orange Cyberdefense orange Business

Navigating the threats and winds of change

The compelling case for SASE for the Manufacturing Sector

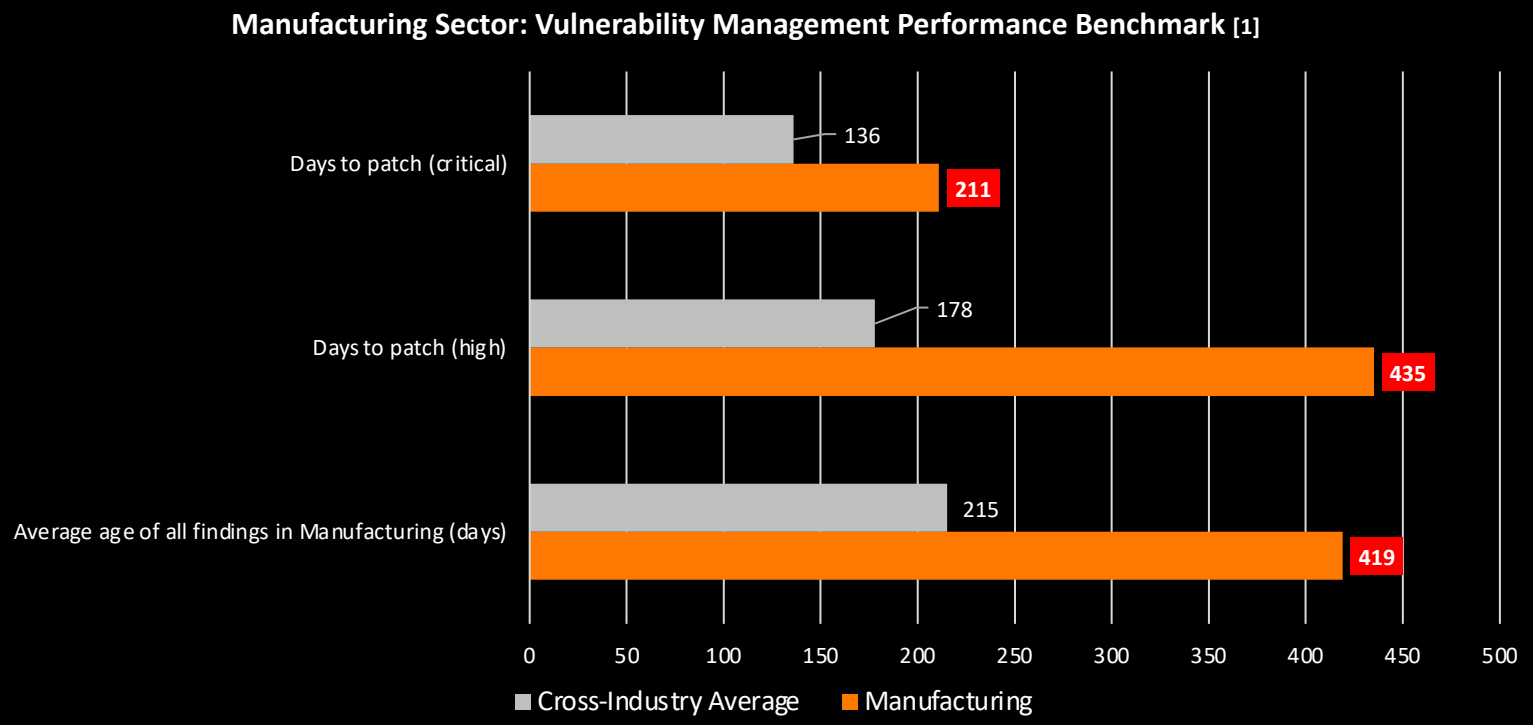
October 2023

Connecting Strategy | Security | Technology | Data |

SASE Market Trends in Manufacturing

Our Orange benchmark threat analysis of the Manufacturing Sector highlights significant vulnerability management concerns

Enterprises should look for pragmatic improvements in vulnerability management and adopt a more pro-active, risk-based posture across the merging IT – Network – Data – Security Operations



Based on 3 million vulnerability scan findings and 1 400 ethical hacking reports

Average pen testing:
Manufacturing 235 days
vs
Cross Industry Average 470 days [1]

Ratio of Vulnerability SOC findings per asset:
Manufacturing 10 times less
vs
Cross-industry Average [1]

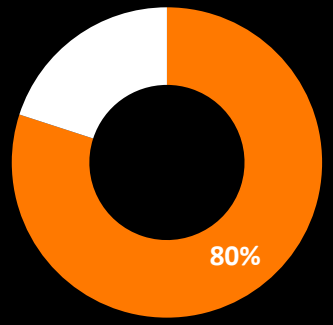
[1] Orange Cyberdefense Security Navigator 2023

2023 Independent Threat Research Trends

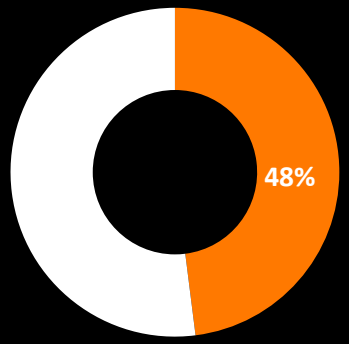
Cloud is the dominant attack surface

Ransomware & OT Cyberattacks are increasing in volume within the Manufacturing Sector

Cloud Attacks:
% of exposures observed on cloud assets [2]



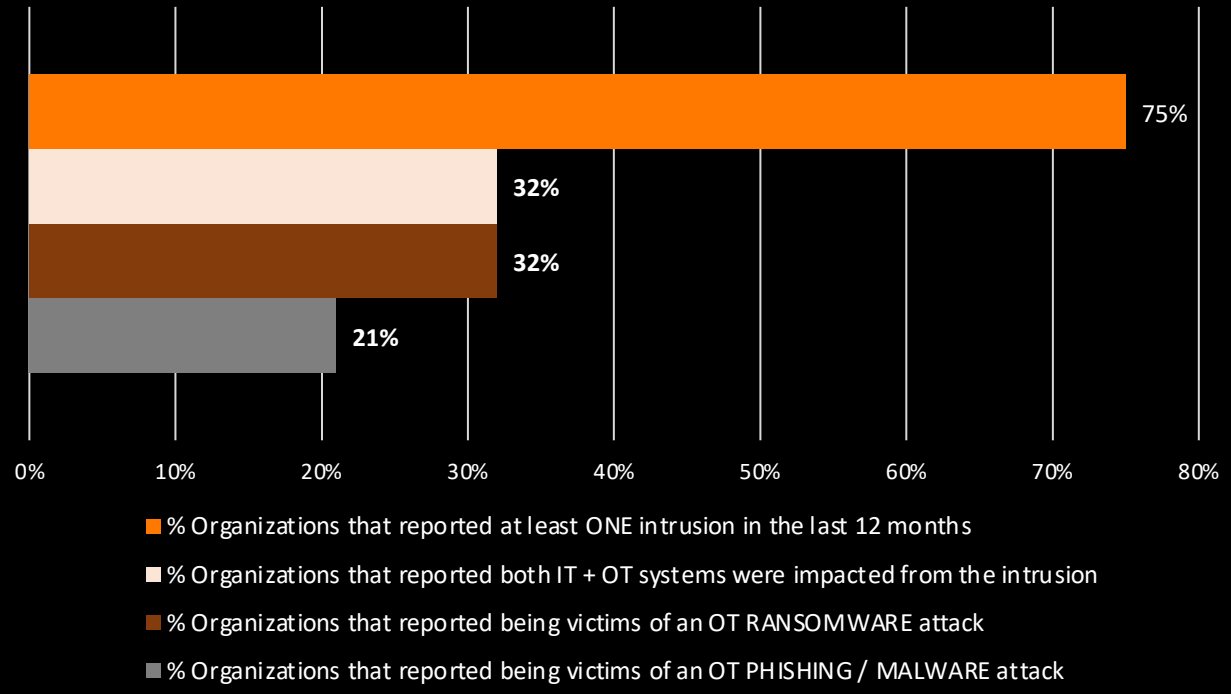
Manufacturing Sector:
% of top exposure risks on the attack surface due to IT – Security – Networking Infrastructure [2]



38% Increase in Manufacturing ransomware attacks Apr'23-22 [3]

15% Of total ransomware attacks were in the Manufacturing Sector Apr'23-22 [3]

OT Cybersecurity Attack profile 2023 [4]



[2] PaloAlto Networks Unit42_ASM_Threat_Report_2023.pdf (paloaltonetworks.com)
[3] Zscaler 2023 ThreatLabz State of Ransomware Report | Zscaler
[4] Fortinet 2023 State of Operational Technology and Cybersecurity Report (fortinet.com)

2024 Predictions: Cybercriminals will leverage AI to scale cyberattack volumes towards a broader set of manufacturing victims

Shift towards targeting new geographical opportunities such as Nordics / Japan

AI-driven cyber extorsion overcomes historical language & cultural 'barriers to entry':

- Authenticity in local language improves dramatically
- Understanding of the cultural & business dynamics of a company for ransomware negotiations now achievable
- Shift from traditional USA / UK focus to niche, 'softer' geographies eg Nordics & Japan

Lowering the bar to become a cybercriminal:

- Cyber extorsion continues to be opportunistic
- AI enables more individuals to enter cybercrime, driving higher volume of attacks from a broader source of countries around the world

Sophisticated threat actors to focus on evolving methods & high-end attacks and automate to scale:

- Cyber criminals will automate elements of their operating model to scale faster and free up expertise for complex tasks
- Ransomware as a Service (RaaS) will grow driving increased attack volumes and increased value of ransom payments
- Demand for criminal Access Broker Services has increased by 112% [5]
- Criminals will intensify attacks on multifactor authentication targeting identity protection vulnerabilities

Encryptionless ransomware attacks are on the rise:

- Focus shifts to stealing and threatening to expose company sensitive data and away from encrypting it
- It drives less business disruption and avoids reputational brand damage for the victim driving a greater propensity to pay a higher ransom fee >> "win-win" for the criminal + victim

Ransomware attacks on cloud services will increase:

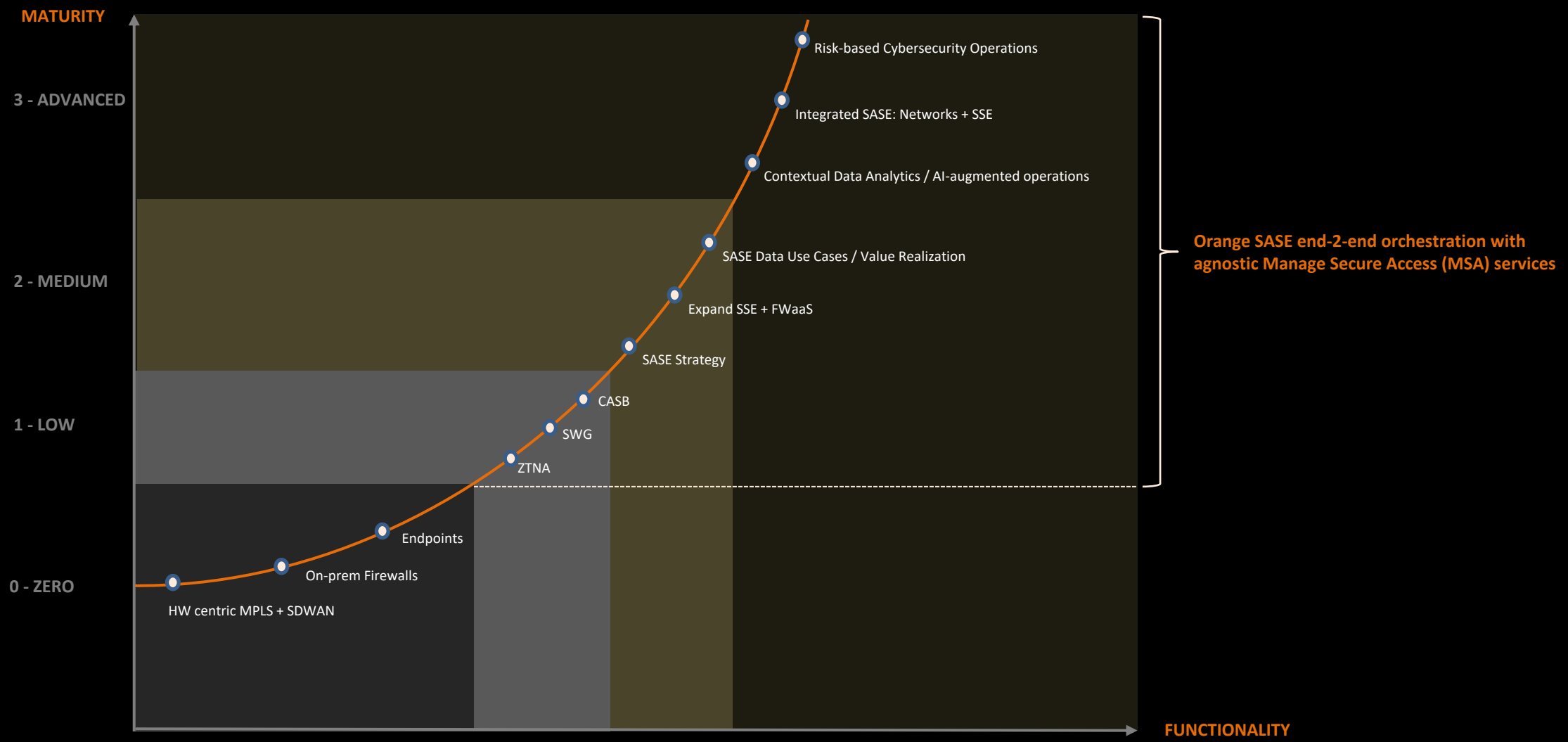
- With increasing adoption of cloud-native computing & storage, adversaries will accelerate cloud exploitation to compromise cloud infrastructure

[5] Crowdstrike 2023 Global Threat Report I CrowdStrike

Orange SASE Maturity Curve

Orange SASE Market Maturity Curve

Shifting from infra point solutions to risk-based, platform value realization



How Orange can help

SASE adoption, AI-augmentation and risk-based contextual data analytics will ‘change the game’ for Cybersecurity operations

This will only be achieved ‘at scale’ through strategic partnering and co-managed services

Current State

Unmanaged / Partially Managed Risks

- Talent gaps
- Scale challenges
- Infra centric
- Vendor specific silos
- Lack of business value realization

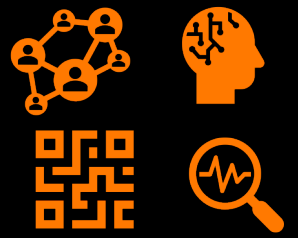
In-house Operations

Target State

Aggregated Data Ecosystems

- Remove the data silos
- Data & Analytics Operating Model
- Data Governance

Contextual AI-augmented Analytics



- Create broader context with real-time industry operational insights

Risk-based Cybersecurity Operations

- Better, faster informed decisions
- Human / AI partnership to enhance critical security + business decision making
- Automate manual standard tasks
- Create time for complex high-value human intervention decisions

Strategic Partnering & Co-managed Services

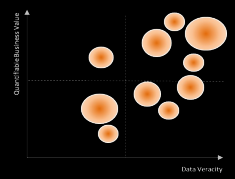
Our Orange pyramid of differentiated Cybersecurity services

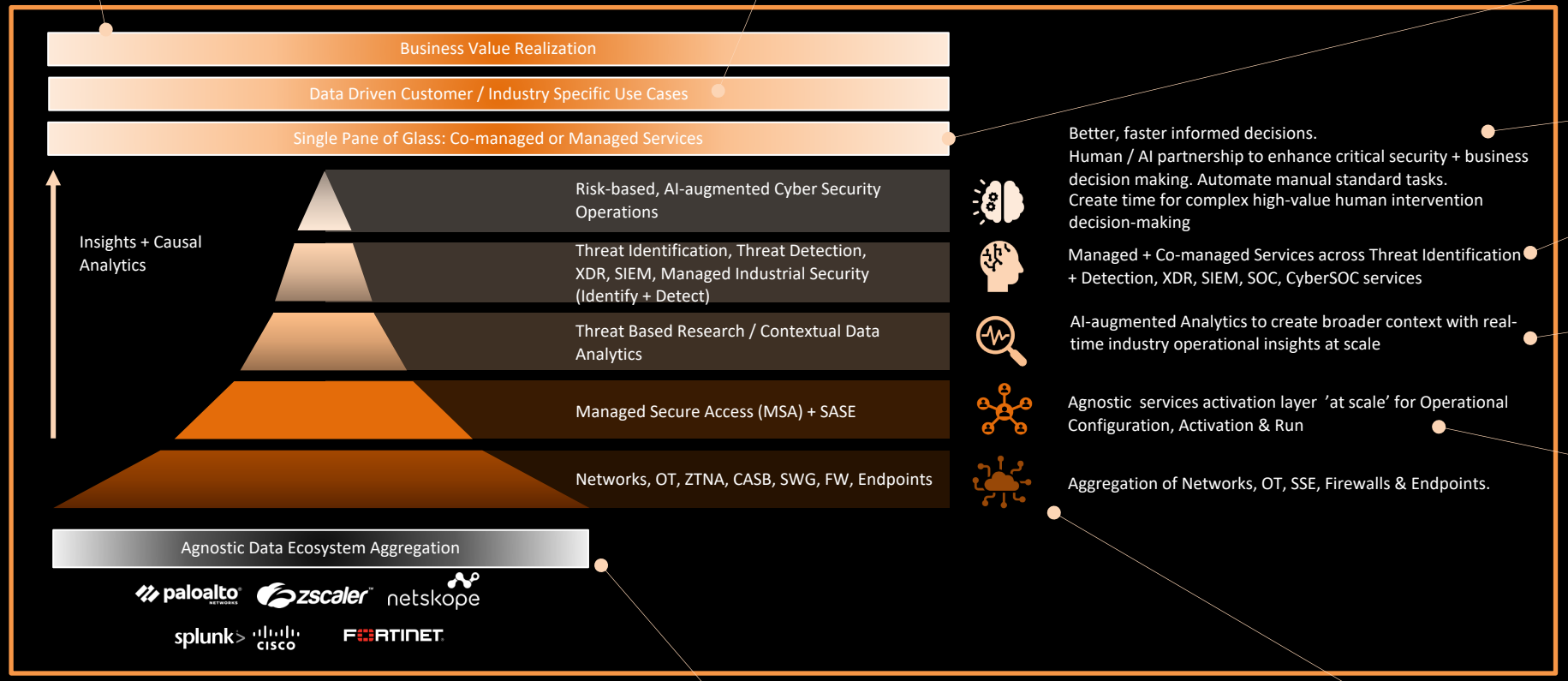
Shifting from infra point solutions to risk-based, platform value realization

9 Implementation of Cybersecurity / SASE business value realization to CFO, CISO and C-suite.
C-suite coaching to develop knowledge & insights to support investment prioritization, governance and incident management in the event of a cyber attack

8 Co-development with our customers for specific Cybersecurity / SASE data use cases

Data Use Case Value Realization





7 An Orange single pane of glass provides operational transparency and complexity reduction for enhanced, data-driven decision making

Better, faster informed decisions.
Human / AI partnership to enhance critical security + business decision making. Automate manual standard tasks.
Create time for complex high-value human intervention decision-making

6 Scaling Automation + AI to enable a risk-based approach to operations and facilitating better informed decision making with less FTEs

Managed + Co-managed Services across Threat Identification + Detection, XDR, SIEM, SOC, CyberSOC services

5 Integrated Threat Identification + Detection, XDR and SIEM co-managed / managed services

AI-augmented Analytics to create broader context with real-time industry operational insights at scale

4 Combining Orange threat based research data from Orange Cyberdefense 18 SOCs + 14 CyberSOCs operations with 3rd party threat based research data

Agnostic services activation layer 'at scale' for Operational Configuration, Activation & Run

3 Orange Managed Secure Access (MSA) platform provides a rich set of end-2-end SASE orchestration services on top of vendor solutions
Our SASE consulting experts can support co-development of your holistic SASE strategy and TCO Business Case

Aggregation of Networks, OT, SSE, Firewalls & Endpoints.

1 Agnostic integration of vendor silos across IT-OT-Networks-Cybersecurity

2 Broad portfolio of managed / co-managed services of vendor solutions across IT-OT-Networks-Cybersecurity

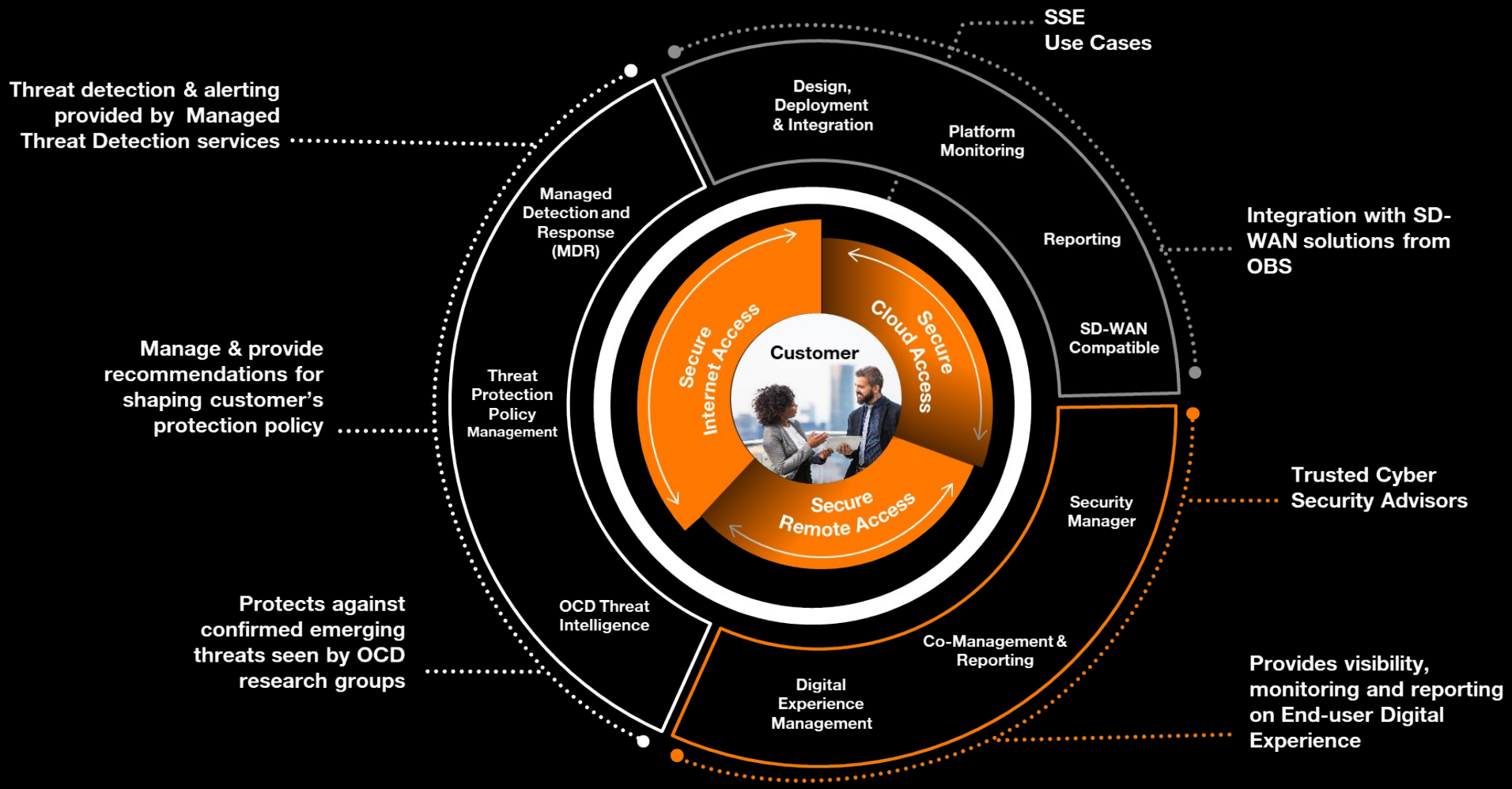
We partner with the market leaders

Gartner 2023 assessment of SASE / SSE technology vendors

SSE Quadrant

SASE Quadrant

Orange Managed Secure Access (MSA) on top of the ‘out of the box’ SSE vendor solutions



Our Managed / Co-Managed Agnostic Services Offering MSA :

Rich set of security posture services, operational configuration / service activation and AI-data use case acceleration built on top of 'out of the box' technology vendor functionality

Business Services

Orange Cyberdefense

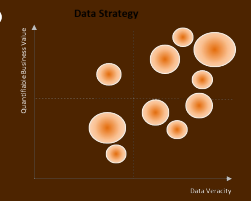
Managed Service Access (MSA)

Fully Integrated Managed / Co-Managed Service

Orange Security Analytics & AI-augmented Data Use Cases

- Security Analytics
- IT Service Intelligence
- Contextual, AI-augmented Data Use Cases
- AIOps Enablement
- Elastic Log Monitoring
- Homomorphic Encryption

Data Use Case Value Realization



Orange Managed Secure Access (MSA) Operational Configuration, Activation & Run

- Service Activation
- Self-service Access
- Co-management Access
- Vulnerability Mgmt.
- Change Enablement
- Incident, Problem, Service Request Mgmt.
- Reporting **Self-service / Advisory**
- Monitoring & Event Mgmt.
- Service Configuration Mgmt.
- Threat Intelligence
- Release Mgmt.

Secure Posture Management

- Threat Policy Management
- CASB Policy Management
- DLP Policy Management
- Digital Experience Management

Tech Vendor Out of the box

zscaler™ netskope paloalto NETWORKS®

End-2-end SASE Orchestration

Invest time to define your SASE Strategy which should have C-suite active sponsorship and organization alignment

Raise your ambition to a rich set of risk-based SASE services that are agnostic from the technology vendors and deliver business value realization within 6 months

A fully aligned SASE Strategy is becoming a business imperative to address the AI-augmented threat landscape and to enable business differentiation:

- This is no longer an infra-centric conversation
- Avoid short-term mindsets with fragmented technology vendor silos and ‘in-house only’ operations
- Selecting your tech vendor, without a SASE Strategy, will not bring an immediate ‘magical fix’ to your cyber security posture challenges or business differentiation ambitions
- Focus on achieving value, scaling operations and harnessing contextual risk-based operations with embedded AI assets

Consider partnering or co-managed services to address the deteriorating talent gap and spiralling cybersecurity threat challenges:

- Almost all organizations lack sufficient cyber experts or data scientists
- Get independent, credible advice
- Be open to consider consulting and agnostic, co-managed / managed services to address immediate scale and ensure contextual considerations are built-in to your cyber security resilience
- Act quickly!
  The threat landscape is continuously changing and increasing in complexity and lethality
  Standing still or repeating the same historical approaches of the past is placing your business at increasing risk
- Ensure your C-Suite are actively engaged in your SASE journey and committed to seeking rapid business value realization.

Our Orange differentiation

Helping organizations scale securely to risk-based SASE business value realization within 6 months

Joint co-development of your SASE data use cases with our consulting experts:

- The key to your SASE journey is ensuring your broad stakeholder base remain supportive through effective delivery of real tangible business value from your selected SASE data use cases
- Achieved through detailed joint analysis for data use case prioritization
- Shift beyond industry generic SASE use cases to your actual specific, business prioritized data use cases that must deliver results within 3-6 months

Aggregated data ecosystems and agnostic services integrated with AI-augmented contextual insights at scale:

- We are the leading Cybersecurity advisory & managed services partner in Europe with a deep understanding of the cybersecurity market and emerging trends
- Our uniquely positioned Managed Secure Access (MSA) solution provides agnostic, aggregated SASE services on top of the SSE technology venfors
- We aggregate cybersecurity data ecosystems from Zscaler, Netskope or Palo Alto with additional IT & network data, such as Splunk, Sentinel, Snowflake or Thousand Eyes ecosystems, whilst supplementing with Orange Cyberdefense global data from 18 SOCs and 14 CyberSOCs [6]
- This enables AI-augmented contextual Security Analytics insights + IT Service Intelligence to support your AIOps ambition and ensure business value realization to your prioritized data use cases.
- ‘Human in the loop’ still remains critical for high-end, complex decision making and should be reflected in your Operating Model design.

[6] [Orange Cyberdefense Executive Navigator 2023: Research-based cybersecurity insights to drive smart business decisions

Our Recommendations

Pragmatic initial steps to accelerate towards effective SASE adoption

Bring greater focus to effective vulnerability management:

- Up to date security patches should be rigorously applied to your assets
- Avoid slow, manual approaches to patching
- Use AI & a risk-based analysis processes to ensure your key assets are patched

Deploy least-privileged access architecture:

- Limit access to users that need it for their roles

Implement Zero Trust Network Access (ZTNA):

- Restrict user access to apps and data regardless of location in order to hinder lateral threat movement and reduce the exposure to the ransomware blast radius

Expand ZTNA to a consolidated Security Service Edge (SSE) architecture:

- Combine ZTNA to SWG and CASB to provide a layered approach for protection
- Avoid vendor lock in by ensuring a comprehensive, agnostic SASE strategy is aligned across your organization
- Seek collaboration / co-managed services partnerships in order to successfully scale your SSE plans to manage higher attack volumes
- Gain access to threat-based research insights and AI-augmented analytics
- Seek SASE data use cases for value realization ‘quick wins’

Explore beyond MPLS / SD-WAN for future network overlay solutions with SSE vendors:

- Ensure your SASE strategy addresses your future network ambition
- Shift away from HW centric networks
- Address network needs at branch locations then expand toward traffic intensive locations eg factories
- Seek advice, demand market best practice considerations and how this may fit with your historical network / security investments