SASE Solution offering for Manufacturing Vertical

Powered by Zscaler

Industry Trends

Digital Transformation

Global presence reduces latency which corresponds to near real-time security capability with better user experience / productivity

Smart Factories

Increased adoption of Industry 4.0 principles like automation and robotics and IoT to enhance efficiency and reduce labor costs

AI and Machine Learning

Leveraging AI and machine learning for predictive maintenance, quality control, and process optimization

Supply Chain Resilience

Improving supply chain transparency and resilience to mitigate disruptions

Sustainability Initiatives

Focus on sustainable practices, including reducing carbon footprints and adopting renewable energy sources

Cyber Security Challenges

Digital Transformation

Insufficient Cyberskills

Lack of skilled cybersecurity professionals within the manufacturing sector, leading to gaps in security practices

Legacy Systems

Many facilities still use outdated infrastructure that may not have modern security measures, making them more susceptible to attacks

Insider Threats

Employees or contractors with access to sensitive data can pose significant risks, either intentionally or unintentionally

Secure Cloud Migration

Ensuring that sensitive data is protected during and after the migration process is crucial

Smart Factories

Remote Access to systems

Organizations are finding it difficult to provide secure remote access to IT and OT infrastructure in plants

IT and OT Convergence

The integration of IT and OT introduces new vulnerabilities as these systems were traditionally separate

AI and Machine Learning

Segmentation

Organizations are struggling to have proper segmentation to limit the spread of malware and to limit the attack surface at the same time provide required access

Identity Management

Implementing effective access control measures to ensure that only authorized personnel have access to critical systems and data

Edge Computing

Implementing and managing secure edge computing infrastructure is challenging for many organizations

Supply Chain Resilience

Supply Chain Vulnerabilities

The complex supply chains in facilities can be exploited by cybercriminals, leading to disruptions and potential security breaches

Sustainability and Practices

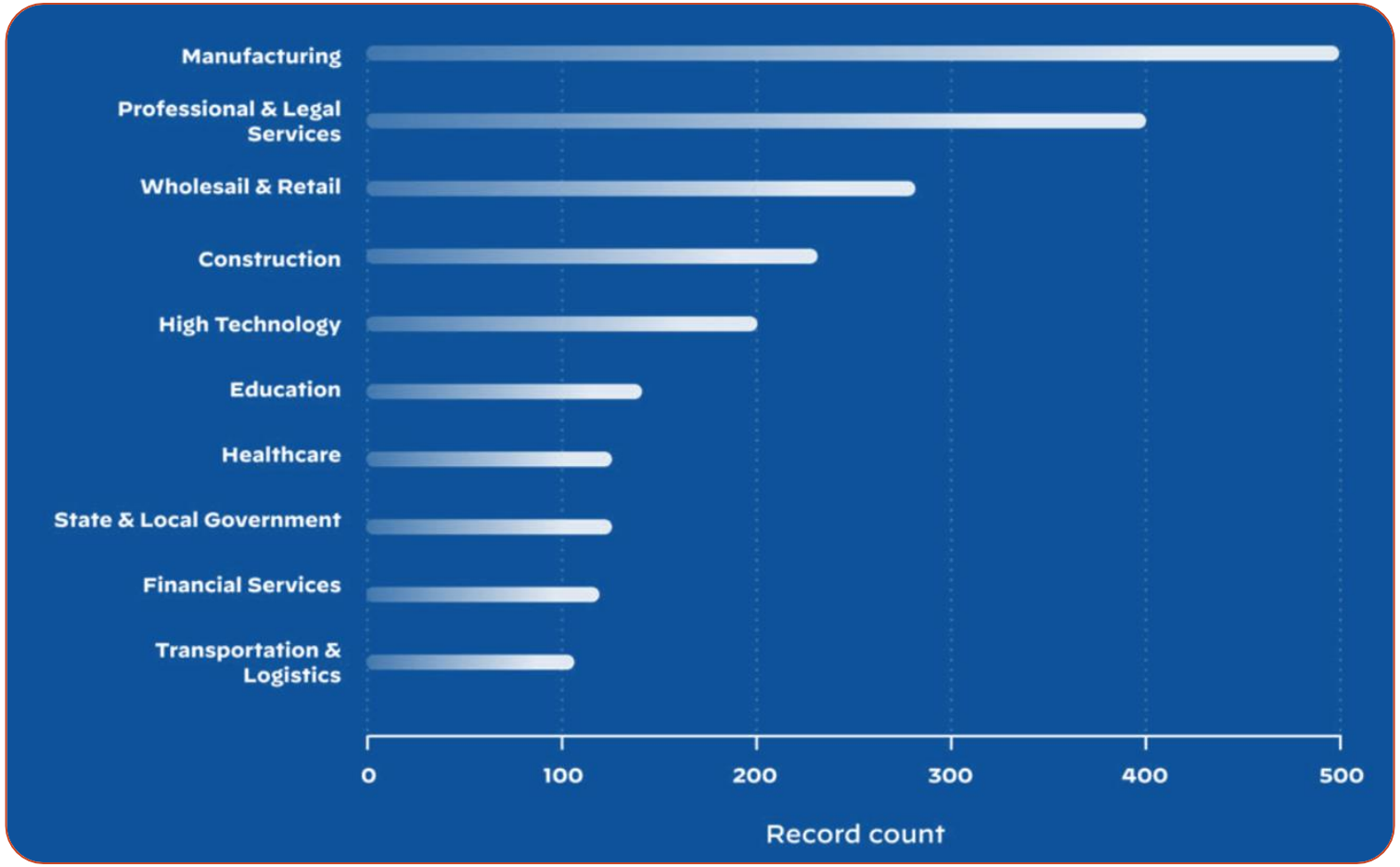
Regulatory Compliance

Navigating regulatory landscape for cybersecurity and data protection can be complex and challenging

Physical Security

Protecting physical assets from theft, vandalism, and unauthorized access remains a significant challenge

Manufacturing is the most targeted industry by ransomware gangs



Criminals often seek targets in industries where it's critical for business operations to be able to provide certain products or services in a timely manner

Source: Unit 42 2023 Unit 42 Ransomware and Extortion Threat Report
Industries most heavily impacted by extortion attacks (leak site data, 2022)

Top manufacturing targets and recent attacks

Top manufacturing targets

- ✓ Ransomware target
- ✓ Intellectual property
- ✓ Financial information
- ✓ Personally identifiable information
- ✓ Disrupt operations

Incentives

- ✓ Financial gain
- ✓ Espionage
- ✓ Disrupt critical infrastructure

Brunswick Corporation
Attack type: unknown
Location: Global
Year: 2023
Cost: $85 million USD

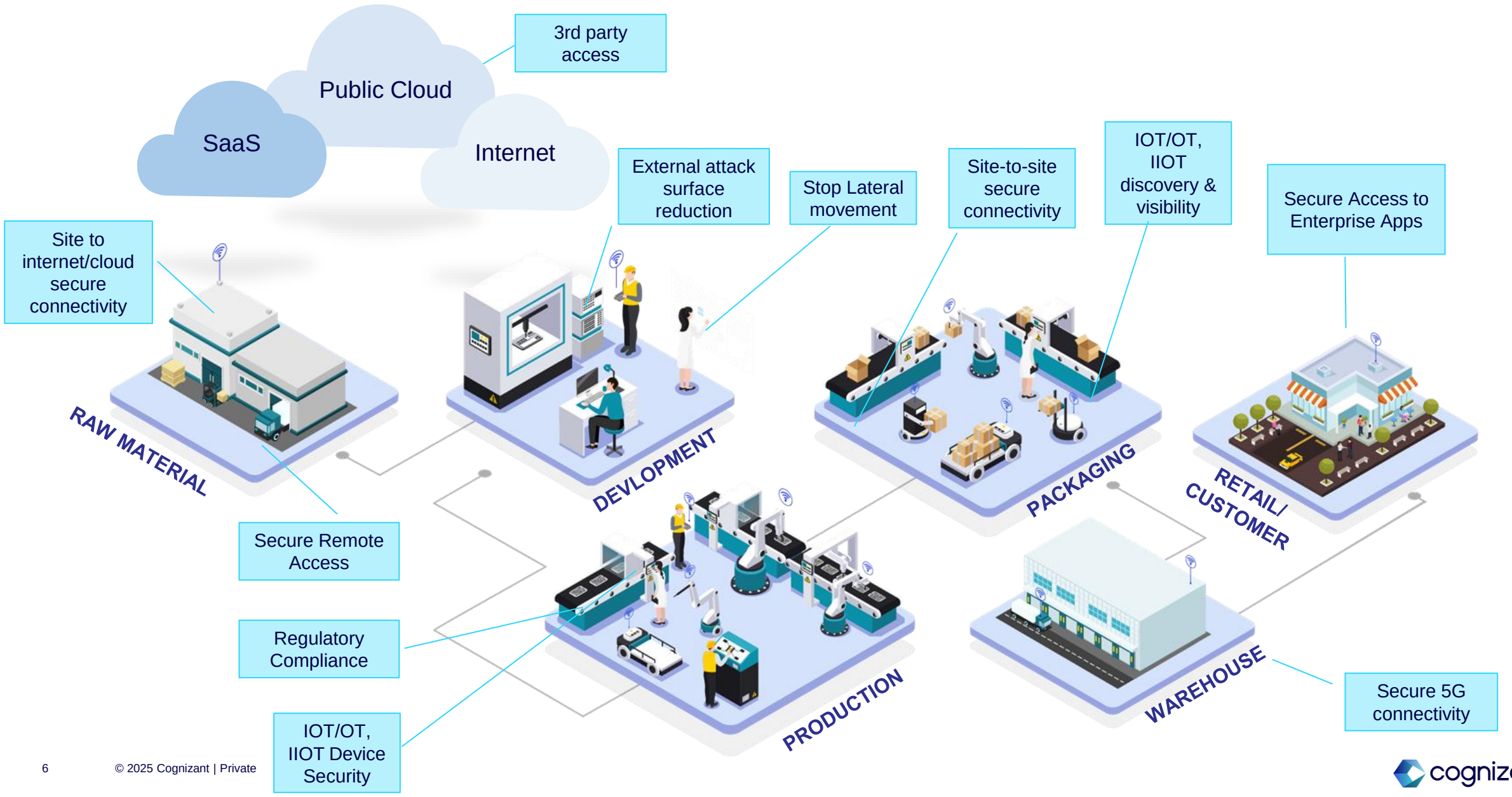
Norsk Hydro
Attack type: Ransomware
Location•. Norway
Year: 2019
Cost: $70 million USD

IBS
Attack type: Ransomware
Location: Australia and North America
Cost: $11 million USD
Year: 2021

Clorox
Attack type: Unknown, but has indications
Location: North America
Year: 2023
Cost: $356 million USD

Mondelez International
Attack type: Encrypting malware
Location: Based in Chicago
Year: 2017
cost: $100 million USD

Smart Factory and security use cases



ICS vulnerabilities in an upward trend

CISA ICS-CERT activity on 2020-2023

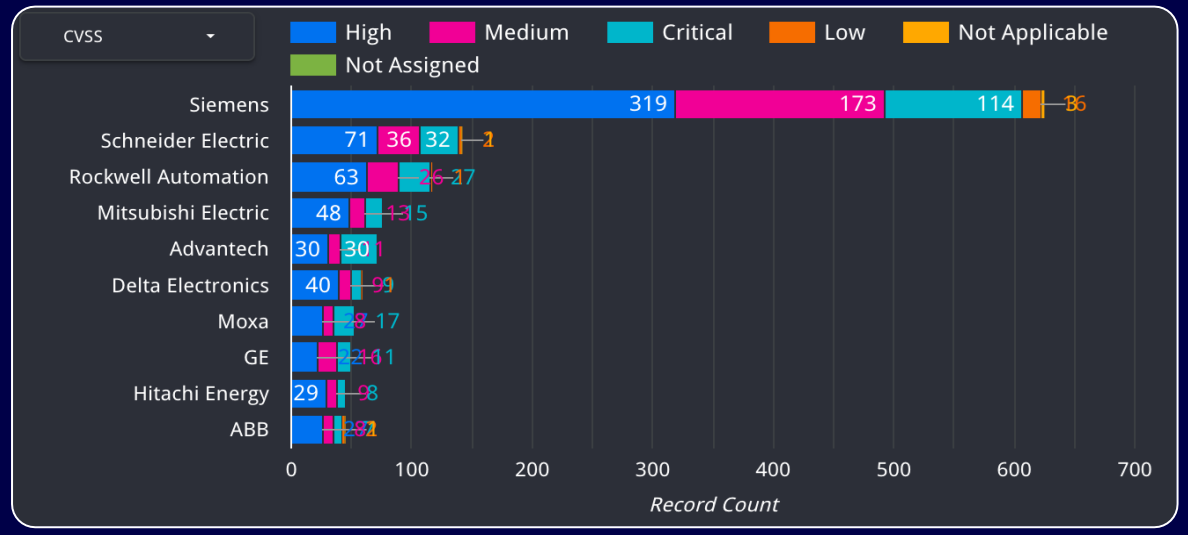
2500
Advisories

500
Vendors

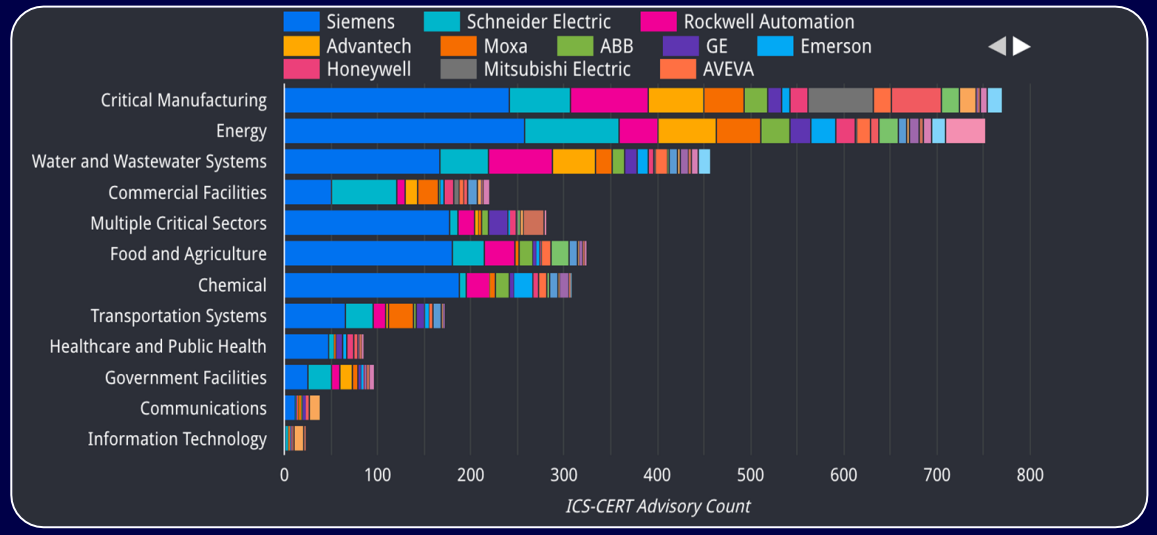
2000
ICS products affected

71%
Patch availability

Top ICS vendors in ICS-CERT advisories



Distribution of ICS-CERT advisories across manufacturing and industrial sectors



Source: Industry Control System Advisory Project on 7/6/2023

Cognizant's Managed Zero Trust SASE Solution

"Managed Zero Trust SASE solution for business growth and transformation"

Fastest way to scale SD-WAN

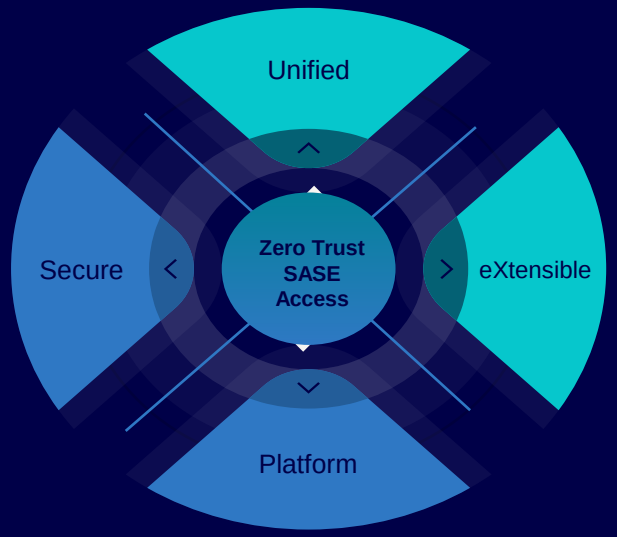
Zero Trust SASE
Powered by Domain-Specific AI Models

Security intelligence with fastest detection

A unified framework, incorporates several technologies working together.

Reliable and Efficient Security: Zero Trust SASE streamlined by Cognizant's MSS

- Cloud Managed
- Full Stack Solution
- Simplicity
- Reliability



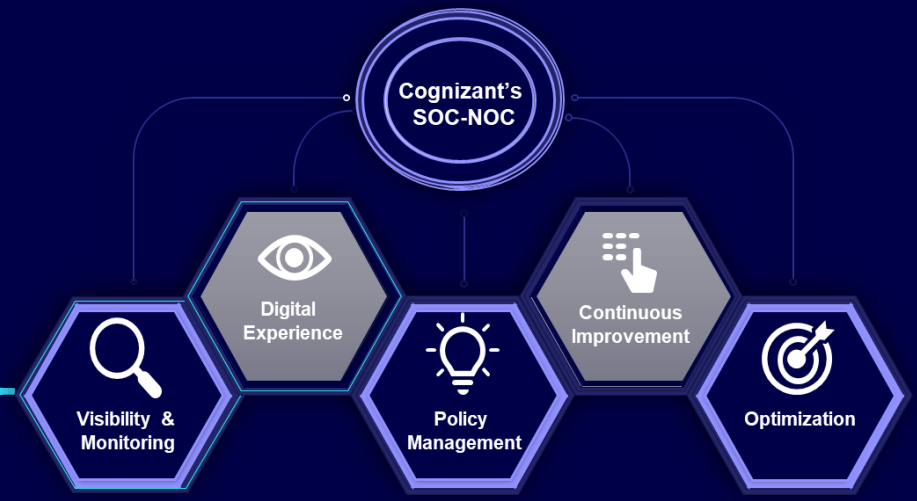
- Zero Trust Network Access
- Advanced Threat Protection
- Faster Detection

- Flexible Integration using Open APIs
- Continuous enhancements

- Cyber Threat Protection (SWG, FWaaS, DNS Security, Sandbox, Browser Isolation
- Data Protection (CASB, DLP)
- Zero Trust User-app access (ZTNA)
- Digital Experience Management

- Zero Trust Networking
- WANaaS, CDN, SD WAN, Multi-Cloud Connectivity
- Workload Communication
- Secure OT / IOT after workload communication

Integration



AI led Network Security Operations powered by Cognizant's Neuro AI

cognizant

Managed Zero Trust SASE Solution Components

SCALES
WITH BUSINESS

ENHANCES
SECURITY AND MANAGEMENT

AUTOMATE
PROCESSESS with Neuro increases 40% productivity

LOWER TCO
40% setup costs
20% annual operating Costs

FWaaS, Secure Web Gateway **DNS Security, Sandboxing**	**Zero Trust Architecture** **Digital Experience Management**	**Secure OT Convergence** **Full Stack Solution**	**Integrated SASE** **Extended Detection and Response**	**Cloud Access Security Broker** **Data Loss Prevention**	**Enterprise Browser** **Governance, Risk and Compliance**
Insider Threats	Secure Remote Access	IT and OT convergence	Segmentation	Supply Chain Vulnerabilities	Legacy Systems
Physical Security	Identity Management	Insufficient Cyber Security Skills	Edge Computing	Secure Cloud Migration	Regulatory Compliance

Challenges Addressed

Unlocking Potential with Zero Trust SASE: Use Cases

IOT/OT, IIOT discovery, visibility, Security

- Identify and fingerprint devices
- Seamlessly integrate IoT devices into the cloud admin panel upon connection
- Dashboard to provide visibility in the device landscape

External Attack Surface reduction

- You cannot attack what you cannot see.
- All connections are inside out thereby eliminating traffic originating from outside

Secure remote and 3rd party access

- Identity based secure application access
- Least privilege implemented at user, apps, device layers
- Credential injection and session recording for remote access

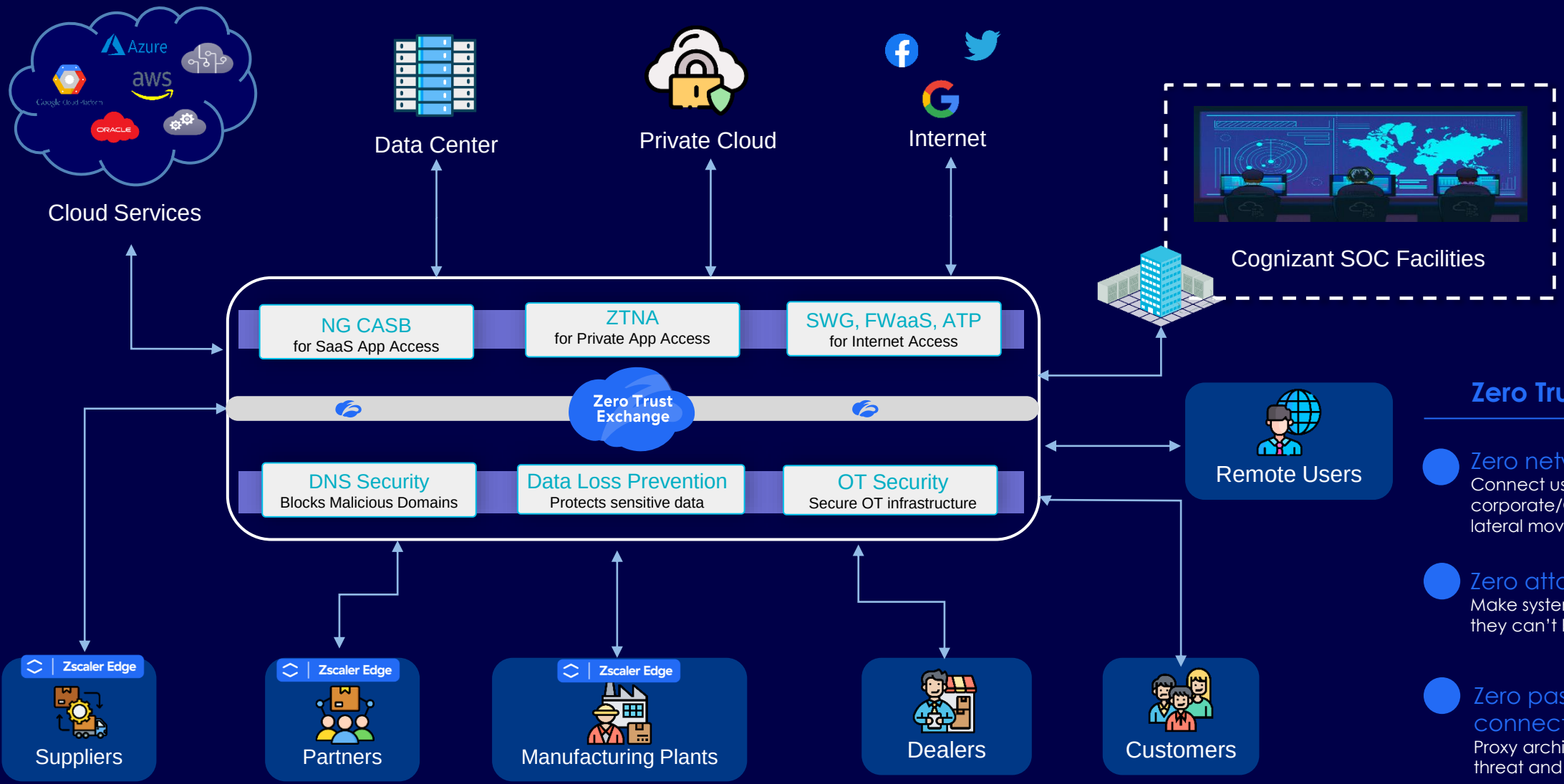
Secure internet/cloud/ site-to-site connectivity

- All connections are brokered
- Advance cyber security controls delivered at the cloud
- Complete north-south traffic inspection

Stop lateral threat movement

- Policy based device to device access
- Advanced segmentation capability to reduce attack surface and lateral movement

Zero Trust SASE – Reference Architecture – for Manufacturing Sector



Zero Trust Exchange

- **Zero network access**
  Connect users to systems/apps, not corporate/OT networks, to prevent lateral movement
- **Zero attack surface**
  Make systems invisible so they can't be attacked
- **Zero passthrough connections**
  Proxy architecture for better cyber threat and protection

cognizant

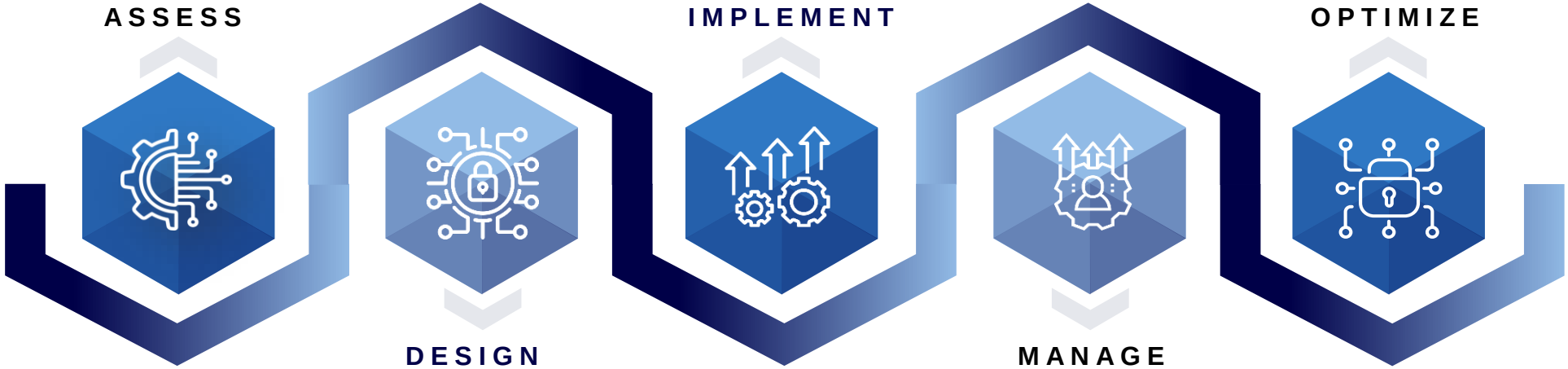
Approach Advantage - Fortified Security with fully Managed SASE

Cognizant tailors its standard methodology to help organizations evaluate their existing network security models, establish a target state and develop a transformation roadmap

- Discovery of device and assets
- Security assessment and policy formulation.
- Identify SD-WAN use cases and multi-cloud visibility.
- Define SASE objectives.
- Develop SASE implementation roadmap.

- Stage-wise SASE onboarding.
- Blueprint execution.
- Network security setup and tuning.
- SASE-cloud integration.
- Industry-standard benchmarking and hardening.
- Policy alignment.
- Platform validation.

- Maximize Cyber investment utility through defensive enablement services, integrations, best practices, and insights from Cognizant's diverse customer experiences.
- Optimize operational efficiency.



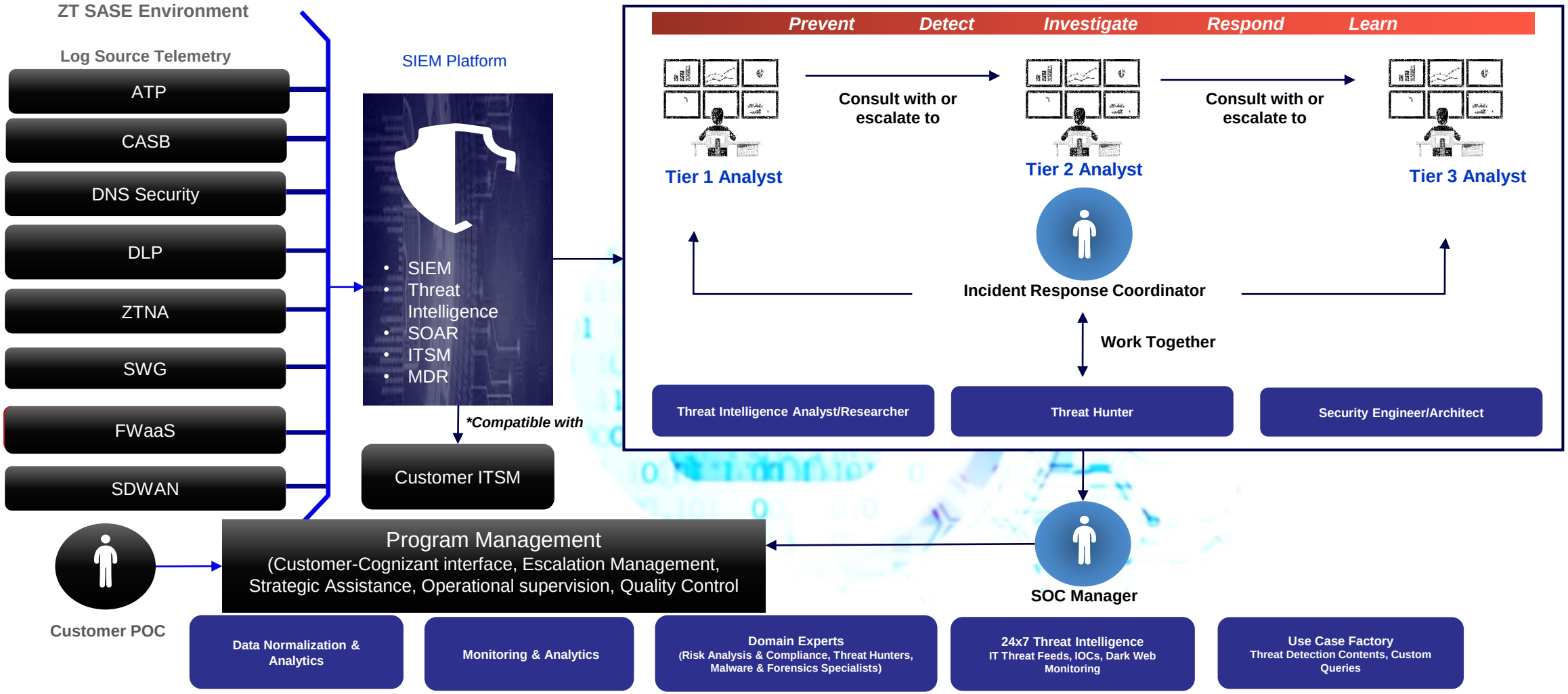
- SASE Blueprint design for industry use cases.
- Zero trust framework development within SASE.
- Unified management console development.
- High & Low-Level design documentation.

- Continuous monitoring of network, security, and cloud infrastructure.
- Manage and maintain the SASE platform.
- Automate security policies.
- Enhance SLA metrics.

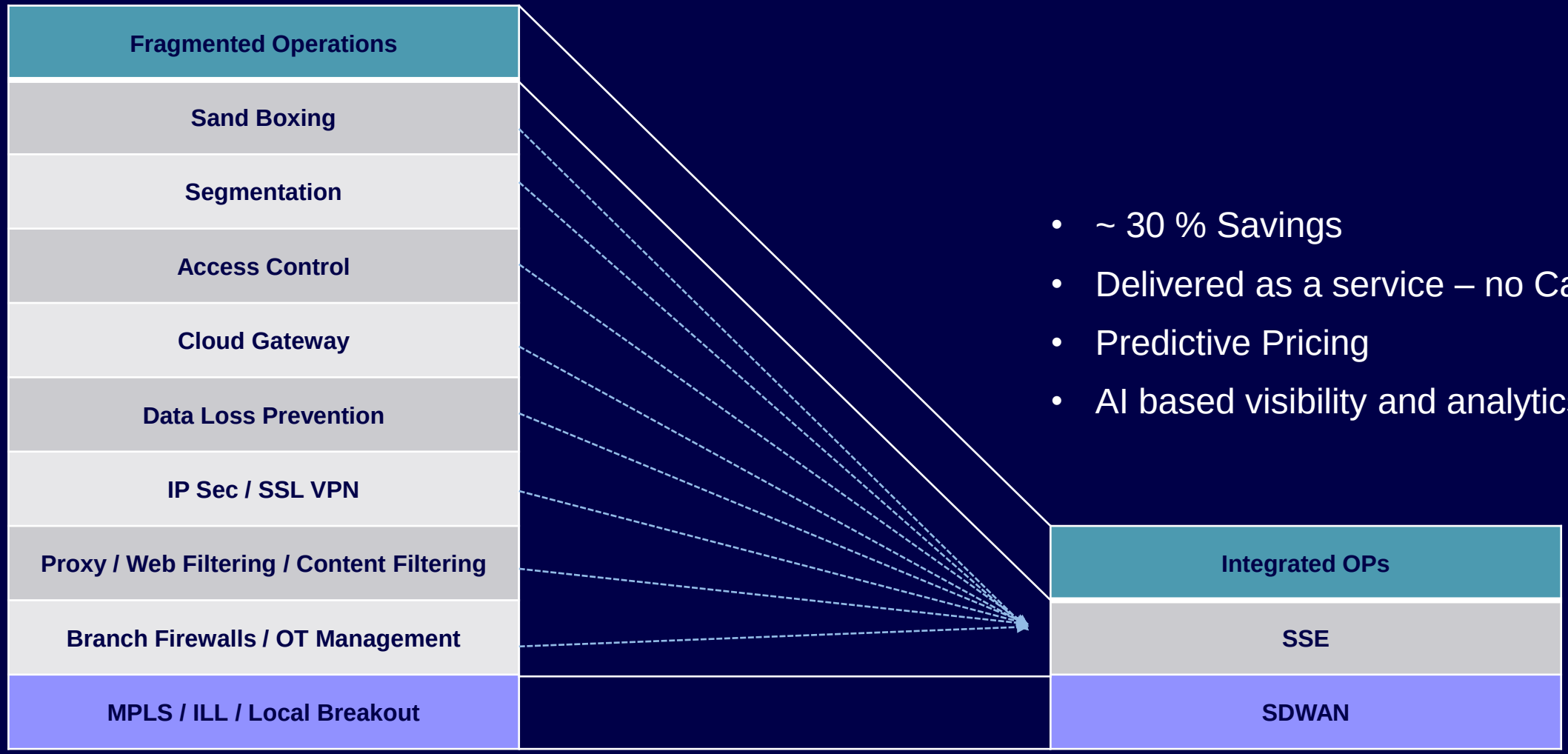
CONSULT TRANSFORM MANAGE

cognizant

Operations differentiator – Tighter integration through collaboration for maximise synergy and minimize risk



Commercial differentiator - Committed Savings



- ~ 30 % Savings
- Delivered as a service – no Capex
- Predictive Pricing
- AI based visibility and analytics

Current mode of operations

With Managed Zero Trust SASE

How Manufacturers Benefit from SASE

Secure Global Connectivity	SASE securely connects employees across multiple plants to SaaS, cloud and on-premises applications, supporting networks like the internet, MPLS, and cellular.
Zero Trust Network Access (ZTNA):	Implements least-privilege access controls, ensuring only authorized users and devices access specific resources, minimizing attack surfaces.
Enhanced security:	Enables faster detection, identification, response, and remediation of cybersecurity incidents.
Data Loss Prevention (DLP):	Prevents unauthorized access and exfiltration of sensitive data like production plans and intellectual property.
Cost reduction:	Manufacturers can save up to 30% annually by transitioning to SASE, freeing employees to focus on strategic projects.
Smooth transition:	Quick deployment makes the process nearly hassle-free. Also helps in smooth migration to cloud applications and app migration to cloud
Improved user experience and collaboration:	Enhances connectivity speed and performance, boosting employee satisfaction and productivity.
Compliance with Regulations:	Helps organizations comply with data privacy and security regulations like GDPR and HIPAA, essential for Industry 4.0.

Cognizant accelerators

Making solution work for business domain with domain centric reference architecture approach

Frictionless adoption with seamless integration with territory services end user management services and awareness and risk management functions.

Golden Templates validation checklist and standardized policy for fast-track failsafe implementation

700+ trained and certified SASE resources. 25+ successful implementations

Flexible and agile operating model and commercial model assuring cost advantage.

Automation and AI first approach for provision detection and mitigation actions

Successful execution of cyber strategy - prevention, detection, recovery.

Customer Snapshot

Case Study

SUMMARY

British American Tobacco is a British multinational company that manufactures and sells cigarettes, tobacco, and other nicotine products. Established in 1902, today, the company is the largest tobacco company in the world based on net sales, with roughly 200 brands and operations in around 180 countries.

Industry - Food, Beverage, and Tobacco

HQ: London, England, UK

Size: 55,000 employees in 180 countries

Customer Asks

- Renewal of licenses from Orange Business Services (OBS)
- MSP partner for Zscaler
- Replace traditional VPN gateways
- Full capability utilization of Zscaler
- ZIA & ZPA licenses with uplift (41,000)
- Zero trust journey partner
- App segmentation (500 apps)

Cognizant Solution

- Flexible consumption model
- Customized delivery model
- Consult, operate and run services
- Shift to a zero-trust model
- Enriched & enhanced use-cases delivered
- Improved operational telemetry from key connectors in Azure and On-premise DC

Business Outcome

- Total deal value – $15M
- Operational efficiencies (30%)
- Win – Win – Win for the all the 3 parties
- 5-year deal with no price rise and with $1M TCO reduction
- Zscaler – 5 year assured deal with $6M uplift of new Licenses and Services $3M

Cognizant Zscaler MSP Solution

Thank You