COMMVAULT®

Last line of defense

Data Protection Redefined

Ernst Christian Dvorak
Arnold Schwingenschlögl

We’re the world’s leader in data protection.

Over 100K of the world’s leading organizations

depend on Commvault to protect more than 3.8 exabytes of cloud data.

We help them:

- Continuously run their businesses
- Secure, defend and recover data
- Seize new business opportunities

A1

BUNDESRECHENZENTRUM BRZ

AKH Die menschliche Größe

SPAR

Adobe

SONY

BARON

DOW JONES

Telefónica

RAUCH

AuRep Austrian Reporting Services GmbH

UniCredit Leasing

Österreichische Nationalbibliothek

NTT DATA

adidas

AstraZeneca

HarperCollinsPublishers

orange Business Services

Austrian

Data is everywhere

(And harder to protect than ever before)

89% of companies are multi-cloud[1]

50% of enterprise-critical data will be outside a company's cloud[2]

60% of companies lack complete visibility into where data reside[3]

COMMVAULT

1. Flexera State of the Cloud Report 2023, 2.Gartner 12 Data and Analytics Trends to Keep on Your Radar,
3. 5th Annual Nutanix Enterprise Cloud Index

Skyrocketing cybercrime is fueling risk.

Commvault is the only provider with products to protect the full data protection lifecycle.

Early Warning

Threat Scanning

Risk Analysis

Backup & Recovery

eDiscovery & Compliance

Immutable Storage

COMMVAULT'S UNIFIED PLATFORM

Secure

Only Commvault offers ubiquitous recovery across all hybrid workloads – the result is the highest level of business continuity across enterprise data

Defend

Only Commvault provides real-time visibility into cyber and other risks to your data – across production and backup environments – to minimize data loss

Recover

Only Commvault offers the unmatched choice of SaaS, software, or appliance delivery, with flexible storage options to optimize cost and performance

Metallic® DMaaS

Future-proof data management – as a simple, cloud-native solution.

SaaS Applications

Unlimited storage included.

Metallic®
Office 365 Backup†
For Exchange, Teams, SharePoint, OneDrive, Project

Metallic®
Backup for Microsoft Dynamics 365
For CRM applications

Metallic®
Salesforce Backup
For production and sandbox environments

Hybrid Cloud Data Protection

Metallic® Recovery Reserve™ available as a storage target.

Metallic®
VM & Kubernetes Backup
For VMware, Hyper-V, VMC, Azure VM, AVS, Oracle Container Engine for Kubernetes (OKE), Amazon EC2, OCI VM

Metallic®
Database Backup
For Microsoft SQL Server, Azure SQL Server, Azure MySQL, Azure MariaDB, Azure PostgreSQL, Azure Cosmos DB, Oracle, Oracle RAC, Oracle Database Cloud Service (DBCS), Oracle ExaData Database Service on OCI / on premises, SAP HANA, Amazon RDS, Amazon DynamoDB, Amazon DocumentDB Amazon Redshift

Metallic®
File & Object Backup
For Windows Server, Linux/UNIX, Azure Blob & Files, OCI Object Storage, Amazon S3

+

Cloud Storage

Secure cloud storage.

Metallic®
Recovery Reserve™
For long and short-term retention

Microsoft Azure

ORACLE

Ransomware Detection

Integrated cyber deception.

Metallic®
ThreatWise™
For early warning into threats

Endpoints

Unlimited storage included.

Metallic®
Endpoint Backup†
For laptops and desktops

Active Directory

FREE w/any paid Metallic subscription.

Metallic®
Active Directory Backup
For Azure & Microsoft AD

†eDiscovery available

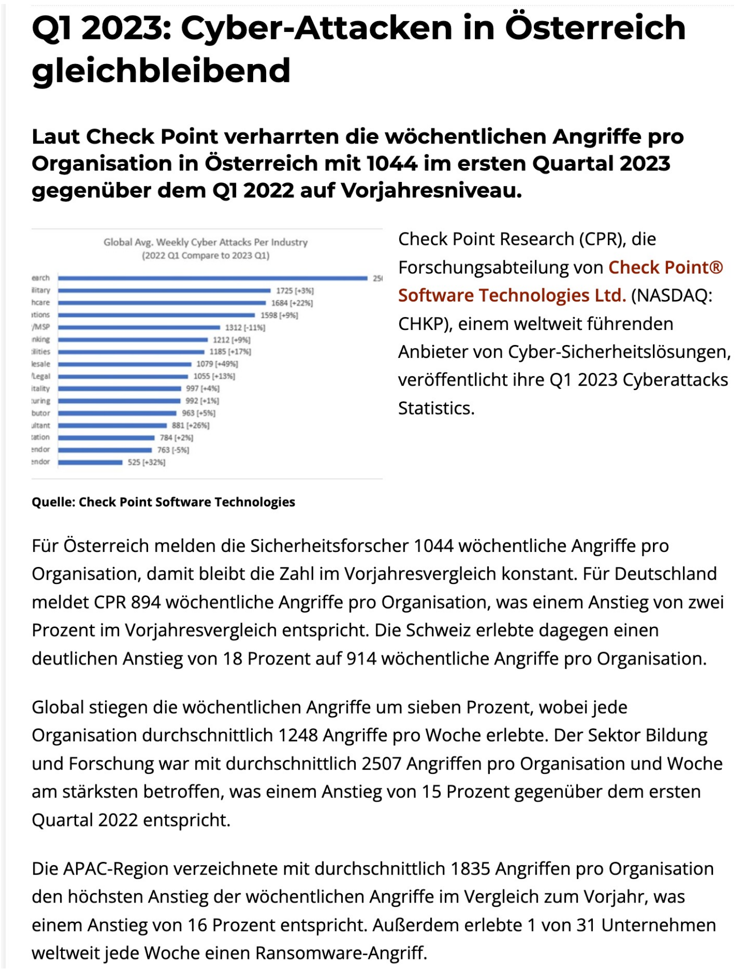
Metallic Government Cloud also available (FedRAMP High, hosted on Azure Government)

Industry-leading SaaS, from the minds of Commvault

metallic
A Commvault Venture

COMMVAULT

75 % der Unternehmen, die mit Ransomware infiziert wurden, verwendeten eine aktuelle Endpoint-protection



Q1 2023: Cyber-Attacken in Österreich gleichbleibend

Laut Check Point verharrten die wöchentlichen Angriffe pro Organisation in Österreich mit 1044 im ersten Quartal 2023 gegenüber dem Q1 2022 auf Vorjahresniveau.

Check Point Research (CPR), die Forschungsabteilung von Check Point® Software Technologies Ltd. (NASDAQ: CHKP), einem weltweit führenden Anbieter von Cyber-Sicherheitslösungen, veröffentlicht ihre Q1 2023 Cyberattacks Statistics.

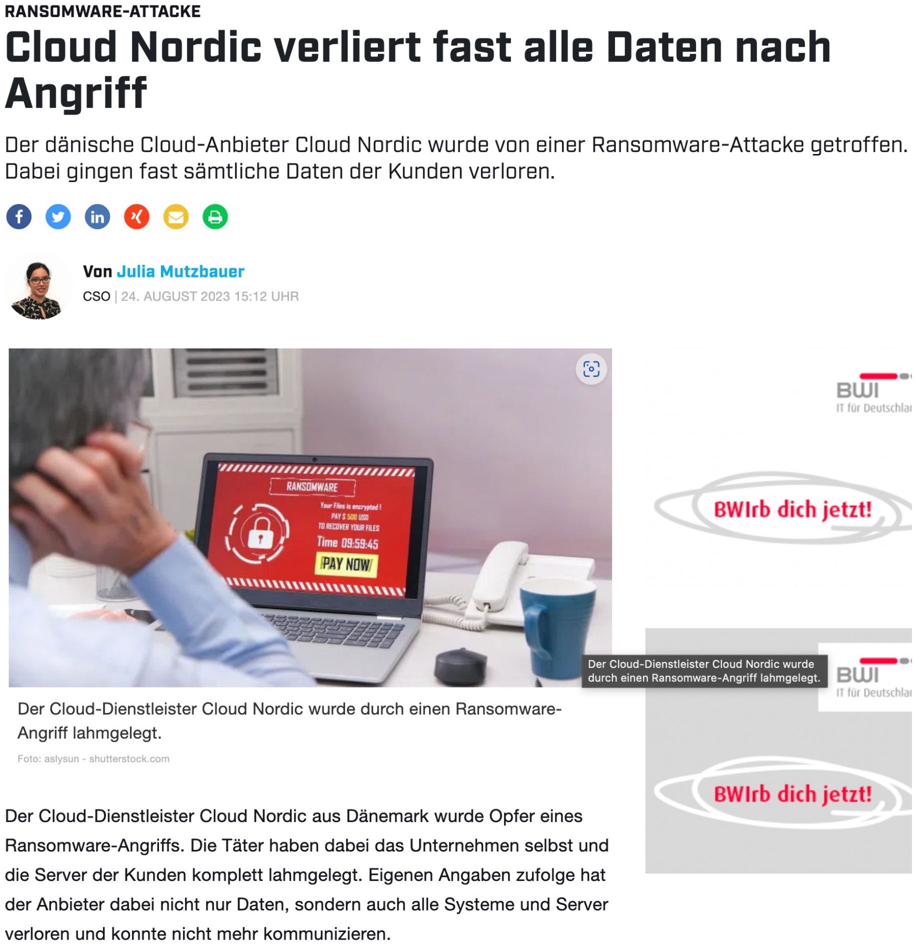
Quelle: Check Point Software Technologies

Für Österreich melden die Sicherheitsforscher 1044 wöchentliche Angriffe pro Organisation, damit bleibt die Zahl im Vorjahresvergleich konstant. Für Deutschland meldet CPR 894 wöchentliche Angriffe pro Organisation, was einem Anstieg von zwei Prozent im Vorjahresvergleich entspricht. Die Schweiz erlebte dagegen einen deutlichen Anstieg von 18 Prozent auf 914 wöchentliche Angriffe pro Organisation.

Global stiegen die wöchentlichen Angriffe um sieben Prozent, wobei jede Organisation durchschnittlich 1248 Angriffe pro Woche erlebte. Der Sektor Bildung und Forschung war mit durchschnittlich 2507 Angriffen pro Organisation und Woche am stärksten betroffen, was einem Anstieg von 15 Prozent gegenüber dem ersten Quartal 2022 entspricht.

Die APAC-Region verzeichnete mit durchschnittlich 1835 Angriffen pro Organisation den höchsten Anstieg der wöchentlichen Angriffe im Vergleich zum Vorjahr, was einem Anstieg von 16 Prozent entspricht. Außerdem erlebte 1 von 31 Unternehmen weltweit jede Woche einen Ransomware-Angriff.

Q1 2023: Cyber-Attacken in Österreich gleichbleibend (itwelt.at)



RANSOMWARE-ATTACKE

Cloud Nordic verliert fast alle Daten nach Angriff

Der dänische Cloud-Anbieter Cloud Nordic wurde von einer Ransomware-Attacke getroffen. Dabei gingen fast sämtliche Daten der Kunden verloren.

Von Julia Mutzbauer
CSO | 24. AUGUST 2023 15:12 UHR

Der Cloud-Dienstleister Cloud Nordic wurde durch einen Ransomware-Angriff lahmgelegt.

Foto: aslysun - shutterstock.com

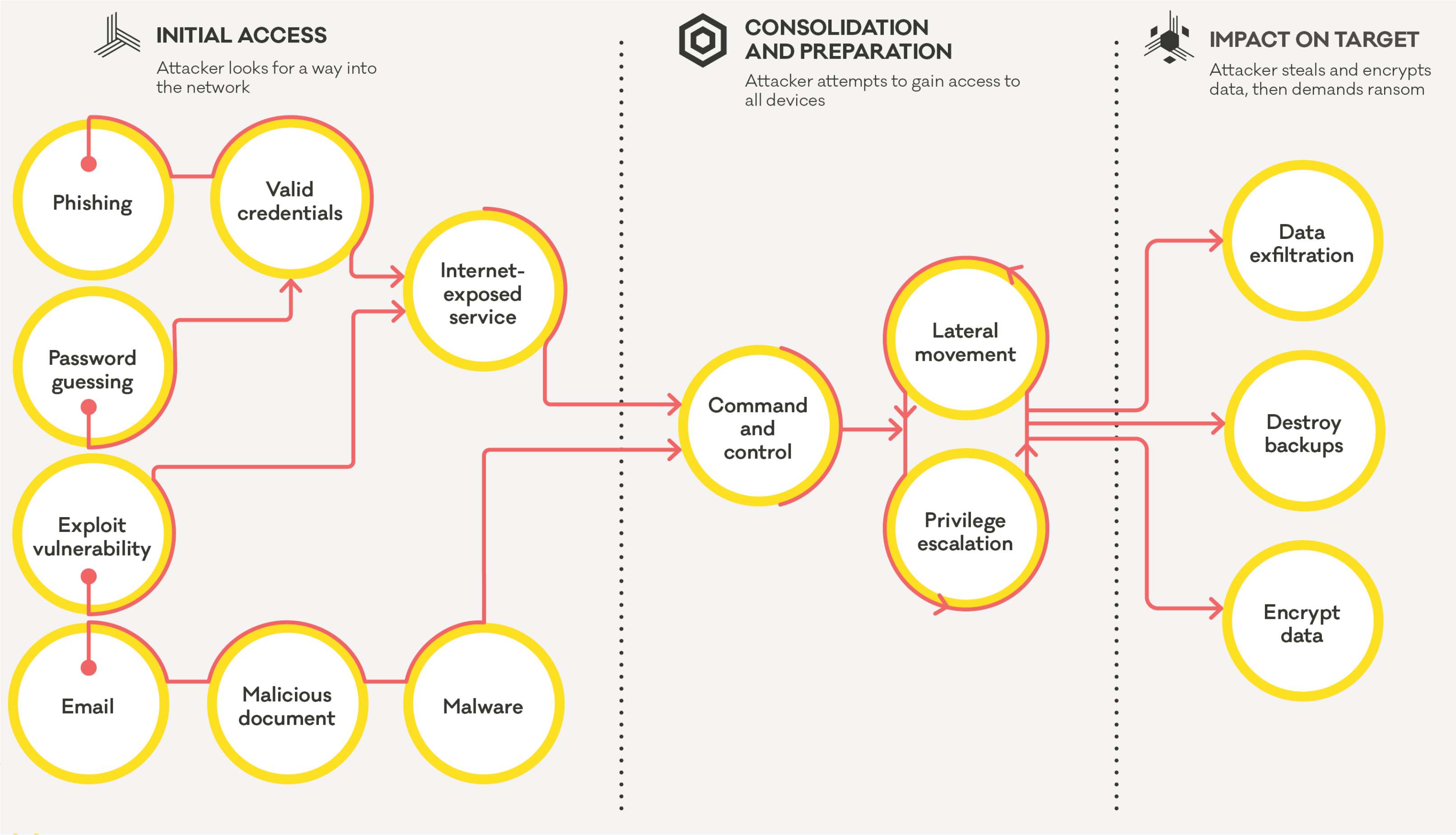
Der Cloud-Dienstleister Cloud Nordic aus Dänemark wurde Opfer eines Ransomware-Angriffs. Die Täter haben dabei das Unternehmen selbst und die Server der Kunden komplett lahmgelegt. Eigenen Angaben zufolge hat der Anbieter dabei nicht nur Daten, sondern auch alle Systeme und Server verloren und konnte nicht mehr kommunizieren.

Ransomware-Attacke: Cloud Nordic verliert fast alle Daten nach Angriff - CSO (csoonline.com)

- https://phoenixnap.com/blog/ransomware-statistics-facts

Ransomware lifecycle

- Cyberthreats continuously infiltrate and spread
- 20 – 50 day dwell time*
- Backups are continuous



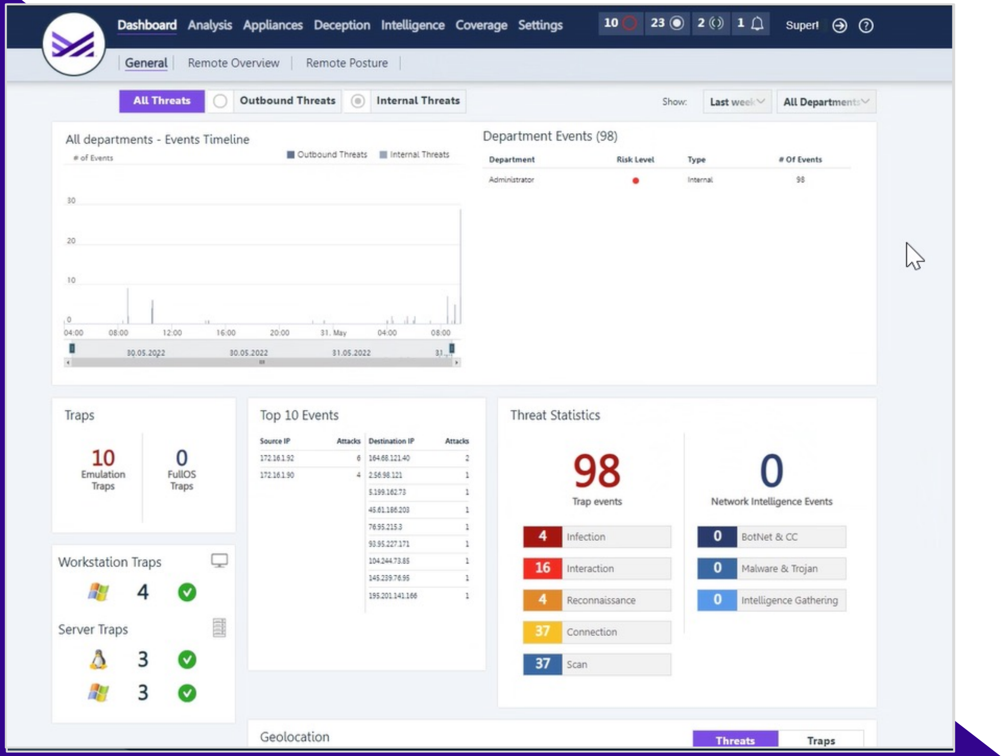
20 – 50+ day dwell time*

- *https://www.sophos.com/en-us/press-office/press-releases/2022/06/attacker-dwell-time-increased-by-36-percent-sophos-active-adversary-playbook-2022-reveals

COMMVAULT

Metallic® ThreatWise^{TM}

Integrated Cyber Deception



Department Events (98)

Department	Risk Level	Type	# Of Events
Administrator	●	Internal	98

Traps

10 Emulation Traps

0 FullOS Traps

Workstation Traps

4 ✓

Server Traps

3 ✓

3 ✓

Top 10 Events

Source IP	Attacks	Destination IP	Attacks
172.16.1.92	6	164.68.121.40	2
172.16.1.90	4	2.56.98.121	1
		5.199.162.73	1
		45.61.186.203	1
		76.95.215.3	1
		93.95.227.171	1
		104.244.73.85	1
		145.239.76.95	1
		195.201.141.166	1

Threat Statistics

98 Trap events

4	Infection
16	Interaction
4	Reconnaissance
37	Connection
37	Scan

0 Network Intelligence Events

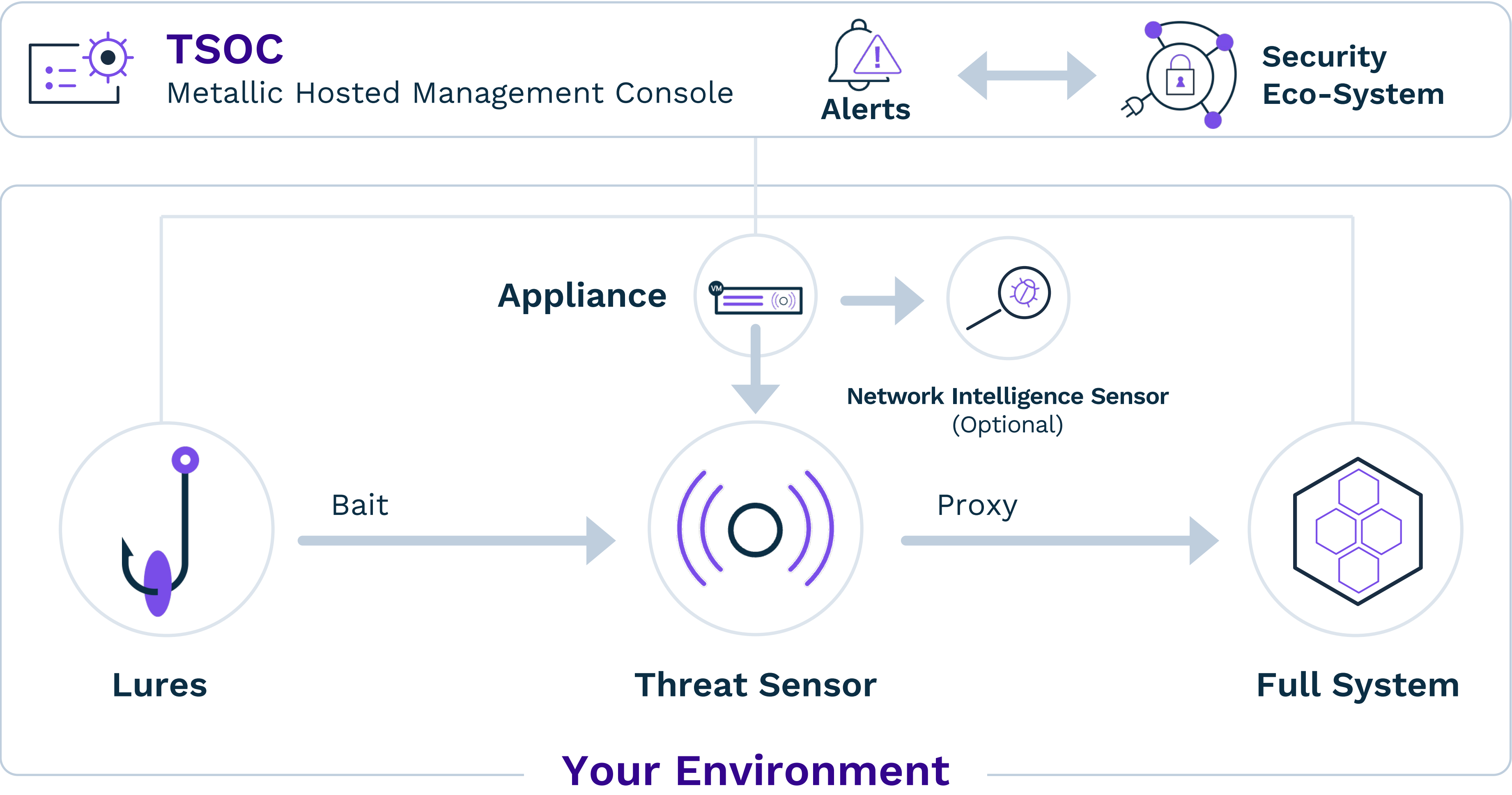
0	BotNet & CC
0	Malware & Trojan
0	Intelligence Gathering

Early Warning Ransomware Detection

- **Intelligent decoys** that mimic and behave-like legitimate assets
- **Precise alerts** to pinpoint threats without false-positives or alert-fatigue
- **Rapid scalability** to protect entire environments and applications in seconds
- **Simple SaaS delivery** with flexible, lightweight architecture

Data protection starts *before* you're compromised.

High Level Architecture



metallic® A Commvault Venture

Security Eco-System

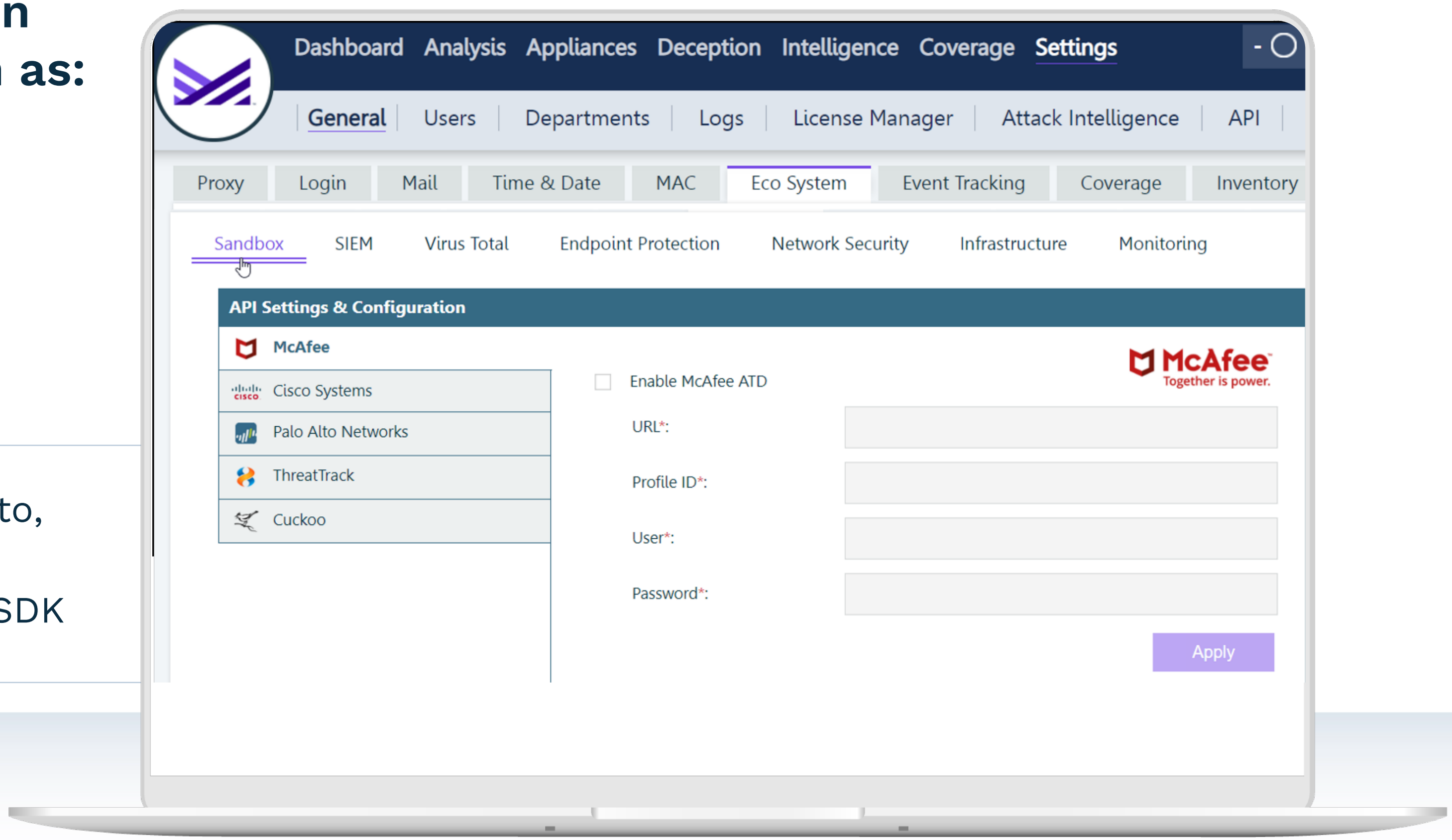
Infrastructure Components

The Eco-System allows easy integration with third-party security systems such as:

- SIEM (via SYSLOG), this is most common request for SOC integration
- Firewall
- NAC
- Virus Total
- Sandbox

Common Vendors such as McAfee, Cisco, PaloAlto, Forescout and ODBC are built-in the TSOC

Further integration can be achieved via the API/SDK



□ Enable McAfee ATD

URL*:

Profile ID*:

User*:

Password*:

Thank You!

metallic®

A Commvault Venture

Metallic® ThreatWise™

Key Features & Benefits

Feature	Benefits
Imitate real assets with highly intelligent threat sensors	• Hiding real assets in the crowd for risk mitigation
Real-time alerting	• Ransomware risk mitigation before data impact
Divert bad actors into engaging false resources	• Grow time to impact of bad actor
Agentless deployment	• Suitable for any environment
Provide insights into active and latent threats	• Uncover vesting bad actors on the network
High fidelity alerting	• Accurate alerts with close to 0 false-positives
Mass deployment of Threat Sensors	• Deploy and scale in seconds
Threat Sensors invisible for legit users	• Seamless without business disruption
Integration with top security provider (SIEM, Sandbox, EDR, etc.)	• Accelerating time to remediate and IT collusion (IT&ITSec Convergence)
Lightweight architecture	• Low resources footprint

metallic®
A Commvault Venture

What is Metallic® ThreatWise™?

Early Warning Ransomware Detection

Dilute the Attack Surface

Flood environments with flawless replicated assets, divert threats before they effect data

Expose Silent Threats

Uncover attacks early with real-time high-fidelity alerts before they reach your data

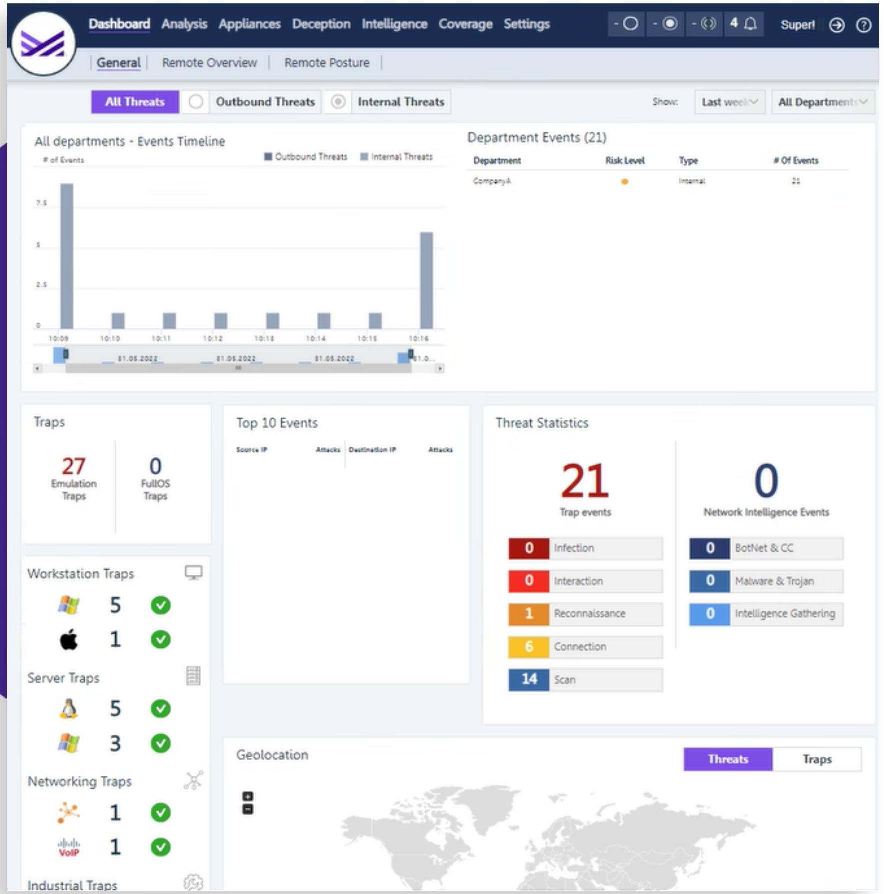
Accelerate Recovery

Drive remediation efforts, limit exposure windows, and extract bad actors

TSOC

ThreatWise™ Security Operations Console

Metallic®
Control Plane



All departments - Events Timeline

Department Events (21)

Department	Risk Level	Type	# Of Events
CompanyA	●	Internal	21

Traps

27 Emulation Traps

0 FullOS Traps

Top 10 Events

Source IP	Attacks	Destination IP	Attacks

Threat Statistics

21 Trap events

0	Infection
0	Interaction
1	Reconnaissance
6	Connection
14	Scan

0 Network Intelligence Events

0	BotNet & CC
0	Malware & Trojan
0	Intelligence Gathering

Workstation Traps

5 ✓

1 ✓

Server Traps

5 ✓

3 ✓

Networking Traps

1 ✓

VoIP 1 ✓

Industrial Traps

Geolocation

Manage ThreatWise™ appliances, deploy threat sensors and view events

Point of Integration to Security Eco-System such as SIEM, Firewall, NAC and Sandboxes

Accessed via **Metallic Hub/Control Plane**

metallic®
A Commvault Venture

Appliance

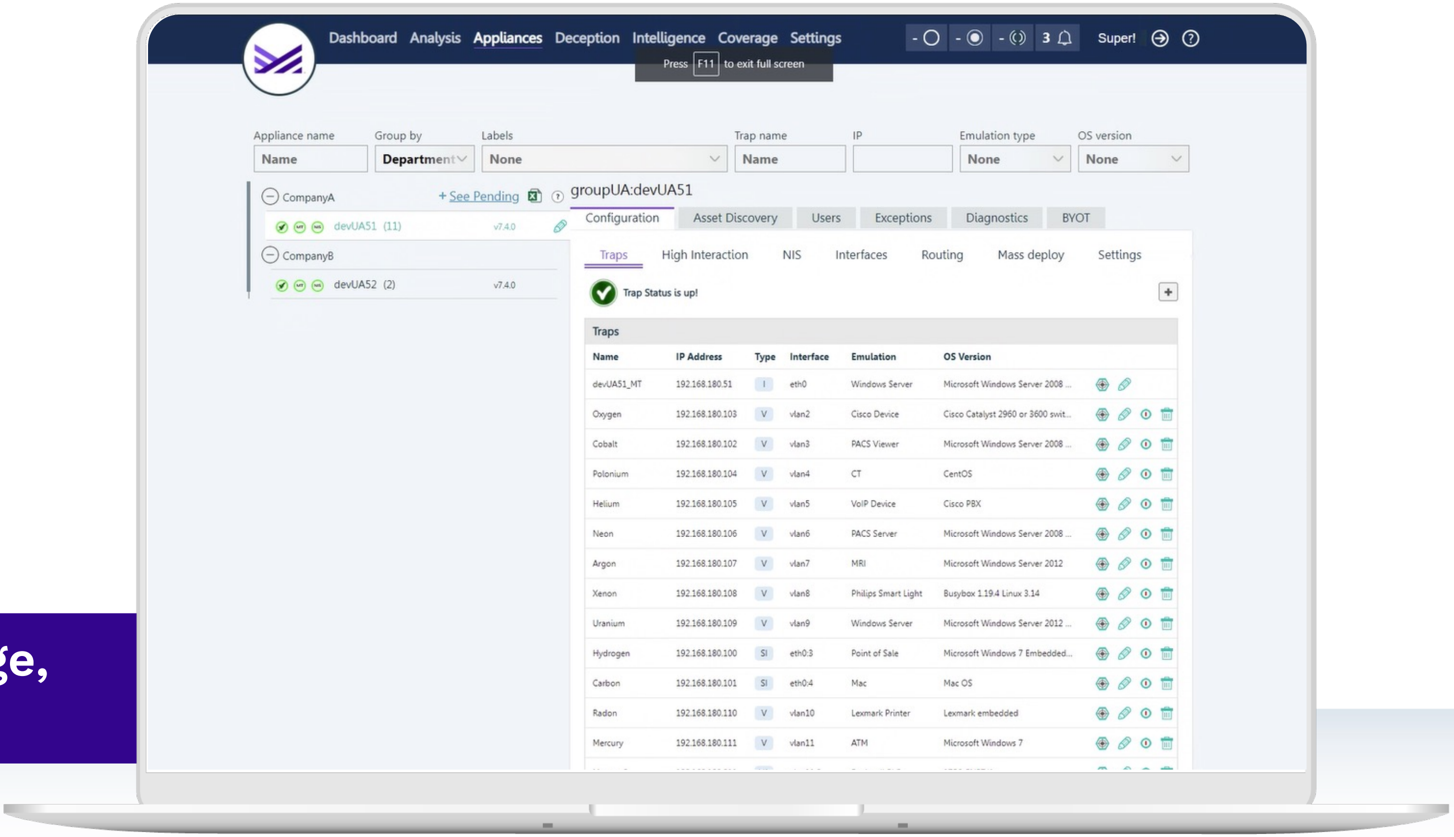
Infrastructure Components

A virtual machine deployed to a hypervisor provided by the customer

(VMware ESXi, Hyper-V, KVM, AWS AMI, Azure)

- Each Appliance supports 512 individual Threat Sensors
- Seamless deployment with Metallic® ThreatWise™ templates
- **Security is enhanced** by using outbound communication to the TSOC

To increase surface area coverage, deploy more appliances



Appliance name: Name
Group by: Department
Labels: None
Trap name: Name
IP:
Emulation type: None
OS version: None

CompanyA
devUA51 (11) v7.4.0
CompanyB
devUA52 (2) v7.4.0

groupUA:devUA51

Trap Status is up!

Traps

Name	IP Address	Type	Interface	Emulation	OS Version
devUA51_MT	192.168.180.51	I	eth0	Windows Server	Microsoft Windows Server 2008 ...
Oxygen	192.168.180.103	V	vlan2	Cisco Device	Cisco Catalyst 2960 or 3600 swit...
Cobalt	192.168.180.102	V	vlan3	PACS Viewer	Microsoft Windows Server 2008 ...
Polonium	192.168.180.104	V	vlan4	CT	CentOS
Helium	192.168.180.105	V	vlan5	VoIP Device	Cisco PBX
Neon	192.168.180.106	V	vlan6	PACS Server	Microsoft Windows Server 2008 ...
Argon	192.168.180.107	V	vlan7	MRI	Microsoft Windows Server 2012
Xenon	192.168.180.108	V	vlan8	Philips Smart Light	Busybox 1.19.4 Linux 3.14
Uranium	192.168.180.109	V	vlan9	Windows Server	Microsoft Windows Server 2012 ...
Hydrogen	192.168.180.100	SI	eth0:3	Point of Sale	Microsoft Windows 7 Embedded...
Carbon	192.168.180.101	SI	eth0:4	Mac	Mac OS
Radon	192.168.180.110	V	vlan10	Lexmark Printer	Lexmark embedded
Mercury	192.168.180.111	V	vlan11	ATM	Microsoft Windows 7

metallic® A Commvault Venture

Lures

Infrastructure Components

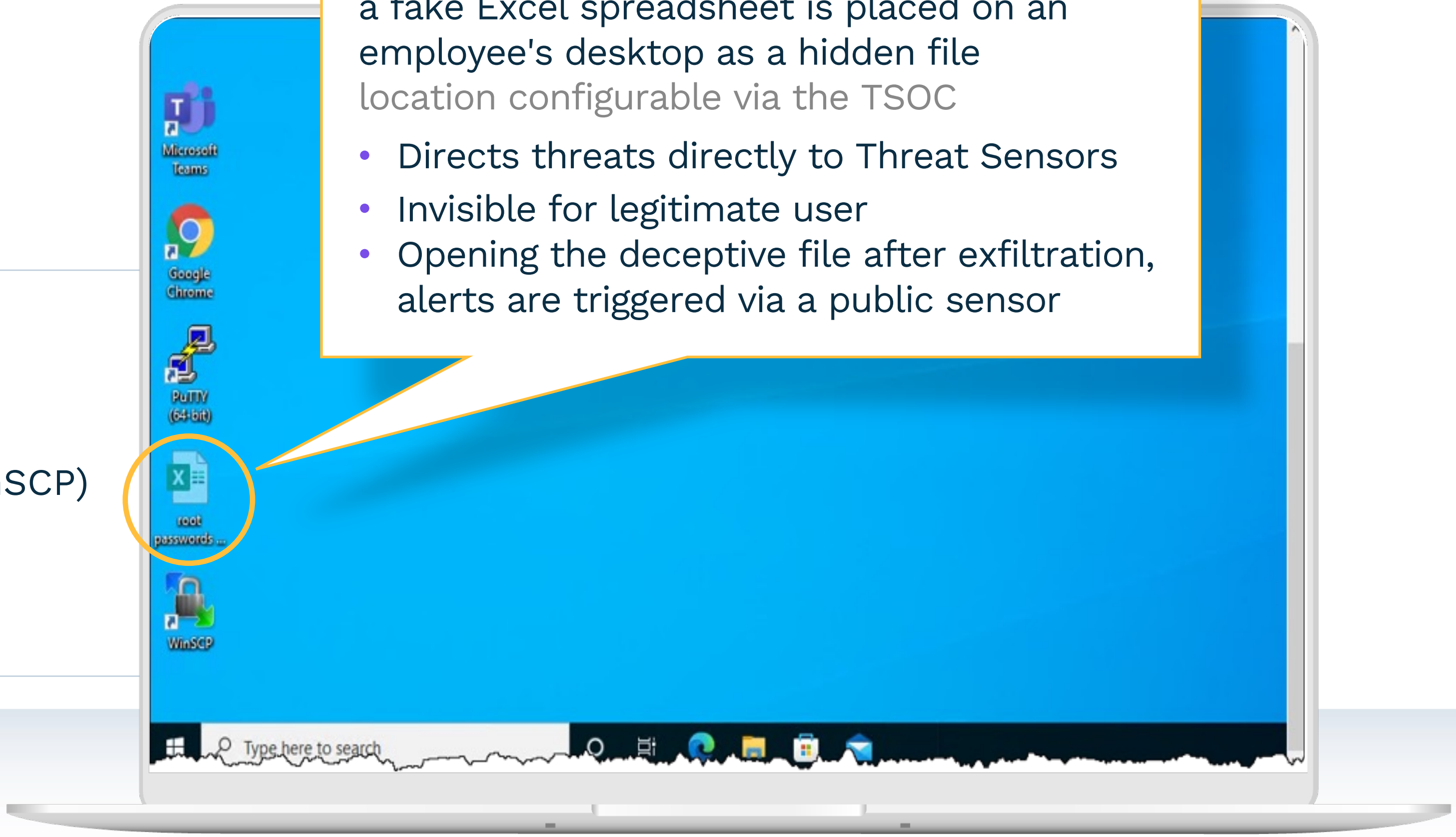
Lures are agentless pieces of data

They lure attackers in and direct them to the Threat Sensors

- Deployed on endpoints or strategic points

Lures include

- Cached credentials
- Deceptive files (Word or Excel files)
- Fake SMB drives
- Browsing history
- Entries to HOSTS file
- Stored sessions (e.g., RDP Shortcut, SSH, Putty and WinSCP)
- Active Directory



a fake Excel spreadsheet is placed on an employee's desktop as a hidden file
location configurable via the TSOC

- Directs threats directly to Threat Sensors
- Invisible for legitimate user
- Opening the deceptive file after exfiltration, alerts are triggered via a public sensor

metallic A Commvault Venture

Technical Prerequisites

Infrastructure Components

TSOC

VMware ESXi, Hyper-V or KVM

- 16Gb RAM
- 500Gb Disk
- 1x NIC

For latest AWS AMI and Azure specifications refer to System Requirements Guide

Appliance

VMware ESXi v5.5 or later

- 4x vCPU
- 8Gb RAM
- 40Gb Disk
- 4x NIC

For latest AWS AMI and Azure specifications refer to System Requirements Guide

Full System

Windows VM

- 4Gb RAM

Running any of the following:

- Windows 10
- Windows Server 2012, 2016, 2019

Surface Area Coverage

Mitigating Cyber Risk

More Threat Sensors = Less Risk

Hide in a crowd

- Reduce Threat Event Frequency by reducing Contact Frequency w/ Metallic® ThreatWise™

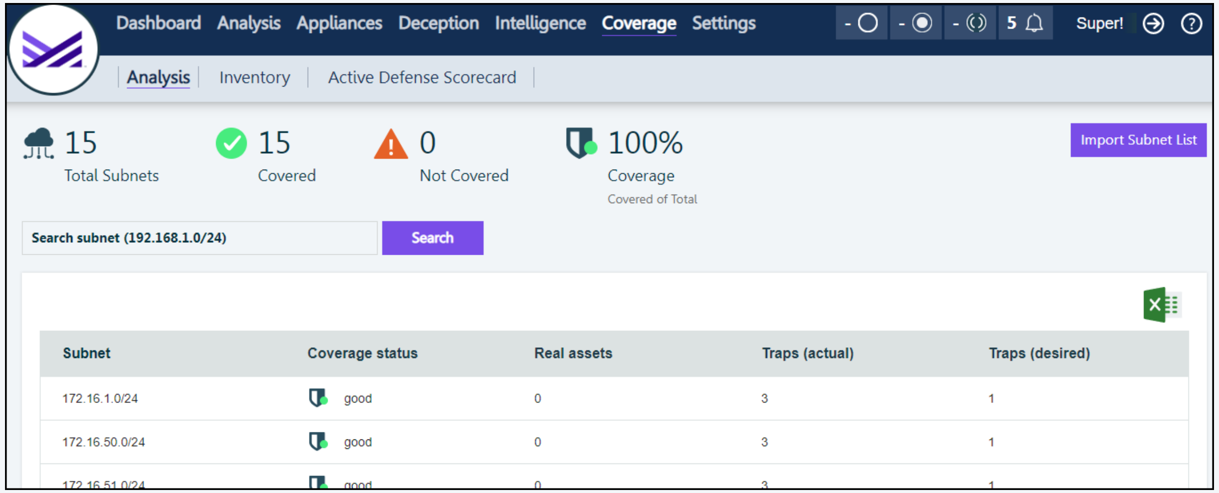
Best Practices for optimal coverage

Validate your deployment

View the effectiveness of your deception deployment

✓ 15-20% Surface Area Coverage of subnet

✓ Active Defence Score Card (mapping to TTPs of MITRE ATT&CK)



15 Total Subnets

15 Covered

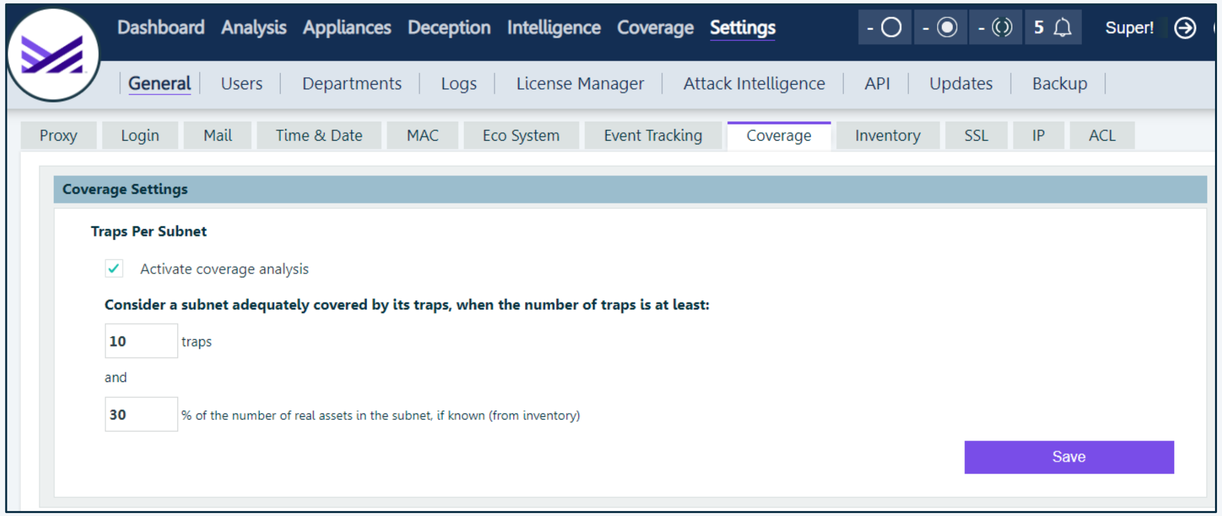
0 Not Covered

100% Coverage

Covered of Total

Search subnet (192.168.1.0/24)

Subnet	Coverage status	Real assets	Traps (actual)	Traps (desired)
172.16.1.0/24	good	0	3	1
172.16.50.0/24	good	0	3	1
172.16.51.0/24	good	0	3	1



Coverage Settings

Traps Per Subnet

☑ Activate coverage analysis

Consider a subnet adequately covered by its traps, when the number of traps is at least:

10 traps

and

30 % of the number of real assets in the subnet, if known (from inventory)

metallic®
A Commvault Venture