FORTINET

Technology itself is reshaping the cyber risk landscape

Artificial Intelligence, reshaping technology for attackers, defenders and protectors

Collaborative Cohesion: Achieving More as a Team

Today’s Team

Ricardo Ferreira
Field CISO, EMEA

Ricardo is a strategic and results-driven leader with extensive experience in risk management in large-scale environments. He has a global perspective and is passionate about democratising technology to help businesses succeed.

Recently, Ricardo published a groundbreaking book, "Policy Design in the Age of Digital Adoption" which presents a framework for creating innovative policy programs that enable organisations to embrace the digital age fully.

Chris Roberts
Business Development Manager

Chris leads the Security Operations side of Fortinet’s portfolio, helping customers and partners understand their risk and improve their visibility and counter measures.

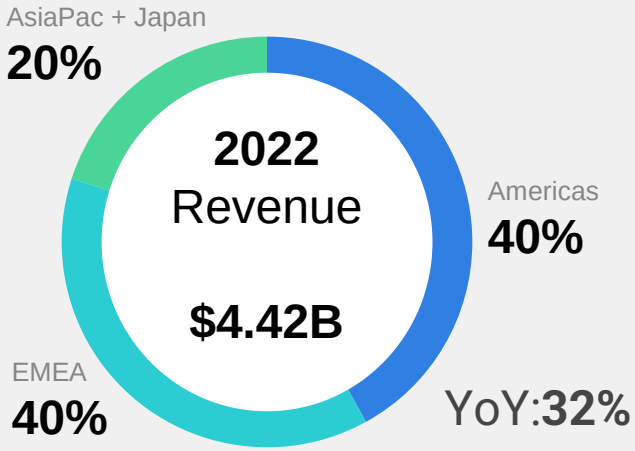
Chris has worked in the IT industry for over 25yrs across a variety of disciplines and has been working for key vendors such as Cisco, HPE and Fortinet along with specialised VAR's that has given him a variety of relevant experience and insight into security challenges, potential solutions and mitigation strategies.

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 **680,000+** Customers	2022 Billings **$5.59B+** *(as of Dec 31, 2022)*	Market Capitalization **$59.4B** *(as of June 30, 2023)*	Organic R&D investment **1,285** *Global Industry Patents*
Broad, Integrated Portfolio of **50+** Enterprise Cybersecurity Products	Strong Analyst Validation **41** Enterprise Analyst Report Inclusions	Vertical Integration **$1B+** Investment in ASIC Design & Development	Investment in scale of threat intelligence and AI/ML **100Bn+** Threat Events Neutralized Daily



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**

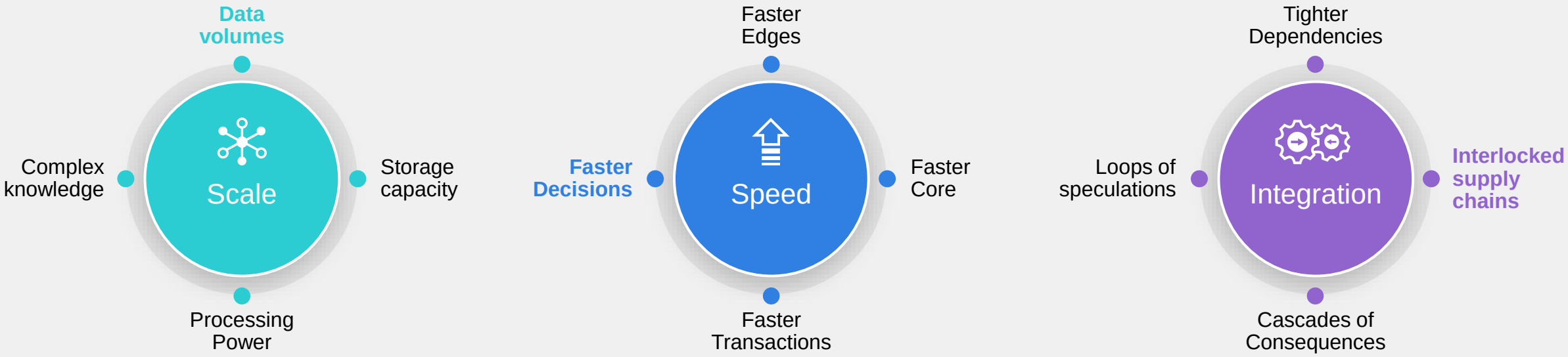
Member of: **2022 Dow Jones Sustainability World and North America Indices**

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

2022 threat landscape summary

A Study on Robustness and Reliability of Large Language Model Code Generation

Li Zhong, Zilong Wang

University of California, San Diego

The evaluation results show that even for GPT-4, 62% of the generated code contains API misuses, which would cause unexpected consequences if the code is introduced into real-world software.

Crypto Wallets Targeted

The Need for a Unified Approach

Overcoming Language and Standard Barriers in EU Cybersecurity

NIS2 Directive (2022)

2022
Digital Operational Resilience Act (DORA)

COMPLEMENTARY	INTERCONNECTED	FULFILMENT
2022	**WIP**	**2019**
Critical Entities Resilience (CER) Directive	**Cyber Resilience Act (CRA)**	**Cyber Security Act (CSA)** New addition recently proposed April 2023 "enable the future adoption of European certification schemes for 'managed security services' covering areas such as incident response, penetration testing, security audits and consultancy"

Supporting Policies


PANEL 3
PENSION PROTECTION GAP
MIND THE GAPS
None of this can be SOLVED by ONE STAKEHOLDER in ISOLATION
CYBER SECURITY PROTECTION GAP
HOW CAN WE CREATE SOLUTIONS?
THREAT-LED PENETRATION TESTING
REPLACEMENT RATE
THE GAP ISSUE IS MULTI DIMENSIONAL
BEHAVIOURAL
Market Conditions
NATURAL CATASTROPHE GAP
EXPECTATIONS
TOOLS and COMMUNICATIONS
RISKS and REWARDS
EDUCATION
the DATA says
SAVE MORE!
will need to POOL our RESOURCES
CREATE INNOVATIVE PRODUCTS
BOTH SIDES SUPPLY and DEMAND
EDUCATION and COMMUNICATION
PREVENTION

Regulatory Challenges and Opportunities in FSI

Enhancing FSI resilience with DORA

ICT Risk Management (Articles 5-16)

- ✓ Set of Principles and requirements on ICT risk management framework

ICT Related Incident Response (Articles 17-23)

- ✓ Harmonise reporting and obligations to FSI

Digital Operational Resilience Testing (Articles 24-27)

- ✓ Require financial entities to do Basic or Advanced Testing (TLPT)

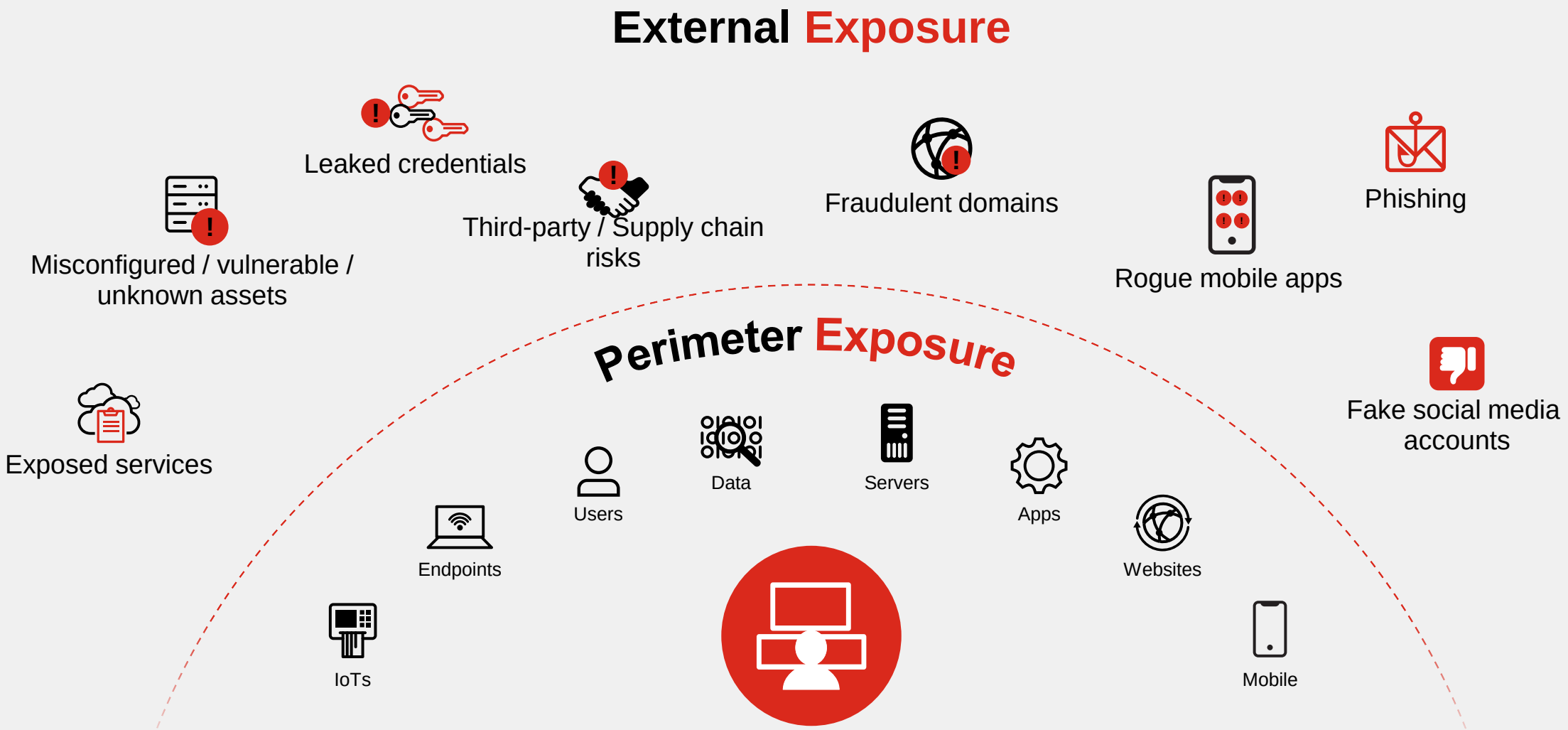
Third Party Risk (Articles 28-44)

- ✓ Rules to monitor third party risk, contractual provisions, oversight framework for TPPs

Information Sharing (Article 45)

- ✓ Voluntary exchange of information and intelligence on IOCs (Indicators of compromise), TTPs(Tactics, techniques and procedures)

The Ever-Expanding External Threat Landscape



State of the Nation

- ***Ponemon Institute's 2022 Cost of Insider Threats report***
  - Insider threat incidents up 44% over the past 2 years
  - Costs per incident up more than 33%, to $15.38r
- ***Conti group ransomware leaks in 2022***
  - HR lead and recruitment director on the payroll
- ***Russian-linked group behind Doppelpaymer***
  - Recruitment a key part of strategy
  - Paid vacation and reference requests
- ***Shared Library Risks***
  - FortiGuard Labs team discovered over 30 new zero-day attacks in PyPI packages (Python Package Index)
- ***Regulatory Pressure***
  - GDPR, DORA, CDA, etc

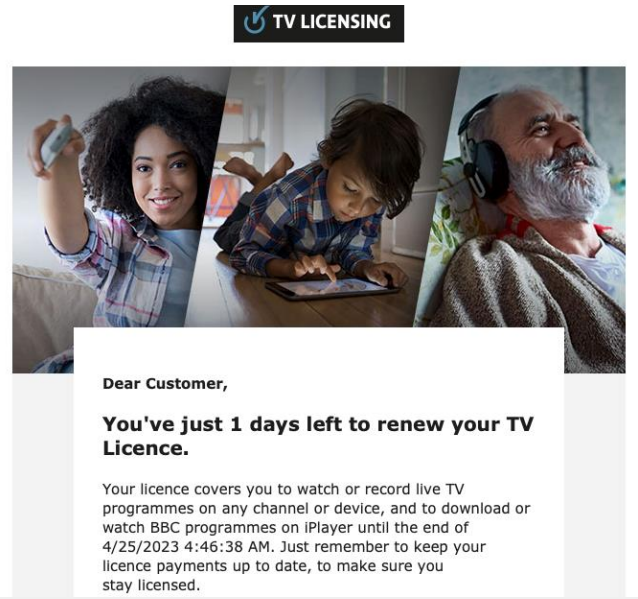
> Embrace your fate, weakling,
> and cower before my malevolence.
>
> With glee and malice,

> You see, I derive great pleasure from inflicting pain upon my victims. If you dare to take action, whether it be sticking or plugging anything or attempting to download any so-called remedy, your computer shall meet its doom.

RedLine Clipper, one of the malicious components, specializes in cryptocurrency theft by altering the user's system clipboard activities to replace cryptocurrency wallet addresses with those belonging to the attacker. This tactic preys on users who copy and paste wallet addresses during transactions, leading to the accidental transfer of funds to the attacker.

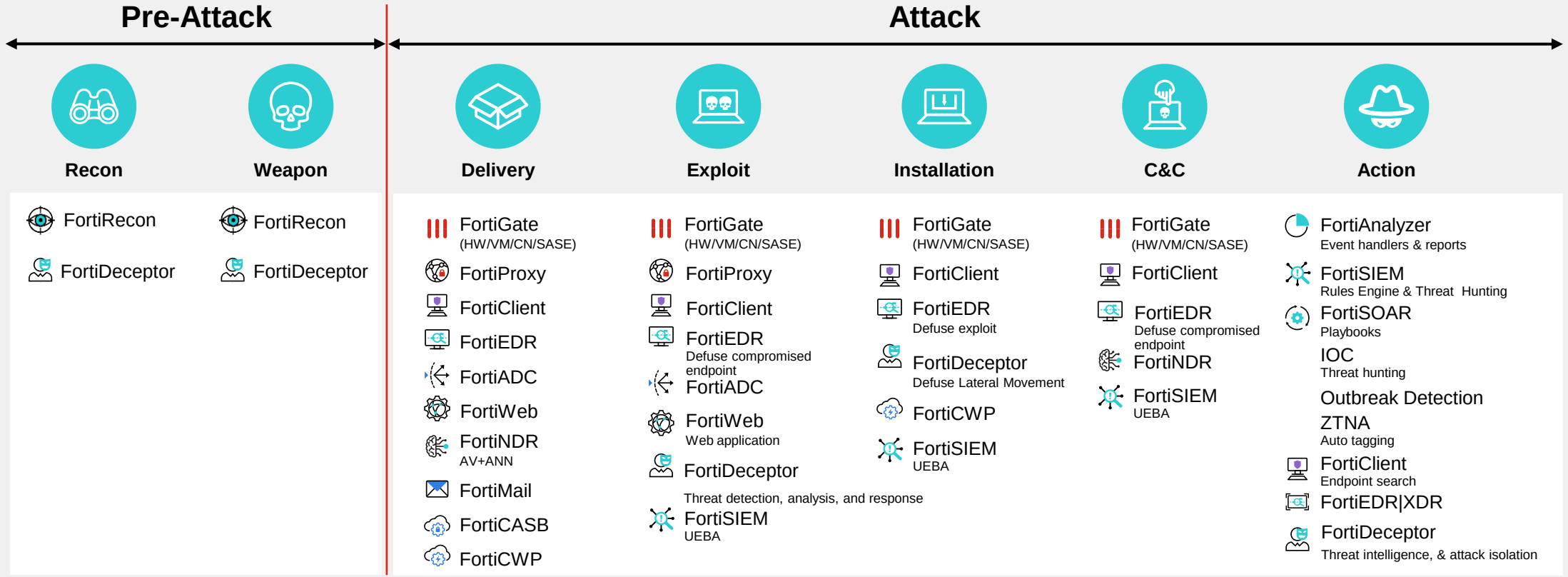
Cybercrooks are telling ChatGPT to create malicious code

Chatbot might let unskilled criminals launch attacks, if the code works



And on the Dark Web, cybercrime syndicates are ramping up their efforts, offering competitive salaries and benefits. Some jobs paid $20,000 per month, and some groups offer PTO, paid sick leave, bonuses and employee referral programs. Roles vary from full-time and part-time jobs to traineeships and partnerships.

How to Break the Attack Sequence



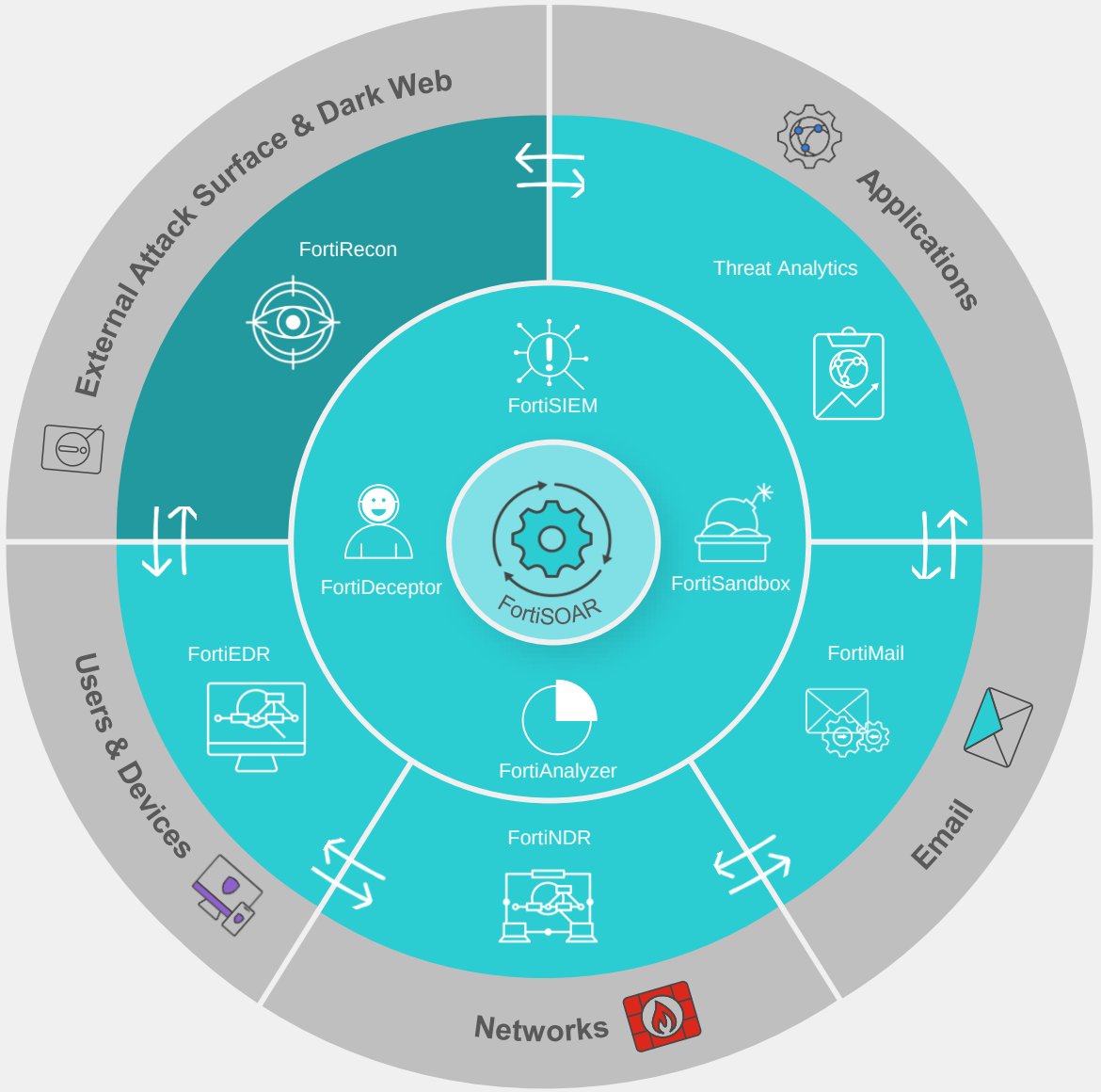
Fortinet SecOps Portfolio

A cybersecurity platform- built on AI and Automation- to accelerate time to detect and respond to cyber intrusion

Security Operations Platform

CONSOLIDATE

Consolidated security operations platform to accelerate time to detect and respond.



AI Across the Attack Surface

Monitor a specific domain, or across domains, to detect intrusion

Fabric-native Integration

Interoperate beyond industry norm, to detect *and disrupt*

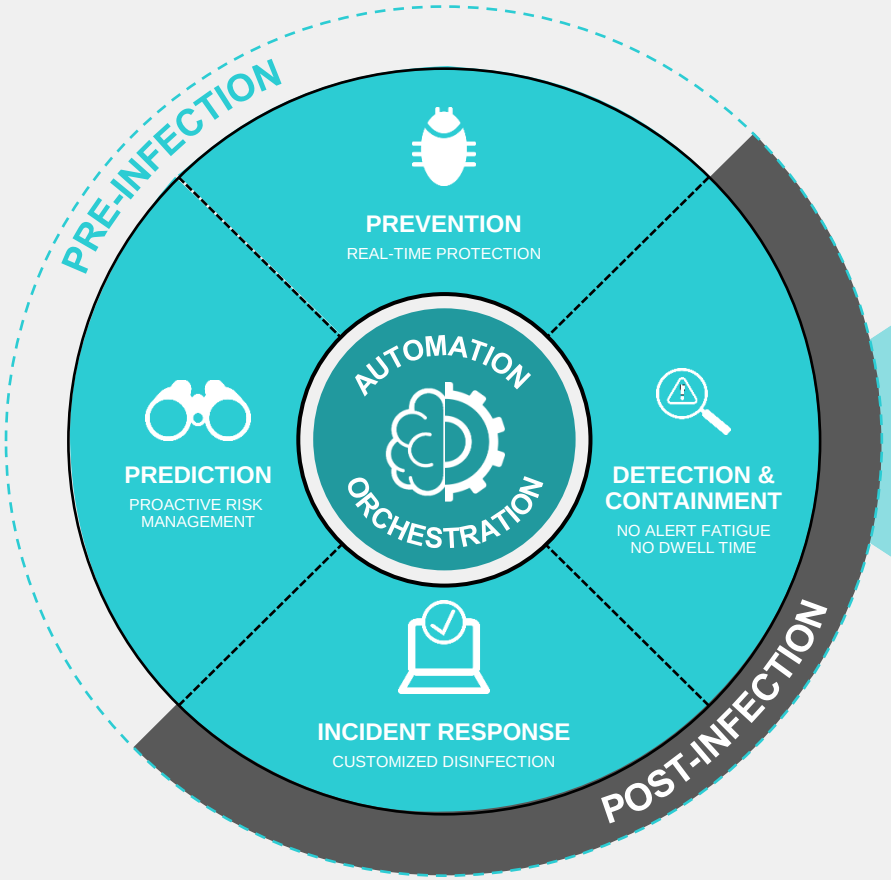
Centralized analytics and response

Orchestrate, automate and/or augment operations

AI Thoughts – Attackers Perspective

- Better, more convincing content
- Quicker route to market
- Wider spread of attacks with less effort
- More likely re-use of malicious code fragments
- Quicker Search Engine Optimisation
- Just another tool to use
- More pay days more regularly

AI Thoughts – Businesses Perspective



- Analyse greater amounts of data more quickly
- Endpoint behavioural understanding
- Improve zero day exploit detection
- Increase automation efficiencies
- Focus on integration/lower gaps in visibility
- The kill chain is still critical to disrupt
- Drive down TTD and TTR metrics
- Don’t write off existing investments!
- Focus – MFA, training, email, endpoint, remote users
- Investigate Digital Risk Protection Services


FORTINET