FORTINET

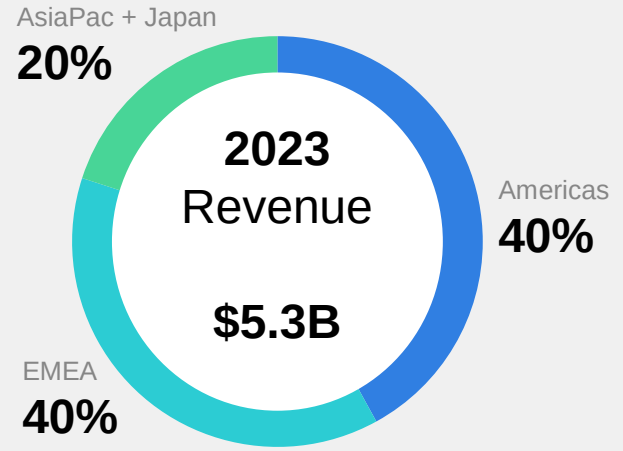
The fast moving world of threat intelligence

The Cybersecurity Partner You Can Count On

Securing people, devices, and data everywhere.

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Global Customer Base **750K+** Customers	2023 Billings **$6.4B+** *(as of Dec 31, 2023)*	Market Capitalization **$52.1B** *(as of March 31, 2024)*	Organic R&D investment **1,318** *Global Industry Patents*
Broad, Integrated Portfolio of **50+** Enterprise Cybersecurity Products	Strong Analyst Validation **100+** Enterprise Analyst Report Inclusions	**$2.5B+** Investment in Innovation since 2017, with 91% R&D (as of Dec. 31, 2023)	Investment in scale of threat intelligence and AI/ML **100Bn+** Threat Events Neutralized Daily



YoY:**32%**

FORTINET®

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500**

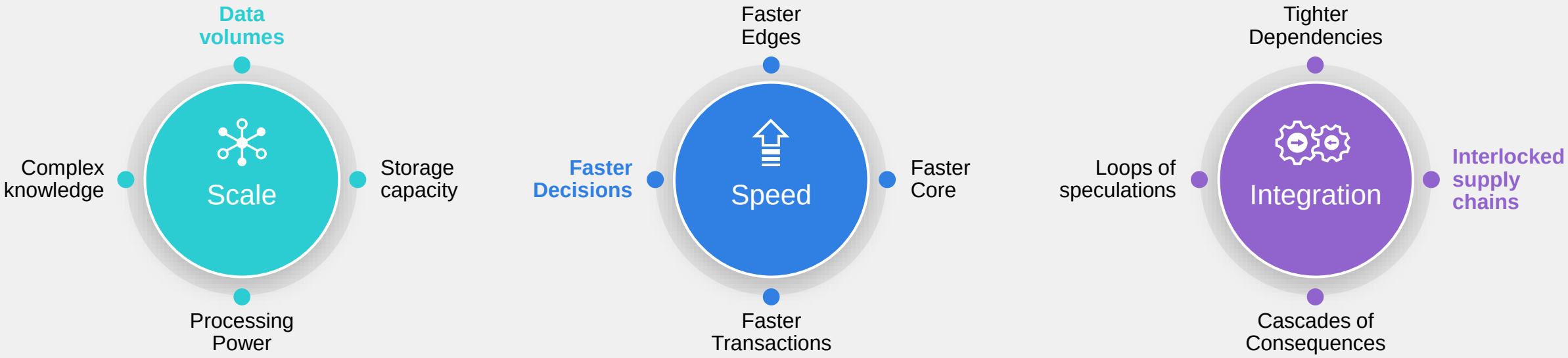
Member of: **2022 Dow Jones Sustainability World and North America Indices**

Security Investment Grade Rating: **BBB+ Baa1**

Mapping the World of Cyber

The interplay between risks and regulation

Cybersecurity Risks



Cybersecurity Regulations

Pressure from the Threat Landscape

Impact on Cyber Insurance

Artificial Intelligence (AI)

- Threat actors and defenders will be increasingly augmented with AI capabilities
- Frequency of claims expected to rise. No change in accumulation modelling so far
- Era of GenAI has just started
- Increasing usage of AI within the insurance industry

Geopolitics

- High impact due to sophistication of actors
- Cyber arsenal might be used by commercial threat actors and APT groups
- Cyber arms race influences supply chain risks

Supply Chain

- Multiple loss scenarios possible: BI, CBI, Data Breach
- Digital bottlenecks and systemic risks will grow (e.g. Cloud Services)
- Difficult to assess 3rd party risks

Data Privacy

- Rising liability for risk owner
- More regulation, compliance and reporting/breach disclosure requirements (e.g. NIS2, SEC, DORA)
- 3rd party elements will remain in demand an a key loss driver

BEC

- High loss expectation in the field of BEC/BCC attacks a high number of unreported cases
- Low sophistication actors might develop more easily in the future

Ransomware

- Ransomware will continue to be the largest risk and loss driver
- Tech progress and tactics point to a more complex and damaging ransomware landscape
- Current trend of increasing ransomware losses seems likely to continue in 2024

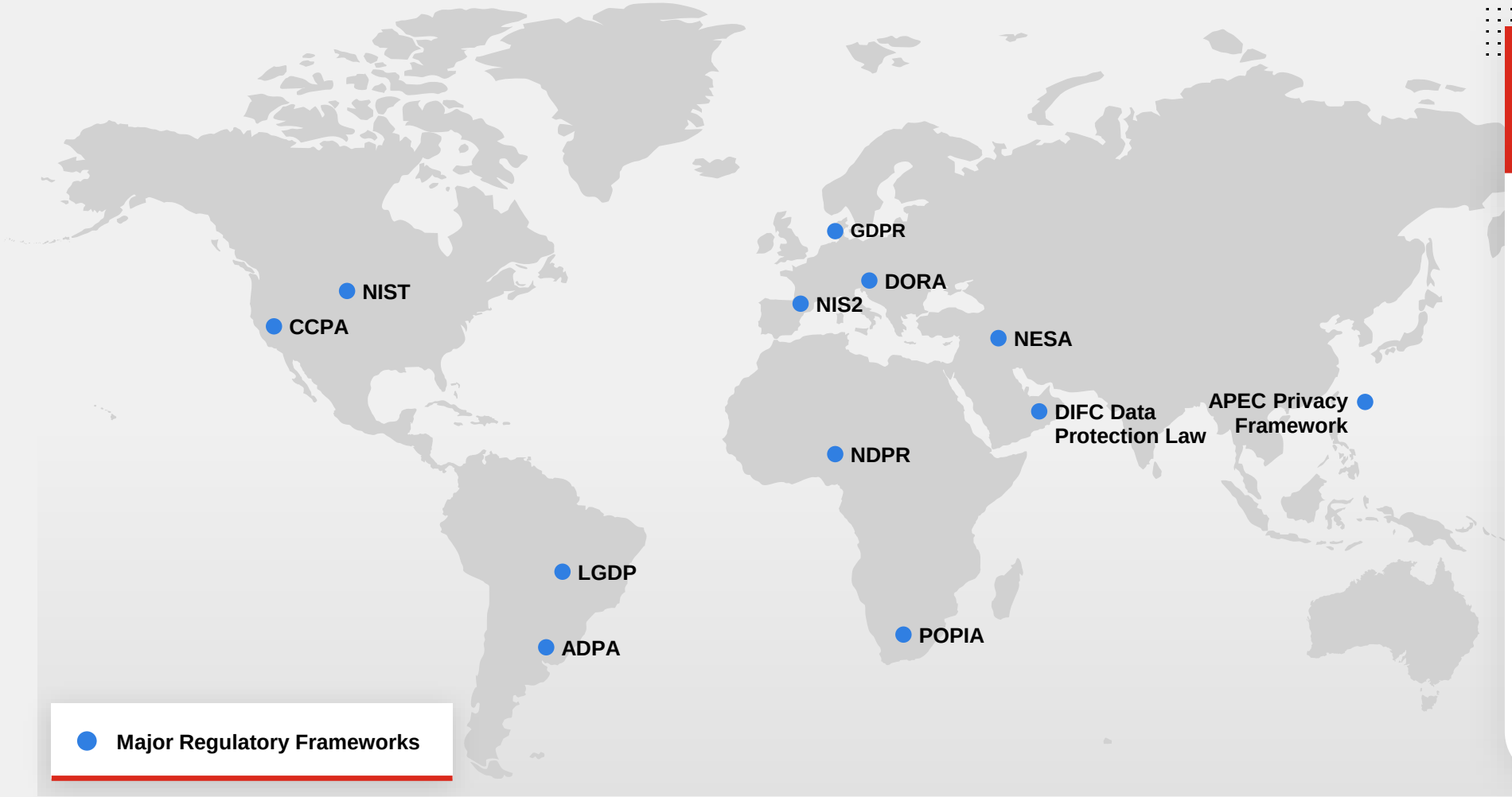
high

very high

Source: Chainalysis | Source: Cybersecurity Ventures | Source: Symantec | Source: Identity Theft Resource Center | Source: Forrester | Source: ISC2

Global Compliance and Regulatory Landscape

Navigating Key Requirements for Cybersecurity Resilience



Securing Networks Globally

Securing Networks Globally

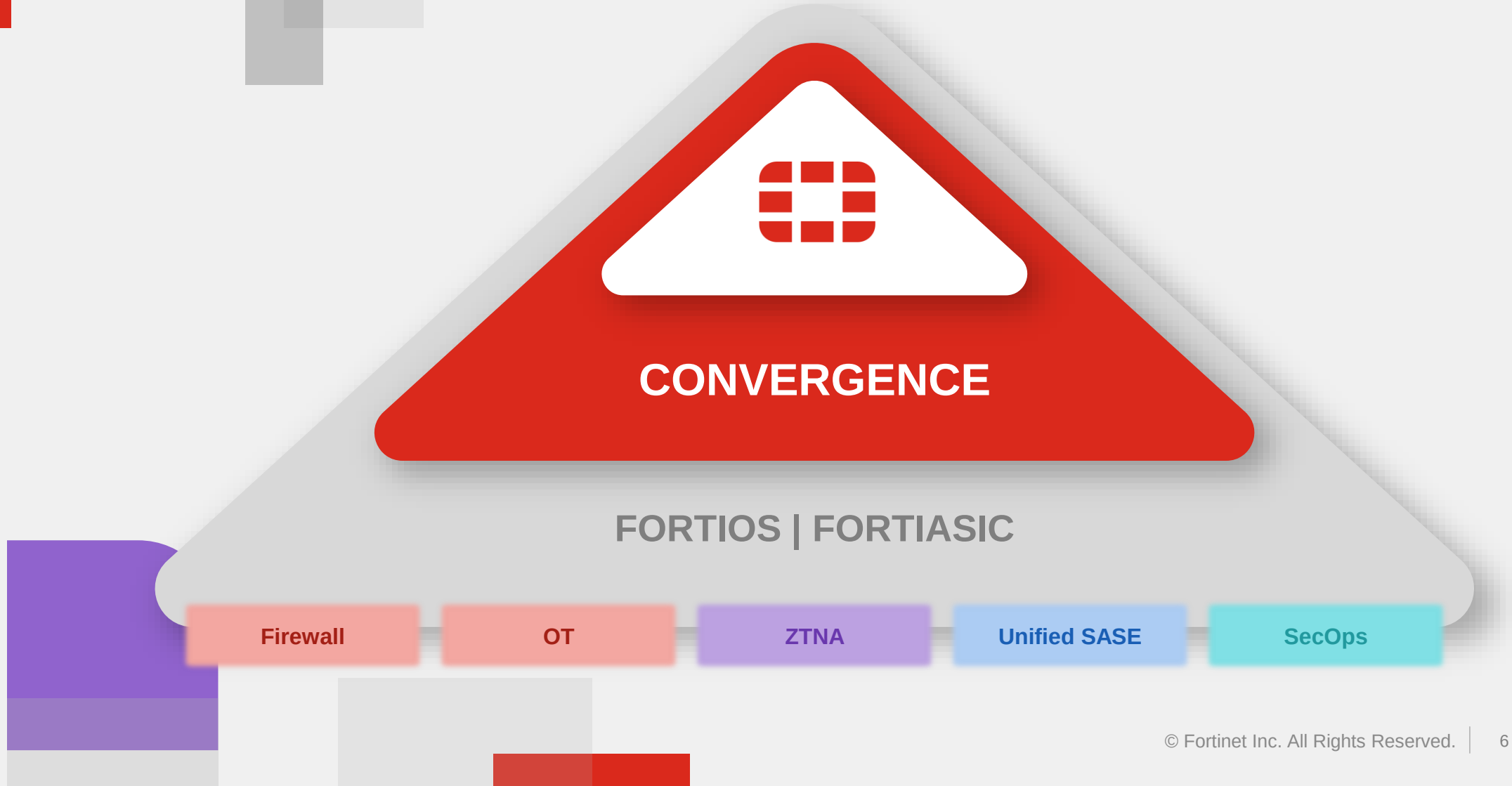
Navigating Compliance
A Platform designed to fulfill regulatory requirements

Comprehensive Security

- Stronger defense, for better detection and prevention
- IT/OT Convergence for better control
- ZTNA- Minimized risks
- Cost Consolidation, Resilience
- Threat Mitigation Acceleration

Converging to Network Security

The Vision



Converging into One OS

The Execution

What Makes Us Think The Vision in Right?

LEADER

December 2022 Magic Quadrant for **Network Firewalls**

LEADER

September 2022 Magic Quadrant for **SD-WAN**

LEADER

March 2024 Magic Quadrant for **Wired & Wireless LAN**

CHALLENGER

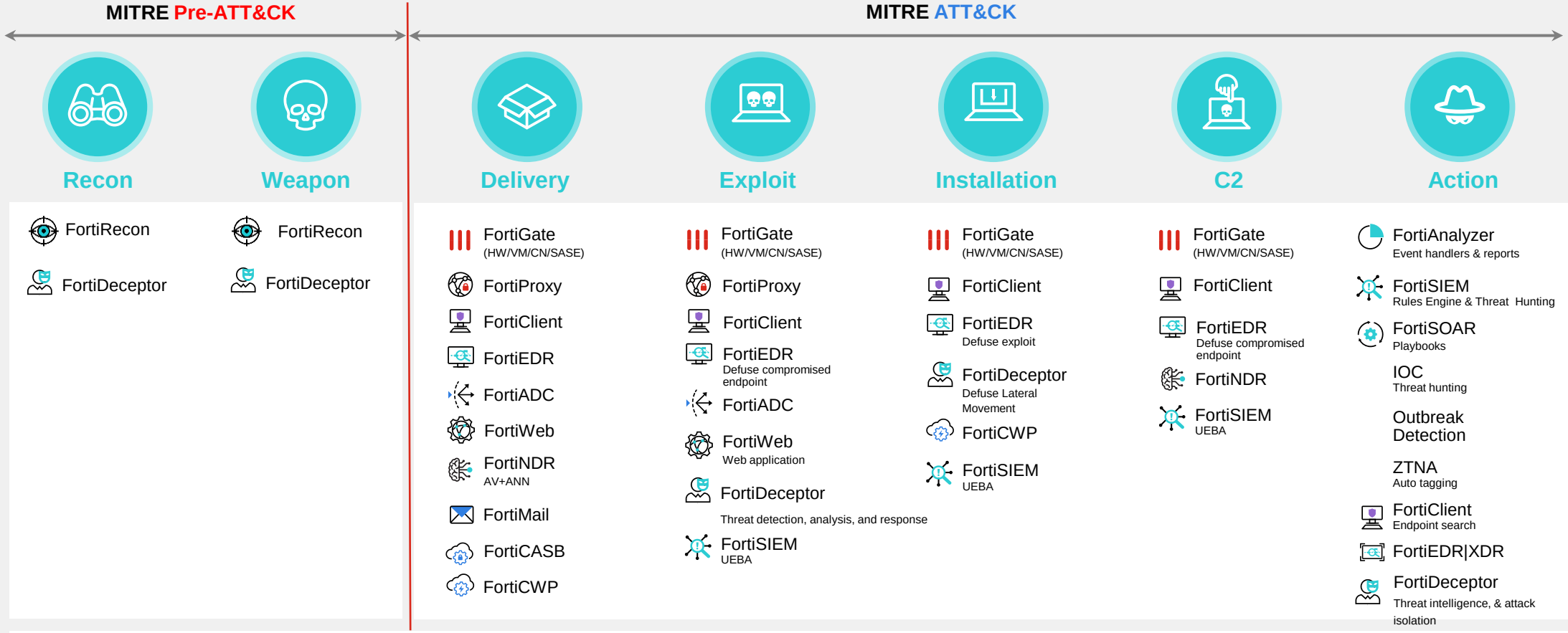
August 2023 Magic Quadrant for **Single-Vendor SASE**

CHALLENGER

April 2024 **Secure Service Edge**

Remarkable: It is the Same Platform across ALL Magic Quadrants

Breaking The Attack Sequence




FORTINET