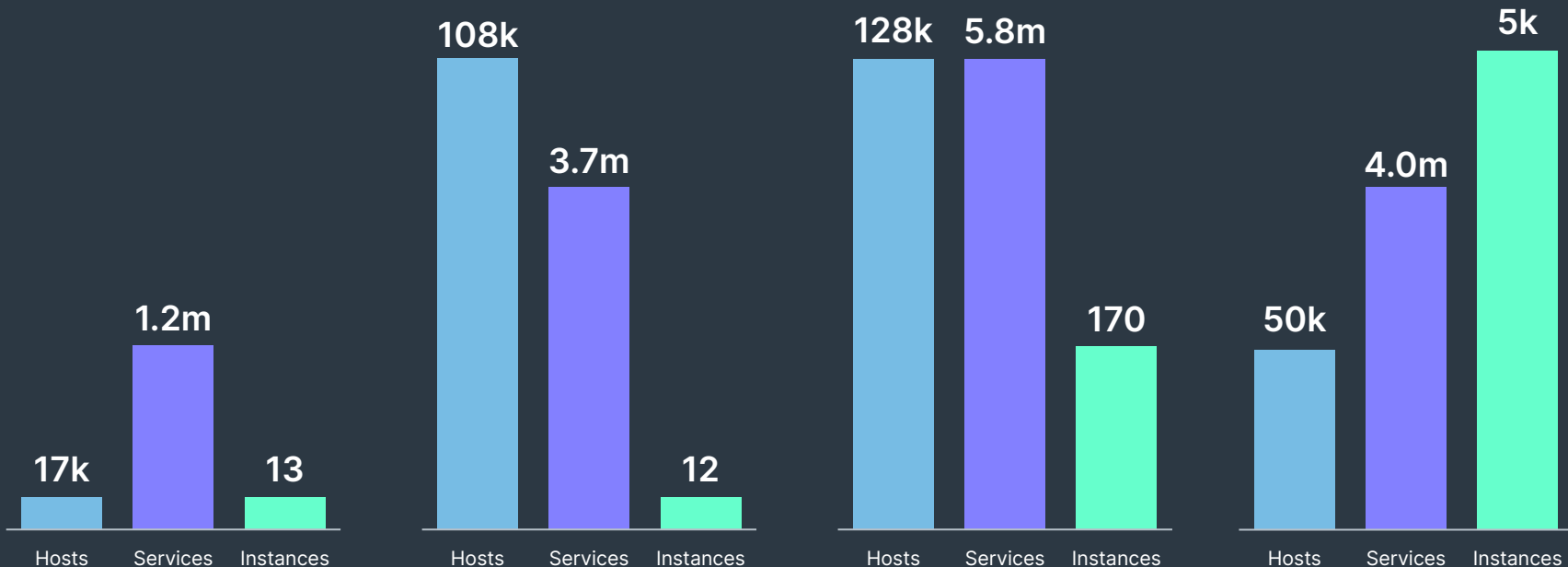
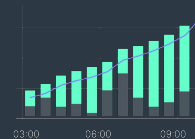
Metrics
dashboards

Application
dashboards

**Automated
alerting**



Hyper-scalable distributed set-ups



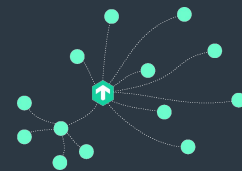
Scale vertically

100k+ services per instance

Scale horizontally

with massively distributed set-ups

Extensible open-source monitoring



Build your own integrations
with simple scripts extending agents or by
writing entire plug-ins yourself

```
from .agent_based_api.v1 import register, Result, Service, State

def discover_myhostgroups(section):
    yield Service()

def check_myhostgroups(section):
    attr = section.get("check_mk")
    hosts = attr["members"] if attr else ""
    if hosts:
        yield Result(state=State.CRIT, summary=f"Default group is not empty: {hosts}")
    else:
        yield Result(state=State.OK, summary="Everything is fine")

register.check_plugin(
    name="myhostgroups",
    service_name="Hostgroup check_mk",
    discovery_function=discover_myhostgroups,
    check_function=check_myhostgroups,
```

Extend existing integrations
to accommodate own requirements

- Majority of code base open source
- Easily readable and modifiable Python code
- Developer APIs for writing monitoring integrations
- Built-in logic to handle customized code
- Large partner ecosystem for customizations

The Checkmk Community

Where IT Monitoring experts meet



User forum

>6.000 users
>10,000 daily visits

GitHub

>180 contributors

Integration exchange

540+ packages

Translations

6 languages

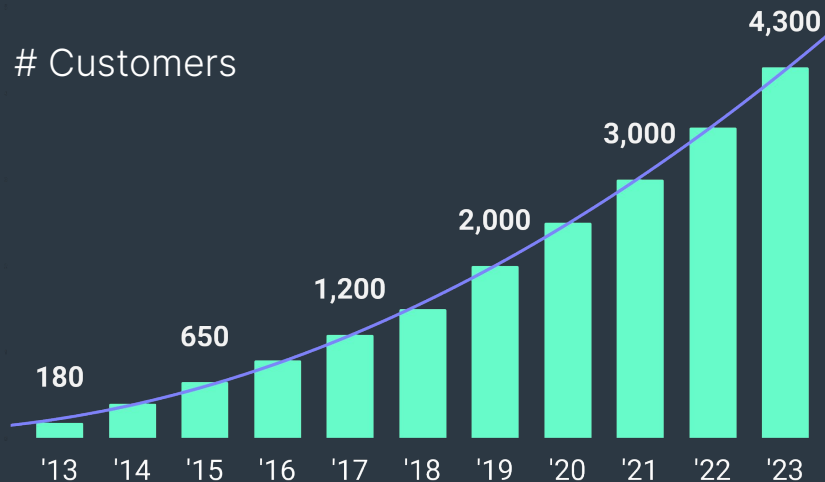


Checkmk — The Company



- 150+ employees, privately held, debt free
- Based in Munich, Germany, and Atlanta, USA
- Focusing on IT monitoring for 15+ years
- Open-source enthusiasts

Customers



Checkmk + ntop



Integrate network flow monitoring in Checkmk



What you already get from Checkmk

- Network performance monitoring & metrics
 - Bandwidth (e.g. bits in/out)
 - Packet rate
 - Error rate
- Network interface status and speed
- Alerting



What you might want to do in addition

- Deeper root cause analyses (e.g. quick identification of network bottlenecks)
- Network flow analyses (e.g. top talkers, ...)
- In-depth performance monitoring (e.g. delay, round-trip-times, ...)
- Support threat detection (e.g. quick identification of threats like DDoS attacks)



Real-life scenario



Low bandwidth capacity at remote location - only 2Mbit :(
Machines there mostly use Citrix Virtual Desktop. Normally bandwidth sufficient, but every once in a while, completely unusable as someone occupying all bandwidth



Bandwidth monitoring via Checkmk to receive alert when 'culprit' is at work again.



Alert!!!
Look into ntop for analysis. A lot of ssh traffic!



Infrastructure was 'unknowingly' used by students who copied a lot of research data around with scp...





Service random-machine, Interface 3

Monitor > Overview > All hosts > random-machine > Services of Host > Service

Commands Service Host Add to Export Display Help ⌵ ⚠ ⚡ 🔍 ⌵ ⬆

Service state

CRIT

Summary [wlo1], (up), MAC: 74:D8:3E:D3:7D:7C, Speed: 54 Mbit/s, In: 6.82 MB/s (warn/crit at 3.38 MB/s/4.05 MB/s) (101.10%/6.75 MB/s) **CRIT**, Out: 122 kB/s

Details

[wlo1]
Operational state: up
MAC: 74:D8:3E:D3:7D:7C
Speed: 54 Mbit/s
In: 6.82 MB/s (warn/crit at 3.38 MB/s/4.05 MB/s) (101.10%/6.75 MB/s) **CRIT**
Out: 122 kB/s
Errors in: 0%
Discards in: 0 packets/s
Multicast in: 0 packets/s
Broadcast in: 0 packets/s
Unicast in: 4625.92 packets/s
Non-unicast in: 0 packets/s
Errors out: 0%
Discards out: 0 packets/s
Multicast out: 0 packets/s
Broadcast out: 0 packets/s
Unicast out: 1099.27 packets/s
Non-unicast out: 0 packets/s

Service Perf-O-Meter

54.6 Mbit/s / 976 kbit/s



	Minimum	Maximum	Average	Last
	16.6 kbit/s	50.9 Mbit/s	7.09 Mbit/s	50.9 Mbit/s
	15.7 kbit/s	918 kbit/s	221 kbit/s	918 kbit/s
				27.0 Mbit/s
				32.4 Mbit/s



Critical (In)


Configured alert based on speed of interface



Network statistics and flows of build-fr-001.lan.iribn20.com

Monitor > Overview > All hosts > build-fr-001.lan.iribn20.com > Services of Host > Network statistics

Host Display Help   

Host	Traffic	Packets	Ports	Peers	Apps	Flows	Engaged Host	Past Host	Past Flow
IP address			10.200.8.10						View data in ntopng
Name			 build-fr-001.lan.iribn20.com						
Engaged Alerts			0						
Score			0						
Active alerted flows			0						
First Seen			2023-09-09 02:02:33 [11 d ago]						
Last Seen			2023-09-20 13:56:28 [1.00 s ago]						
Sent vs Received Traffic Breakdown			<div><div>Sent</div><div>Rcvd</div></div>						
Traffic Sent			392,363,949 Pkts / 753.30 GiB						
Traffic Received			691,852,833 Pkts / 2.24 TiB						
Additional Host Names			build-fr-001.lan.iribn20.com (DNS Resolution)						
							As client	As server	
	Active			66			0		
	Total			1128056			45477		
				1159			233		
				0			0		
Peers	Active			18			1		



Investigate via ntop integration: Host overview



Network statistics and flows of [redacted]

Monitor > Overview > All hosts > [redacted] > Services of Host > Network statistics

Host Display Help

tcp://127.0.0.1:5556 VLAN 0 2.62 Gbit/s 3 Alerts 34 Flow Alerts 113 919 665 Flows

Host	Traffic	Packets	Ports	Peers	Apps	Flows	Engaged Host	Past Host	Past Flow
Total Unique Hosts	Contacts	Hosts Contacted (as Client)		1872	Hosts Contacts (as Server)		14	View data in ntopng	

Protocol Overview



TCP

Protocol	Sent	Received	Breakdown	Total	
TCP	753.22 GiB	2.24 TiB	<div><div>Sent</div><div>Rcvd</div></div>	2.97 TiB	99.99%
UDP	65.77 MiB	122.70 MiB	<div><div>Sent</div><div>Rcvd</div></div>	188.47 MiB	0.01%









Investigate via ntop integration: Host traffic



Network statistics and flows of [redacted]

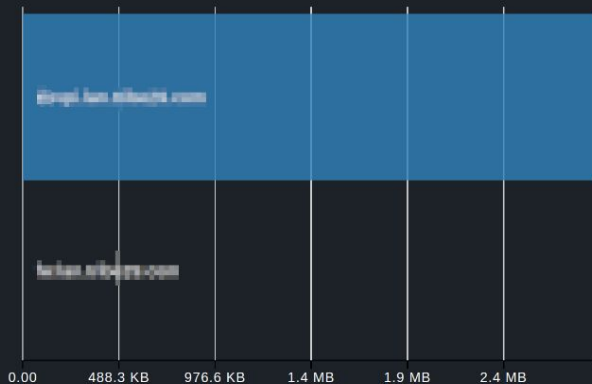
Monitor > Overview > All hosts > [redacted] > Services of Host > Network statistics

Host Display Help   

 tcp://127.0.0.1:5556  VLAN 0 2.62 Gbit/s  3 Alerts  34 Flow Alerts  113  919 665 Flows

Host Traffic Packets Ports Peers Apps Flows Engaged Host Past Host Past Flow

[View data in ntopng](#)



Host	IP Address	Application	Traffic
[redacted]	[redacted]	TLS	2.83 MiB
[redacted]	[redacted]	[redacted]	341.00 B

Investigate via ntop integration: Host peers



Host Display Help

tcp://127.0.0.1:5556 VLAN 0 2.62 Gbit/s 3 Alerts 34 Flow Alerts 113 919 665 Flows

Host Traffic Packets Ports Peers Apps Flows Engaged Host Past Host Past Flow

Client Contacted Services 0 (TLS, HTTP and DNS names) [View data in ntopng](#)

Applications overview



Category overview



Applications Categories

Investigate via ntop integration: Host apps

	Received	Breakdown	Total	
	2.24 TiB	<div><div>Sent</div><div>Rcvd</div></div>	2.97 TiB	100.00%
	240.00 B	<div><div>Sent</div><div>Rcvd</div></div>	424.00 B	0.00%
AmazonAWS	28.41 GiB	<div><div>Sent</div><div>Rcvd</div></div>	58.45 GiB	1.92%



Network statistics and flows of

Monitor > Overview > All hosts > [redacted] > Services of Host > Network statistics

Host Display Help

tcp://127.0.0.1:5556 VLAN 0 2.62 Gbit/s 3 Alerts 34 Flow Alerts 113 919 665 Flows

Host Traffic Packets Ports Peers Apps Flows Engaged Host Past Host Past Flow

Hosts All hosts Status All flows Direction All directions Application All applications Protocol All protocols Category All categories

1 - 20 of 68 << < > >>

	Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes
Info	TLS	TCP	[redacted]	[redacted]	35.0 s	0	Server	1.08 MiB	4.71 MiB
Info	TLS	TCP	[redacted]	[redacted]	19.0 s	0	Server	1.89 MiB	4.48 MiB
Info	TLS	TCP	[redacted]	[redacted]	35.0 s	0	Server	772.82 KiB	3.30 MiB
Info	TLS	TCP	[redacted]	[redacted]	35.0 s	0	Server	771.58 KiB	3.30 MiB
Info	TLS	TCP	[redacted]	[redacted]	35.0 s	0	Server	770.40 KiB	3.29 MiB
Info	TLS	TCP	[redacted]	[redacted]	38.0 s	0	Server	489.38 KiB	2.27 MiB
Info	TLS	TCP	[redacted]	[redacted]	36.0 s	0	Server	495.30 KiB	2.18 MiB
Info	TLS	TCP	[redacted]	[redacted]	39.0 s	0	Server	64.59 KiB	314.90 KiB
Info	TLS	TCP	[redacted]	[redacted]	12.0 s	0	Server	76.48 KiB	114.72 KiB
Info	TLS	TCP	[redacted]	[redacted]	11.0 s	0	Server	82.93 KiB	114.03 KiB
Info	TLS	TCP	[redacted]	[redacted]	5.00 s	0	Server	98.54 KiB	61.59 KiB
Info	TLS	TCP	[redacted]	[redacted]	5.00 s	0	Server	85.97 KiB	53.73 KiB
Info	TLS	TCP	[redacted]	[redacted]	5.00 s	0	Server	85.94 KiB	53.71 KiB
Info	TLS	TCP	[redacted]	[redacted]	4.00 s	0	Server	107.37 KiB	53.68 KiB
Info	TLS	TCP	[redacted]	[redacted]	90 s	0	Server	2.83 KiB	31.85 KiB
Info	TLS	TCP	[redacted]	[redacted]	1.00 s	0	Server	170.80 KiB	21.35 KiB
Info	TLS	TCP	[redacted]	[redacted]	1.00 s	0	Server	170.59 KiB	21.32 KiB









Investigate via ntop integration: Host flows



Network statistics and flows of [redacted]

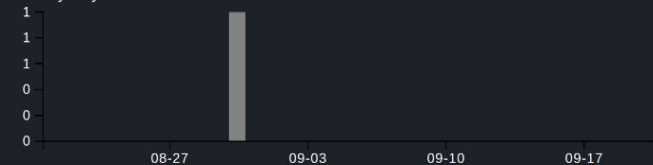
Monitor > Overview > All hosts > [redacted] > Services of Host > Network statistics

Host Display Help   

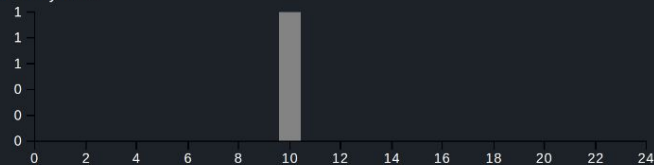
 tcp://127.0.0.1:5556  VLAN 0 2.62 Gbit/s  3 Alerts  34 Flow Alerts  113  919 665 Flows

Host Traffic Packets Ports Peers Apps Flows Engaged Host Past Host Past Flow



Filter by day



Filter by hour



[View data in ntopng](#)

Type  All Severity  All

Filter details by description

Alert details from last 31 days

Date	Duration	Severity	Alert type	Description
30.8.2023 10:19:44	01:03	warning	host_alert_tcp_syn_scan	Host [redacted] is under a SYN scan [3045 > 256 SYN received]



Investigate via ntop integration: Host alerts





Top Talkers

Monitor > Network statistics > Top Talkers

Dashboard Add Dashboards Display Help

eth0 67.83 kbit/s 2 Alerts 99 Flow Alerts 12 10 9 Devices 157 Flows

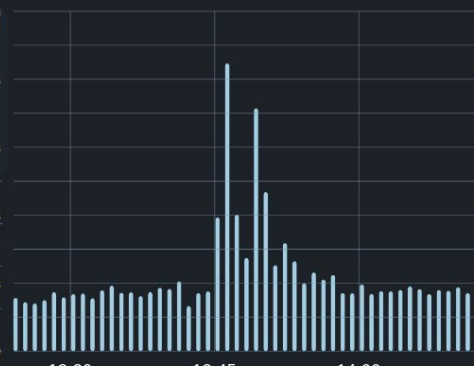
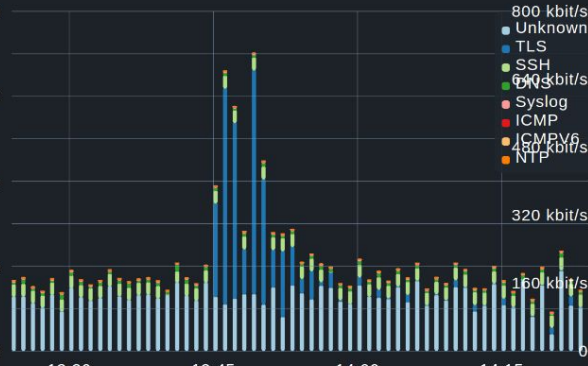
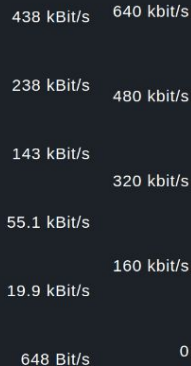
Top local talkers

Actual traffic

Top application traffic: last hour view

Network interfaces: last hour view

192.168.1.1
www.fda.hhs.gov
www.fda.hhs.gov
www.fda.hhs.gov
192.168.1.1
192.168.1.1



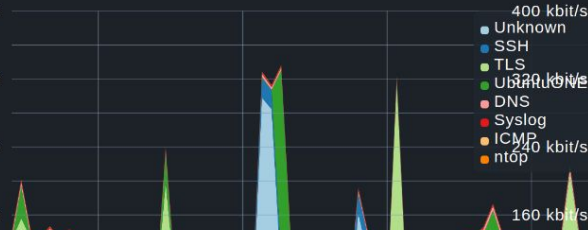
Top remote destinations

Actual traffic

Top application traffic: last day view

Network interfaces: last day view

www.fda.hhs.gov
192.168.1.1
192.168.1.1
192.168.1.1



Investigate via ntop integration: Top talkers



Alerts

Monitor > Network statistics > Alerts



Dashboard Add Dashboards Display Help



eth0 39.09 kbit/s 2 Alerts 120 Flow Alerts 12 7 8 Devices 206 Flows



Engaged Host

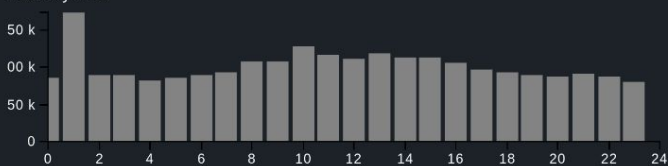
Past Host

Past Flow

Filter by day



Filter by hour



Type All Severity error

Filter details by description Alert details from last 31 days

1 - 20 of 2437017 << < > >>

Date	Severity	Alert type	Score	Description
20.9.2023 14:21:46	warning	alert_known_proto_on_non_std_port	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] App. on Non-Std Port
20.9.2023 14:21:07	warning	alert_ndpi_suspicious_entropy	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] Suspicious Entropy
20.9.2023 14:21:07	warning	alert_ndpi_suspicious_entropy	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] Suspicious Entropy
20.9.2023 14:21:07	warning	alert_ndpi_suspicious_entropy	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] Suspicious Entropy
20.9.2023 14:20:48	warning	alert_known_proto_on_non_std_port	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] App. on Non-Std Port
20.9.2023 14:20:47	warning	alert_known_proto_on_non_std_port	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] App. on Non-Std Port
20.9.2023 14:20:46	warning	alert_known_proto_on_non_std_port	50	192.168.1.100 [192.168.1.100] -> 192.168.1.100 [192.168.1.100] App. on Non-Std Port

Investigate via ntop integration: Alerts



Flows

Monitor > Network statistics > Flows

Dashboard Add Dashboards Display Help

tcp://127.0.0.1:5556 3.64 Gbit/s 3 Alerts 52 Flow Alerts 120 1043 1683 Flows

Hosts All hosts Status All Alerted Direction All directions Application All applications Protocol All protocols

Category RemoteAccess

	Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes
Info	SSH	TCP	red 128.0.0.1:5556	per for 80.1.1.1:8080	<1s	10	Client	0 B	50.00 B
Info	SSH	TCP	red 128.0.0.1:5556	testing client: 80.1.1.1:8080	<1s	10	Client	0 B	50.00 B
Info	SSH	TCP	red 128.0.0.1:5556	red 128.0.0.1:5556	<1s	10	Client	0 B	50.00 B
Info	SSH	TCP	red 128.0.0.1:5556	red 128.0.0.1:5556	<1s	10	Client	0 B	50.00 B



Investigate via ntop integration: Flows

Main purpose of the ntop & Checkmk integration



Single pane of glass

Relevant ntop data directly integrated into Checkmk.
Filters to work with huge amounts of ntop data.



Quick access to further information

Deep links, both to Checkmk and ntop.

Learnings from building a ntop integration



Some learnings for developers



- ⬢ There are API differences between commercial and free ntop
 - ⬢ Make this clear to your users and testers, what is required

- ⬢ Build it early on for multiple API calls to get data - Retrieving, e.g. all engaged alerts not possible via one API call – we used multiple API calls with categories to get all engaged alerts
- ⬢ Performance can become a huge topic.
 - ⬢ Our own environment is 'very small' - no performance problems (after we upgraded to ClickHouse DB)
 - ⬢ Amount of data even in 'smaller environments' quickly explodes: 7 TB per day
 - ⬢ Consider the amount of data of larger environments before you build such an integration – we had to invest a lot of time post-release to solve performance issues

- ⬢ Definitely work with pagination due to amount of data available in ntop
 - ⬢ A definite number of items returned by the API (e.g. if you want alerts from past time to present time)

- ⬢ Work with caching!

ntop REST API can do more than meets the eye



GET /lua/rest/v2/get/flow/alert/list.lua

Get flow alerts list

- **Description:** Get flow alerts list
- **Produces:** ['application/json']

Parameters

Name	Position	Description
ifid	query	Interface identifier
epoch_begin	query	Start time (epoch)
epoch_end	query	End time (epoch)
alert_id	query	Alert identifier (format: 'id;eq', where
severity	query	Severity identifier (format: 'id;eq', where
score	query	Score (format: 'id;eq', where 'id' is the
ip_version	query	IP version (format: 'id;eq', where 'id' is
ip	query	IP (format: 'id;eq', where 'id' is the id a
cli_ip	query	Client IP (format: 'id;eq', where 'id' is t
srv_ip	query	Server IP (format: 'id;eq', where 'id' is

This is also possible.
3 parameters are NOT documented :-)

.../list.lua?start=0&length=10&ifid=2&status=historical

Thanks for the ntop team!
Very helpful. Very resourceful. Very responsive!

Questions?
Thank you!



Checkmk GmbH
Kellerstraße 27
81667 München
Germany

Web — checkmk.com