FORTINET

What You Need to Know About Bill C-26

Compliance & Security Operations Maturity

Fortinet in Alberta

Calgary

Number of Employees: 40

Sales – Account and Channel Managers, Marketing, Security Experts, and Specialists Teams, Technical Support, Professional Services, Software Development, Training

Number of Leadership: 6

- Gordon Phillips - Vice President, Western Canada
- Scott Hay - Regional Director of Sales, Mid Enterprise, Western Canada
- Nahid Asani – Regional Director of Presale Security Experts, Western Canada
- Sean Weiss – Business Development Engineering Manager, Canada
- Kofi Ahulu, Manager of Presales Security Experts, Enterprise, Western Canada
- Genevieve Marcoux, Manager, Technical Training

Edmonton

Number of Employees: 14

Sales – Account and Channel Managers, Security Experts, Specialist Teams, Training, Professional Services and Software Development

Number of Leadership: 2

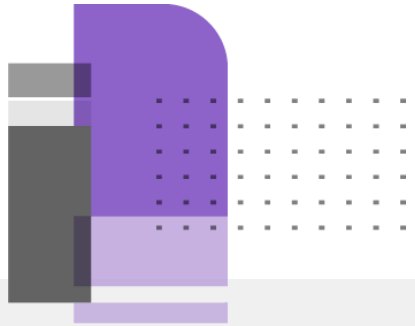
- Shane McMillian – Regional Director of Sales, Public Sector, Western Canada
- Stephen Estephan – Manager of Presales Security Experts, Public Sector, Western Canada

TOTAL

Number of Customers: **2520**

Number of Staff: **54**

Number of Leadership: **8**



Top Cybersecurity company in

Alberta and Canada

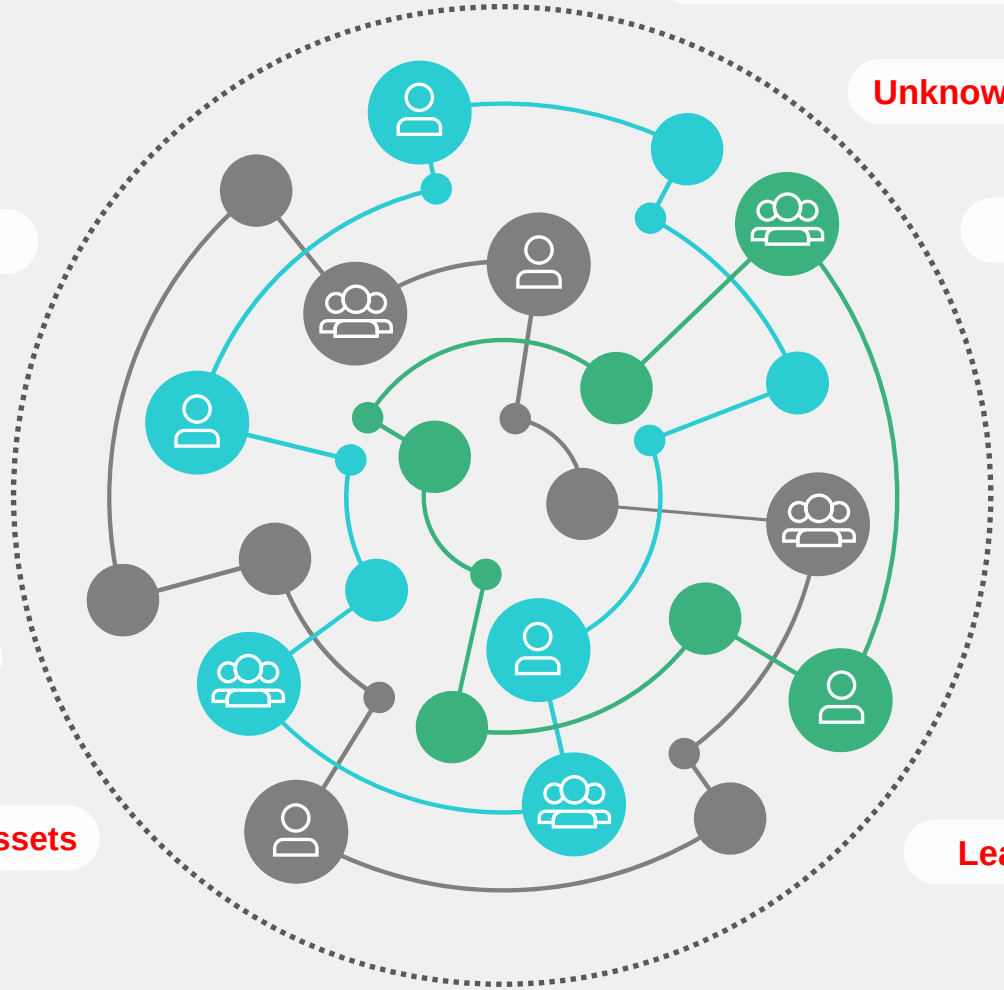
2500 +

Employees Canada Wide

In Canada, Fortinet protects all types of organizations, including governments, major banks, telecommunications providers, healthcare organizations, and many others across

sectors including natural resources, utilities, education, and manufacturing

The Ever-Expanding External Threat Landscape



Phishing, DDoS

Unknown/Unmanaged digital assets

Rogue mobile apps

Fraudulent domains

Exposed services

Fake social media accounts

Leaked credentials

Third-party, publicly-exposed digital assets

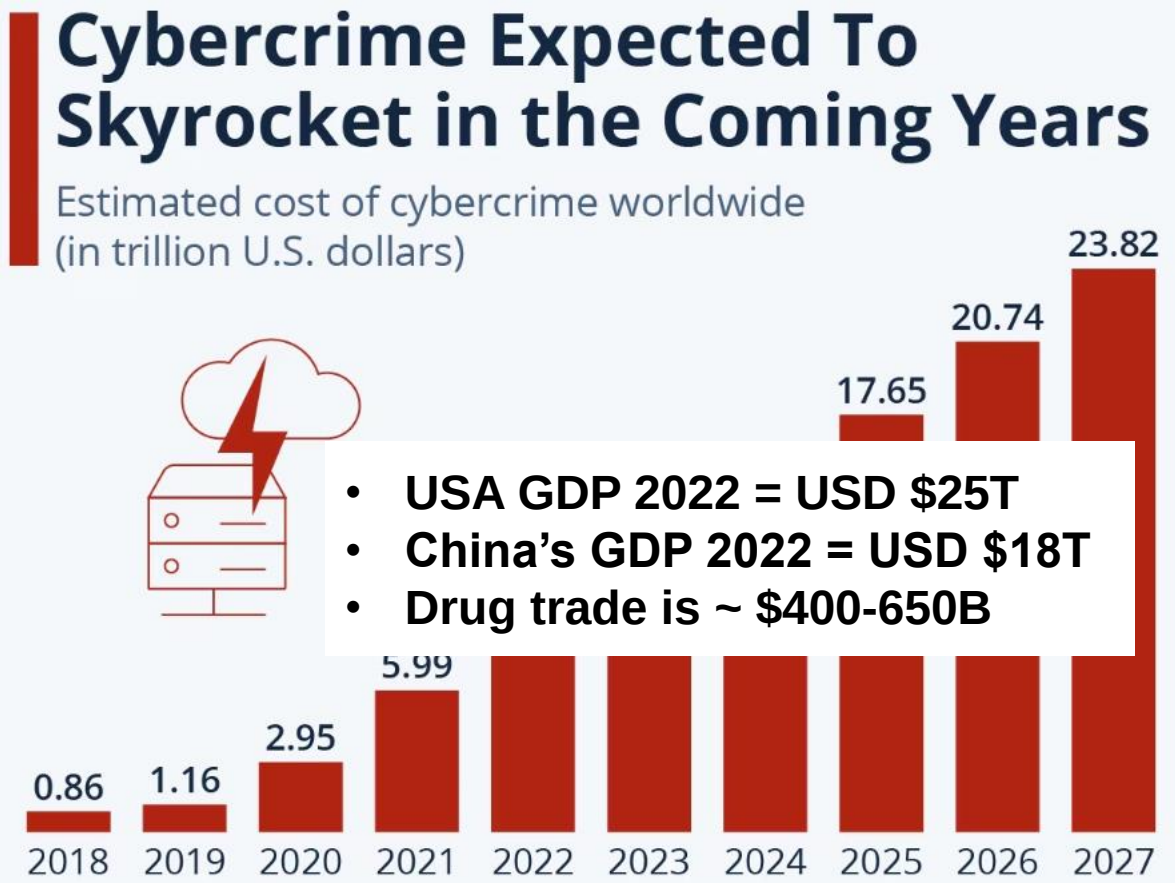
Misconfigurations

Unsecured secrets

Ransomware

Vulnerabilities

Cost of Cybercrime



$9.44M

Average cost of a data breach in the United States

The annual cost of cybercrime to the global economy is estimated to have reached **€5.5 trillion** at the end of 2020.

- European Commission (2021)

Challenge: Securing Operational Technology

- Most industrial control systems lack security by design and are sensitive to change.
- The attack surface for cyber-physical assets is expanding as a dependence on air-gap protection diminishes with Digital Transformation initiatives driving IT-OT network convergence.
- Increasing adoption of new technologies, such as 5G, IoT, and Cloud.
- Remote access requirements for third-parties and employees causing additional risks.
- Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks.
- Asset owners must comply with industry-specific regulations

Canadian Center for Cyber Security

On cybersecurity risks to OT

[There is] an increase in use of malware that directly targets and disables OT. Cybercriminals have developed OT-specific ransomware, and state-sponsored actors have demonstrated the capacity to deploy malware against critical infrastructure to degrade [and] damage OT and IT assets.

– National Cyber Threat Assessment 2023-2024

[There is] an increase in use of malware that directly targets and disables OT. Cybercriminals have developed OT-specific ransomware, and state-sponsored actors have demonstrated the capacity to deploy malware against critical infrastructure to degrade [and] damage OT and IT assets.

– National Cyber Threat Assessment 2023-2024

CCSC: Identified Trends

Accelerated development[1]
Cryptocurrency, machine learning, decryption, advanced exploits

State-sponsorship[1]
“The […] cyber programs of China, Russia, Iran, and North Korea pose the greatest strategic cyber threats to Canada”

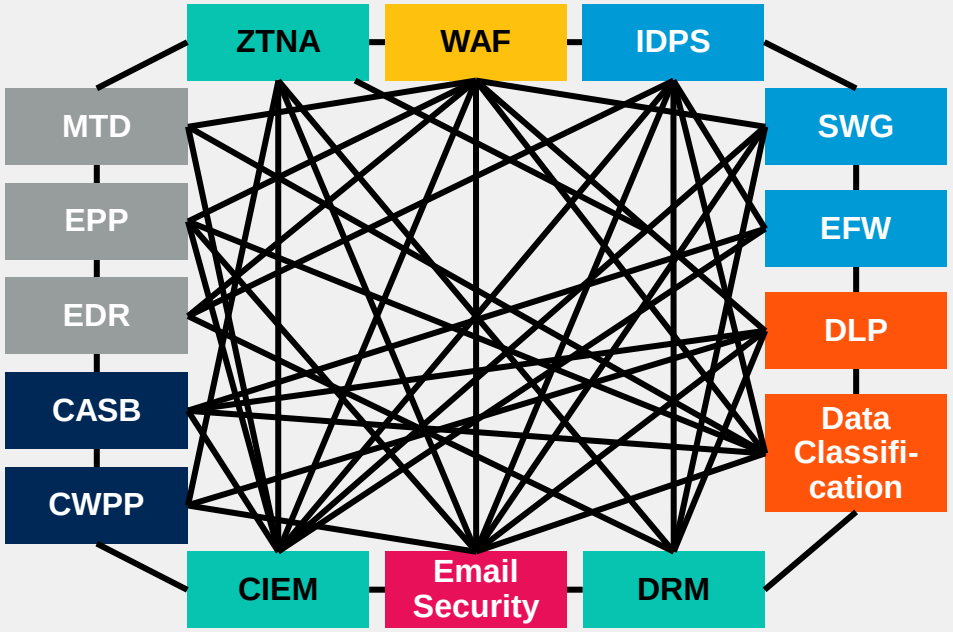
Target trends[1]
“State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities”

1. Canadian Center for Cyber Security (2022), *National Cyber Threat Assessment 2023-2024*

Image: Jerry Wang (2021), **Dr Strangelove Nicolas Cage**, Youtube.com

Cybersecurity Mesh Architecture: **Wholistic Security Coverage**

Gartner®



Executive Guide to Cybersecurity Mesh, 2022

Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

Secure Connectivity
Digital Transformation requires secure data sharing from OT to Data Centers and Cloud

Secure Remote Access
Zero-trust access for authorized remote technicians and third-parties

Converged Security Operations
Synergistically manage security across networks in a converged SOC.

AI-powered Security Services
Enable security solutions to stay ahead of evolving threats

Fortinet Security Fabric

Broad

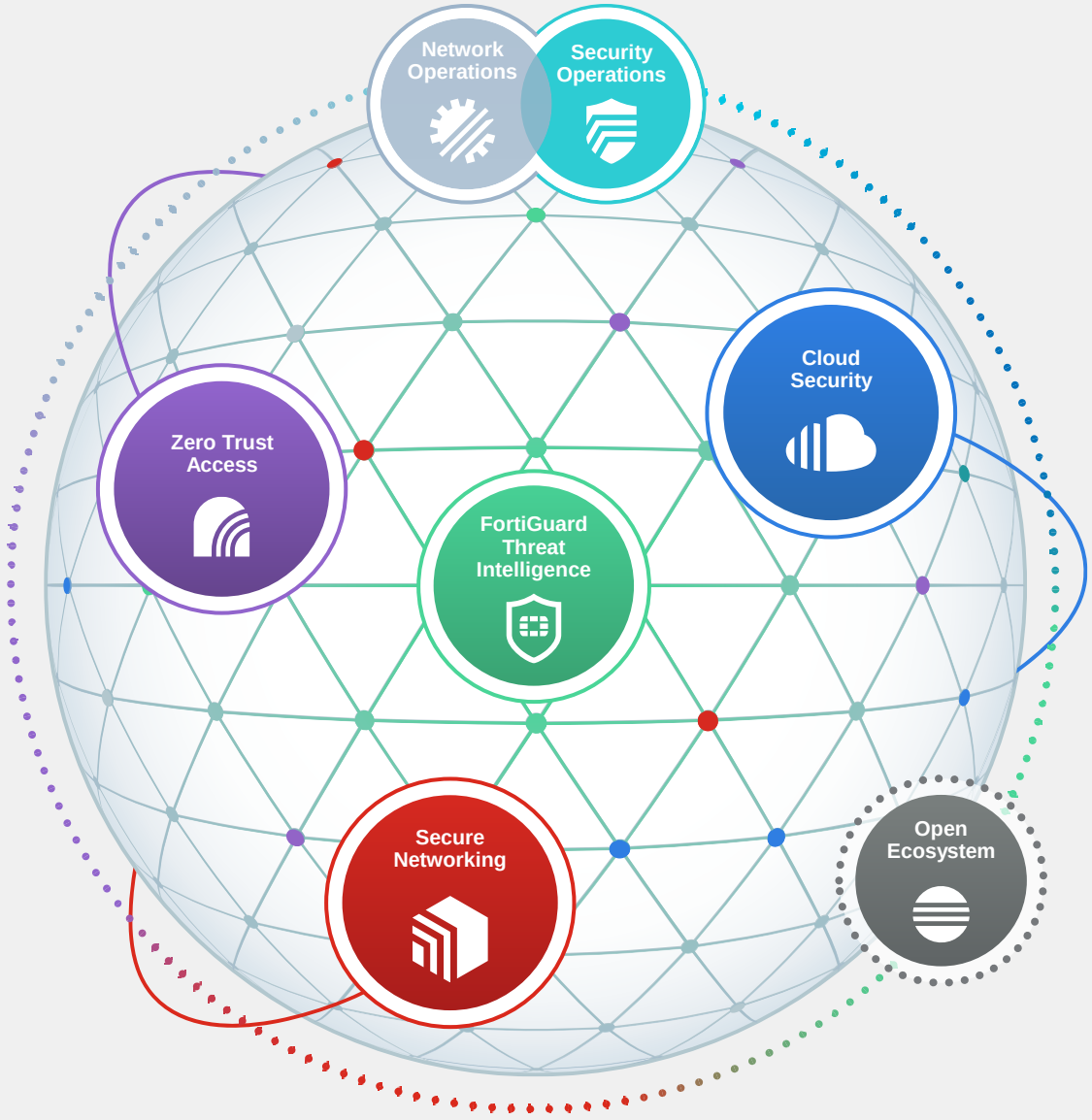
Visibility and protection of the entire digital attack surface to better manage risk

Integrated

Solution that reduces management complexity and shares threat intelligence

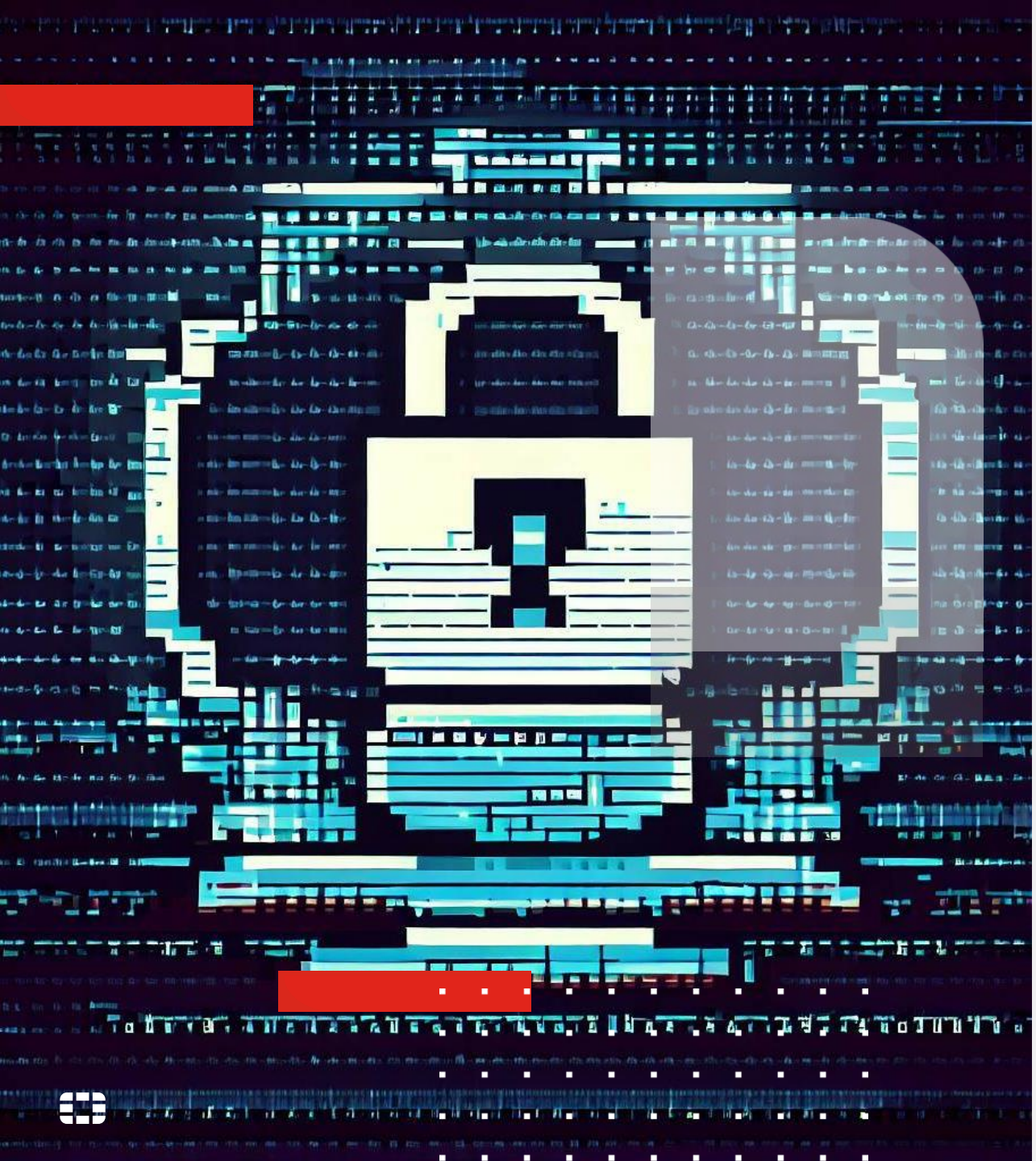
Automated

Self-healing networks with AI-driven security for fast and efficient operations



Bill C-26

An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts



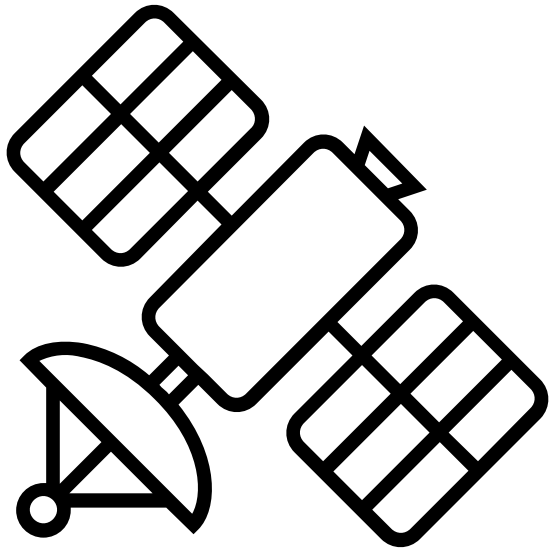
Bill C-26

- Introduced June 14, 2022
- Currently in consideration by the Committee on Public Safety and National Security
- “To [enhance] the security and resilience of the critical cyber systems of the […] private sector”
- Read it yourself: [Bill C-26 - Parliament of Canada]

Image: DALL-E (2023), **cybersecurity legislation for critical infrastructure, pixel art**

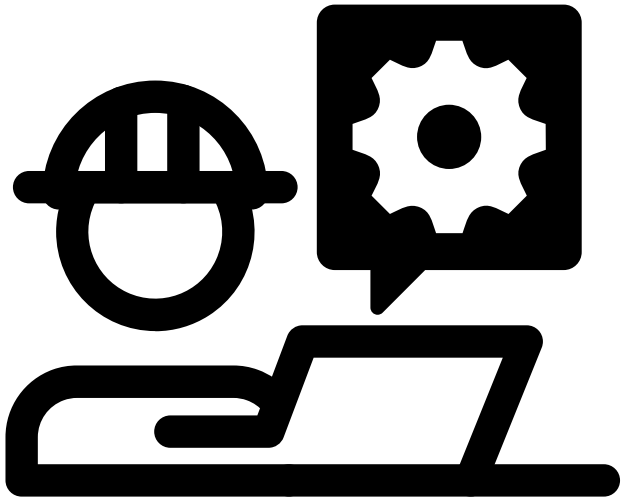
Bill C-26: A bill in two parts

Part 1: Telecommunications Act



- Amendments to the existing Telecommunications Act
- Tl;dr: the Federal Cabinet can require a telco to do or not do something (broadly)
- Financial penalties up to $15,000,000 per day

Part 2: Critical Cyber Systems Protection Act



- A new Act for critical operators
- Tl;dr: implement a cyber security program and do or not do something (broadly) as defined by the regulator
- Financial penalties up to $15,000,000 per day

Part 1

Amendments to the Telecommunications Act

Why? Huewai

Security of Canadian telecommunications system

15.1 (1) If, in the opinion of the Governor in Council, it is necessary to do so to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption, the Governor in Council may, by order,

(a) prohibit a telecommunications service provider from using all products and services provided by a specified person in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities; or

(b) direct a telecommunications service provider to remove all products provided by a specified person from its telecommunications networks or telecommunications facilities, or any part of those networks or facilities.

AKA the Federal Cabinet

Prohibit the future purchase or use of a product, service, or provider

Require the removal of an existing product, service, or provider

Security of Canadian telecommunications system

15.2 (1) If, in the Minister's opinion, it is necessary to do so to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption, the Minister may, by order and after consultation with the Minister of Public Safety and Emergency Preparedness,

(a) prohibit a telecommunications service provider from providing any service to any specified person, including a telecommunications service provider; and

(b) direct a telecommunications service provider to suspend providing for a specified period any service to any specified person, including a telecommunications service provider.

AKA the Minister of Industry

Prohibit delivering a service to any party

Require the suspension of service to any party for a fixed period

Orders from the Minister of Industry

15.2 (2) The Minister may, by order, **direct a telecommunications service provider to do anything or refrain from doing anything** — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption.

AKA the Minister of Industry

What can be ordered?

(c) impose conditions on a telecommunications service provider's use of any product or service, or any product or service provided by a specified person, including a telecommunications service provider;

(d) impose conditions on a telecommunications service provider's provision of services to a specified person, including a telecommunications service provider;

(e) prohibit a telecommunications service provider from entering into a service agreement for any product or service used in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities;

(f) require that a telecommunications service provider **terminate a service agreement** referred to in paragraph (e);

Constrain use of a product or service

Constrain service delivery

Prohibit or terminate service agreements

What can be ordered?

(g) prohibit a telecommunications service provider from upgrading any specified product or service;

(h) require that a telecommunications service provider's telecommunications **networks** or telecommunications **facilities** as well as its **procurement plans** for those networks or facilities, be **subject to specified review processes**;

(i) require that a telecommunications service provider **develop a security plan** in relation to its telecommunications services, telecommunications networks or telecommunications facilities;

(j) require that assessments be conducted to **identify any vulnerability** in a telecommunications service provider's telecommunications services, telecommunications networks or telecommunications facilities or its security plan referred to in paragraph (i);

Prohibit an upgrade

Require review

Require security planning

Identify vulnerabilities (beyond CVEs!)

What can be ordered?

(k) require that a telecommunications service provider take steps to **mitigate any vulnerability** in its telecommunications services, telecommunications networks or telecommunications facilities or its security plan referred to in paragraph (i); or

(l) require that a telecommunications service provider **implement specified standards** in relation to its telecommunications services, telecommunications networks or telecommunications facilities.

Vulnerability mitigation (beyond CVEs!)

Implement standards

"among other things"

Exchange of information

15.6 Despite section 15.5, to the extent that is necessary for any purpose related to the making, amending or revoking of an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a) — or to verifying compliance or preventing non-compliance with such an order or regulation — **the following persons and entities may collect information from and disclose information to each other, including confidential information**:

- (a) the Minister;
- (b) the Minister of Public Safety and Emergency Preparedness;
- (c) the Minister of Foreign Affairs;
- (d) the Minister of National Defence;
- (e) the Chief of the Defence Staff;
- (f) the Chief or an employee of the Communications Security Establishment;
- (g) the Director or an employee of the Canadian Security Intelligence Service;
- (h) the Chairperson or an employee of the Commission;
- (i) a person designated under section 15.4; and
- (j) any other prescribed person or entity.

Collect and share confidential info

Whomever is designated

Administrative Monetary Penalties (72.131)

(a) in the case of an **individual**, not exceeding **$25,000** and, for a subsequent contravention, not exceeding **$50,000**; or

Individuals

(b) in any other case, not exceeding **$10,000,000** and, for a subsequent contravention, not exceeding **$15,000,000**.

Businesses

Continuing violation

72.132 A violation that is continued on more than one day **constitutes a separate violation** in respect of each day during which it is continued.

Per day

73.3.1-3: Individuals include officers, directors, agents, mandataries, employees, contractors

Part 1: Summary

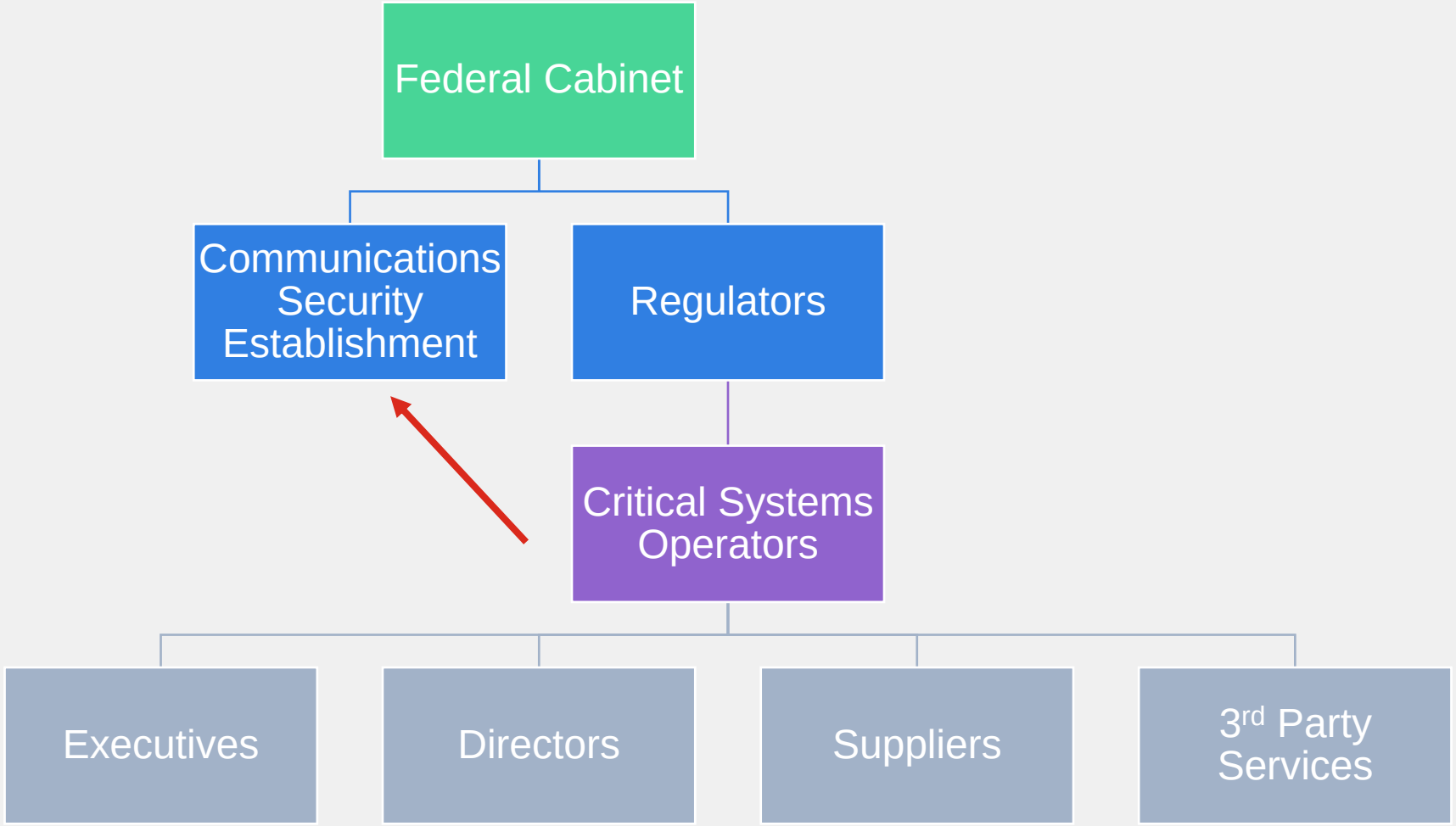
The Federal Cabinet or Minister of Industry can direct a Telecommunications provider (or their officers, directors, agents, mandataries, employees, contractors) to:

- Use or not use a product or service
- Modify or not provide a service
- Identify and mitigate vulnerabilities and cyber security risks
- Implement specific standards
- Report incidents
- Share confidential information with any designate
- Pay a monetary penalty per violation (up to $50,000 for individuals, $15,000,000 for companies – per day)

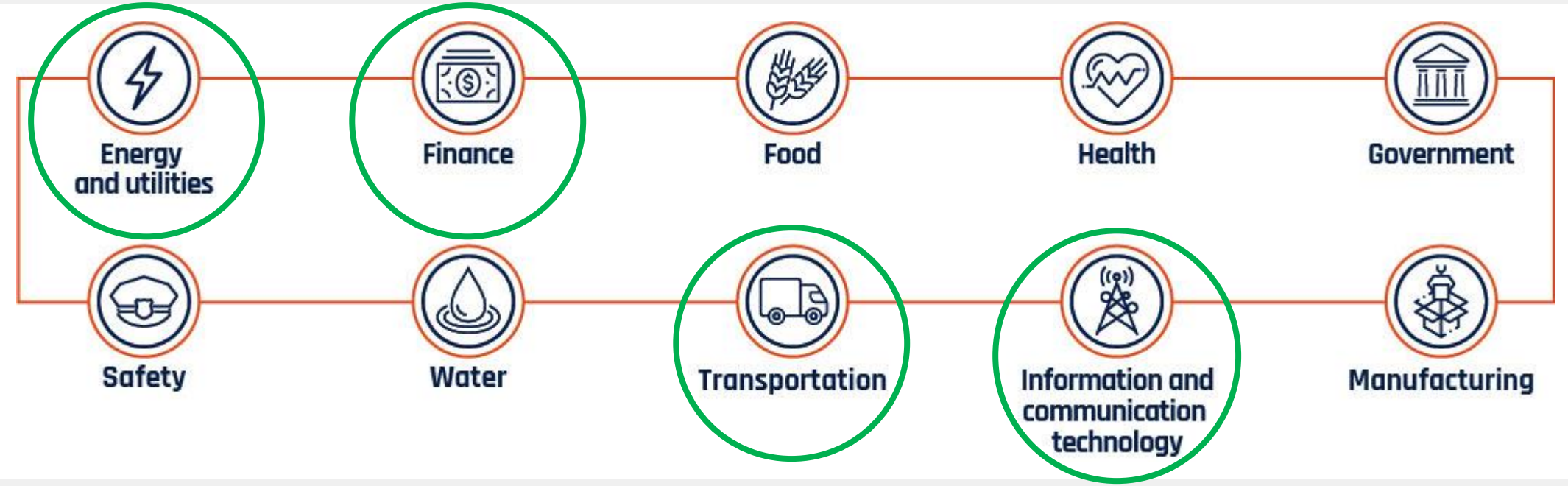
Part 2

Critical Cyber Systems Protection Act

Critical Cyber Systems Protection Act



CCSC/CSE – Critical Infrastructure Sectors



Schedule 1: Vital Services and Vital Systems

Vital Services and Vital Systems	Regulator
Telecommunications services	Minister of Industry
Interprovincial or international pipeline and power line systems	Canadian Energy Regulator
Nuclear energy systems	Canadian Nuclear Safety Commission
Transportation Systems that are within the legislative authority of Parliament	Minister of Transport
Banking systems	Office of the Superintendent of Financial Institutions
Clearing and settlement systems	Bank of Canada

Obligations of the Designated Operators of Critical Cyber Systems

8 A designated operator that owns, controls or operates a critical cyber system **must comply with the requirements of this Act** and the regulations with respect to that critical cyber system.

1. **Establish a cyber security program** within 90-days
2. Provide the program to the appropriate regulator
3. Implement and maintain the program
4. Review the program at least annually
5. **Mitigate supply-chain and third-party risks**
6. **Immediately report cyber security incidents**
7. Comply with any direction from the Federal Cabinet
8. Submit to inspection

Report to the Communications Security Establishment (CSE), then notify the appropriate regulator

Establish a Cyber Security Program

9 (1) After an order that is made under section 7 is published in the *Canada Gazette*, Part II, a designated operator that belongs to a class of operators set out in Schedule 2 **must, within 90 days** after the day on which the designated operator becomes a member of that class, establish a cyber security program in respect of its critical cyber systems and include in the program reasonable steps to, in accordance with any regulations,

(a) identify and manage any organizational cyber security risks, **including risks associated with the designated operator's supply chain** and its use of **third-party products and services**;

(b) protect its critical cyber systems from being compromised;

(c) detect any cyber security incidents affecting, or having the potential to affect, its critical cyber systems;

(d) minimize the impact of cyber security incidents affecting critical cyber systems; and

(e) do anything that is prescribed by the regulations.

- Vulnerabilities
- CVEs
- Credential exposure
- Insecure perimeter
- MFA
- Phishing
- Incident Response
- SOC / NOC
- Risk assessment
- Pentesting
- EDR
- Ingress / egress profiling
- Trust boundaries
- Microsegmentation

Mitigation of Supply-chain and Third-party Risks

15 As soon as **any cyber security risk** associated with the designated operator's **supply chain** or its use of **third-party products and services** has been identified under paragraph 9(1)(a), **the designated operator must take reasonable steps**, including any steps that are prescribed by the regulations, **to mitigate those risks**.

14.1.b: Regulator must be notified of any changes

Examples of supply-chain & third-party products and services:

- Contractors
- Equipment
- PaaS
- Resellers
- SaaS
- Service providers / MSSP
- Suppliers

Regulating Planning, Auditing & Reporting

135 The Governor in Council may make regulations for carrying out the purposes and provisions of this Act, including regulations

AKA the Federal Cabinet

(a) respecting **cyber security programs**;

(b) respecting any condition and criteria respecting **internal audits**;

(c) respecting **the form and manner for reporting** any cyber security incidents referred to in section 17 and the types of incidents that must be reported;

(d) respecting **the management of records** referred to in section 30, including the collection, use, retention, disclosure and disposal of those records;

(e) designating any provision of this Act or of the regulations made under this Act for the purposes of section 90;

(f) classifying each violation as a minor violation, a serious violation or a very serious violation;

(g) fixing the maximum penalty in respect of each violation;

(h) defining, for the purposes of this Act, any word or expression that is used in this Act but is not defined; and

(i) prescribing anything that is to be prescribed under this Act.

Administrative Monetary Penalties

Penalty

91 The amount that may be fixed under any regulations made under paragraph 135(g) as the penalty for a violation must not be more than

(a) $1,000,000, in the case of an individual; and

(b) $15,000,000, in any other case.

Continuing violation

94 A violation that is committed or continued on more than one day **constitutes a separate violation** in respect of each day on which it is committed or continued.

Per day

93: Individuals include any director or officer of the designated operator

Part 2: Summary

The Federal Cabinet or Minister of Industry can direct a critical systems operator (or their officers, directors, agents, mandataries, employees, contractors) to:

- Do or not do anything
- Implement a cybersecurity program
- Identify and mitigate vulnerabilities and cyber security risks, including those stemming from 3rd parties and supply-chains
- Report incidents to the CSE
- Report on changes to the cybersecurity program, including any risks or vulnerabilities identified, and steps taken to mitigate the same, to the appropriate regulator
- Share confidential information with any designate
- Pay a monetary penalty of up to $15 million per violation, per day

Critical Cyber Systems Protection Act

Principal Requirements

Reputable Vendors / Services / Suppliers

Cybersecurity Plan

Mitigate 3rd Party & Supply Chain Risk

Protection, Monitoring, Detection, and Response

Reporting, Audit, and Assessment

Security Operations

Some Fundementals

The Current Approach to Detection & Containment is Inadequate

197 days

Average time to identify a breach[1]

70 days

Average time to recover from a breach[1]

15 minutes

On average until cybercriminals begin automated scanning & exploitation of new CVEs[2]

<5 hours

Time from initial access to domain compromise for more than 60% of hackers[3]

<5 days

Dwell time before ransomware deployment[4]

1. https://techjury.net/blog/data-breach-statistics/
2. https://www.acronis.com/en-us/cyber-protection-center/posts/report-attackers-scan-for-vulnerabilities-within-15-minutes-of-cve-disclosure/
3. https://www.computerweekly.com/news/252525373/Most-hackers-exfiltrate-data-within-five-hours-of-gaining-access
4. https://www.bleepingcomputer.com/news/security/ransomware-hackers-dwell-time-drops-to-5-days-rdp-still-widely-used/

Shortcomings in Incident Response

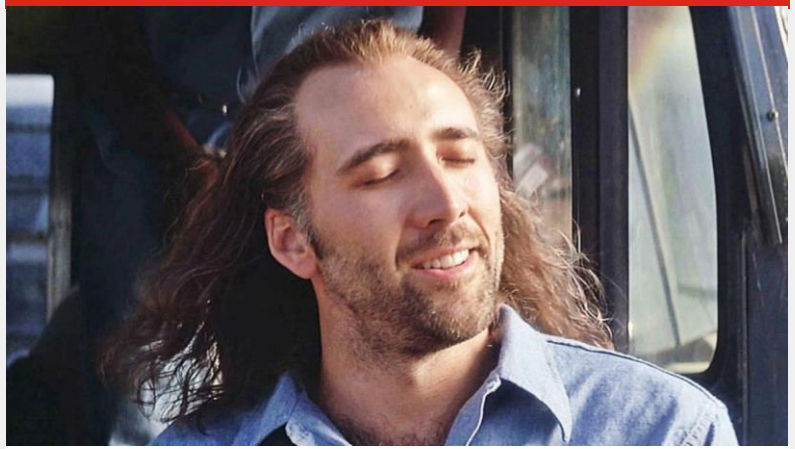
Conventional incident response methods fail to mitigate the risk posed by APTs because they make two flawed assumptions:
***response should happen after the point of compromise**, and*
***the compromise was the result of a fixable flaw**.*

– Lockheed Martin Corporation

https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Becoming Adequate: Knowing about knowing

Known Knowns



- Conceivable and measured
- Identified vulnerabilities
- Admin accounts
- Plans and procedures
- Detected compromise

Known Unknowns

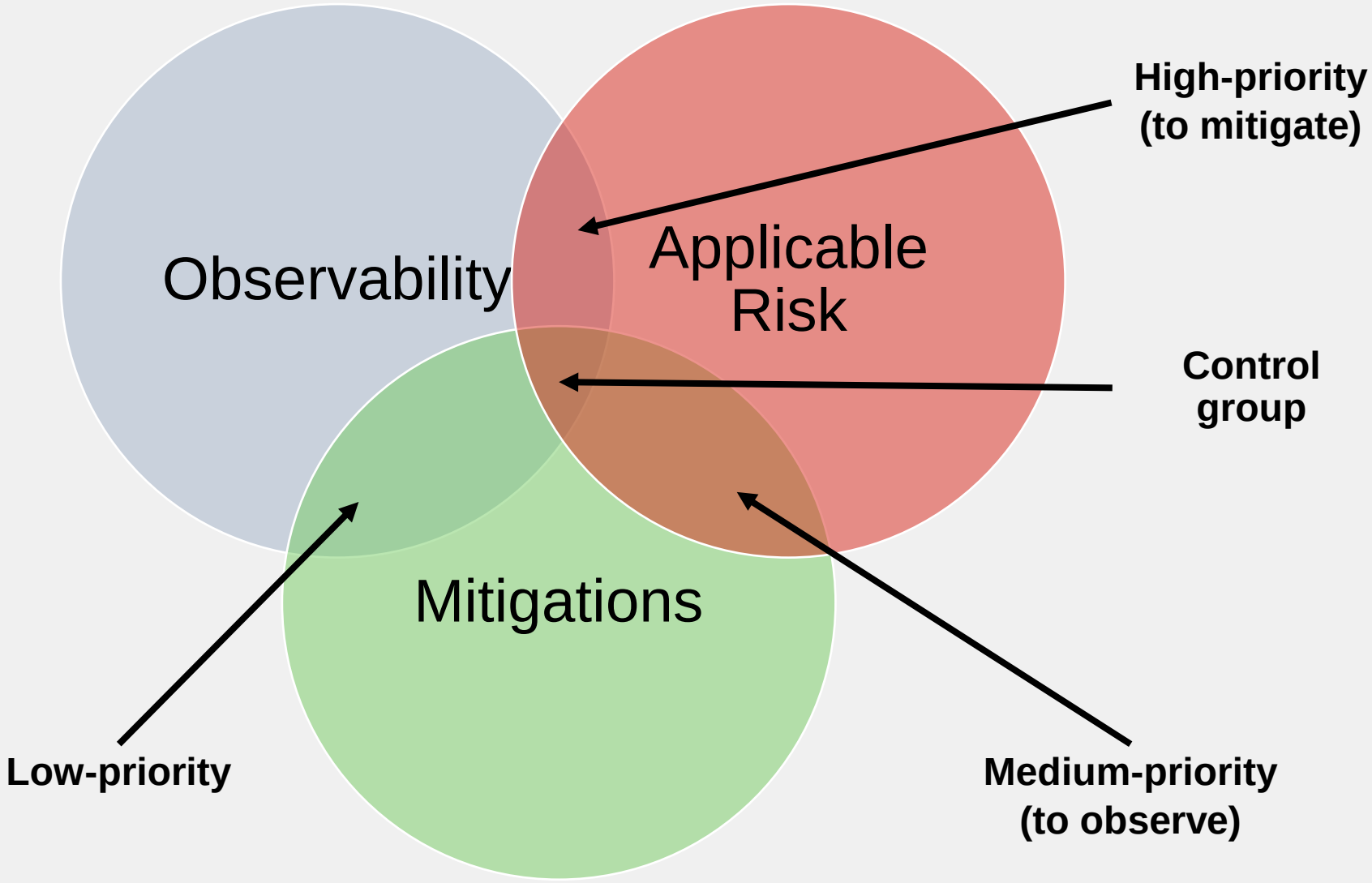
- Conceivable and **not** measured
- Unidentified, known vulnerabilities
- Compromised credentials
- Misconfigurations
- Third-party risk
- “Assume the breach”

Unknown Unknowns

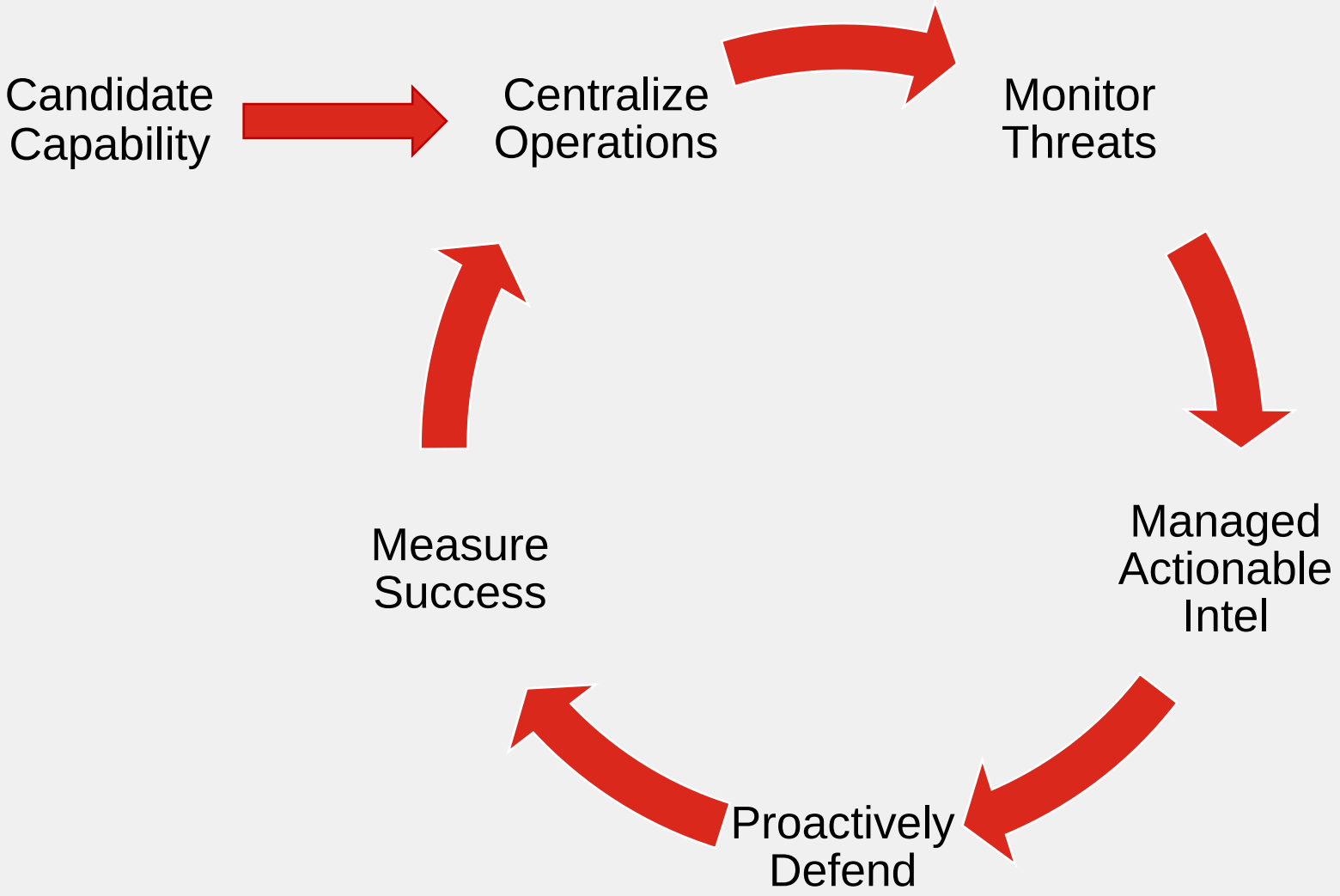
- Inconceivable and unmeasured
- Zero-days
- Unaccounted risk
- Undetected, unaccounted for compromise

Identifying Observability & Mitigation Gaps

Measure coverage against MITRE ATT&CK!



Iteratively Improving Security Operations…



https://lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html

… to Increase Security Operations Maturity

Basic
- Inventory
- Log collection
- Identify priorities

Reactive
- Detect & respond to compromise

Proactive
- Analysis
- Gap assessment
- Deceive
- Segment
- Threat modelling

Predictive
- Prevent delivery
- Countermeasures
- Mitigations
- Attack Surface Management

https://lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html

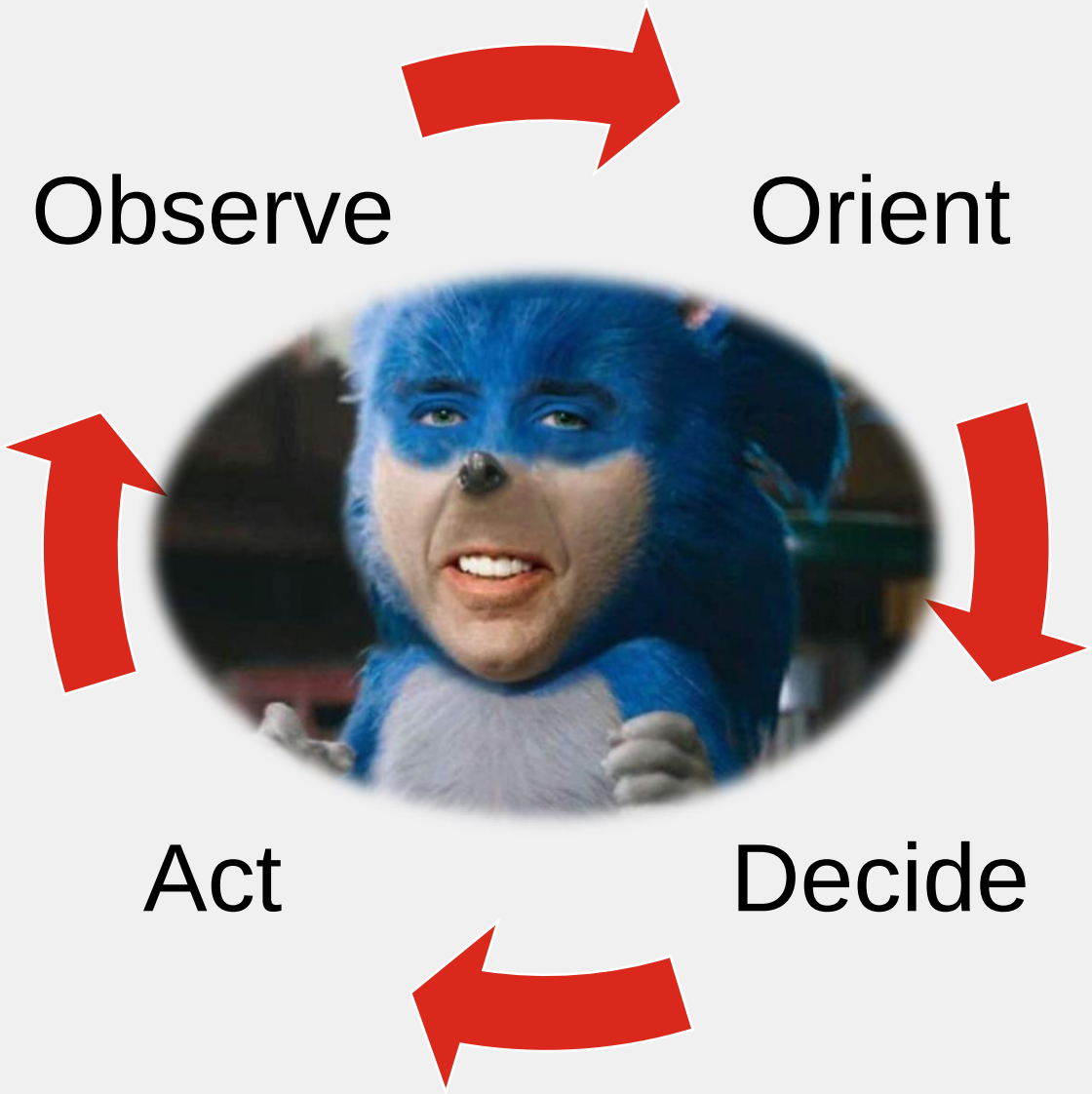
Or Simply: Respond to Threats Faster

In order for an intrusion to be economical, adversaries must re-use tools and infrastructure.

Defenders must be able to move their detection and analysis up the kill chain and more importantly to implement [mitigations] across the kill chain.

In this way, the defender increases the adversary's cost of executing successful intrusions.

– Lockheed Martin Corporation

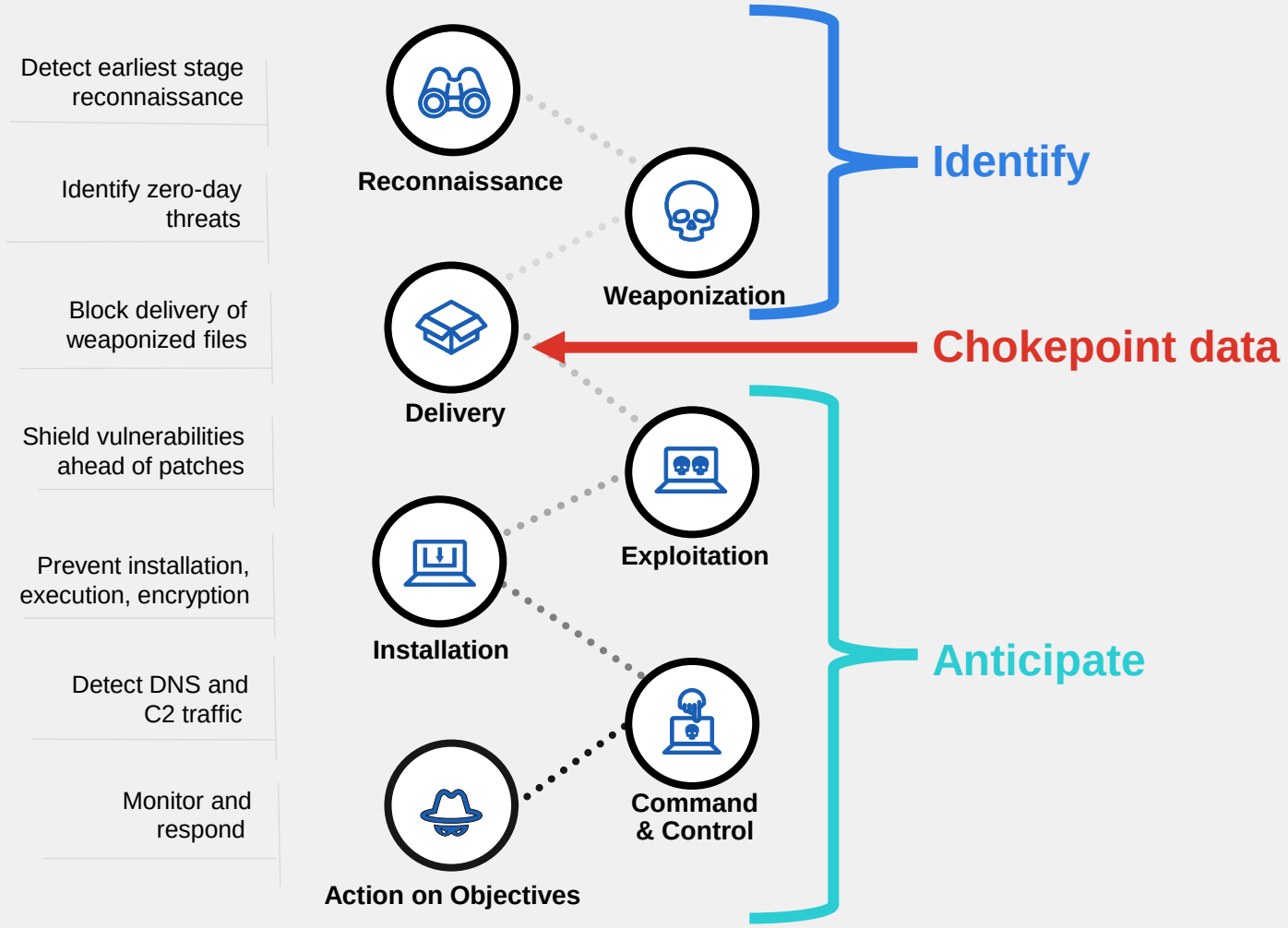


https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Improving Security Operations Maturity

Nicolas Cage will be shoehorned into this

The Security Mesh Improves Detection & Prevention



Full Coverage of the Attack Surface

Unified Security Infrastructure

NG-SOC

NGFW, Mail
WAF/ADC

1
Perimeter

Pain point

Inline Coverage Gaps	Endpoint Security	Network Blind Spots	Skills Gap	Automation Gap
				

Managed Service Options

NGFWaaS

SASE,
Managed Firewall

Protect

Delivery Analytics for Realtime Deep Inspection

Unified Security Infrastructure

NG-SOC

NGFW, Mail
WAF/ADC

1
Perimeter

Machine Learning,
Sandboxing, Outbreaks

2
Advanced
Threats

Pain point

Endpoint
Security

Network
Blind Spots

Skills
Gap

Automation
Gap

Managed Service Options

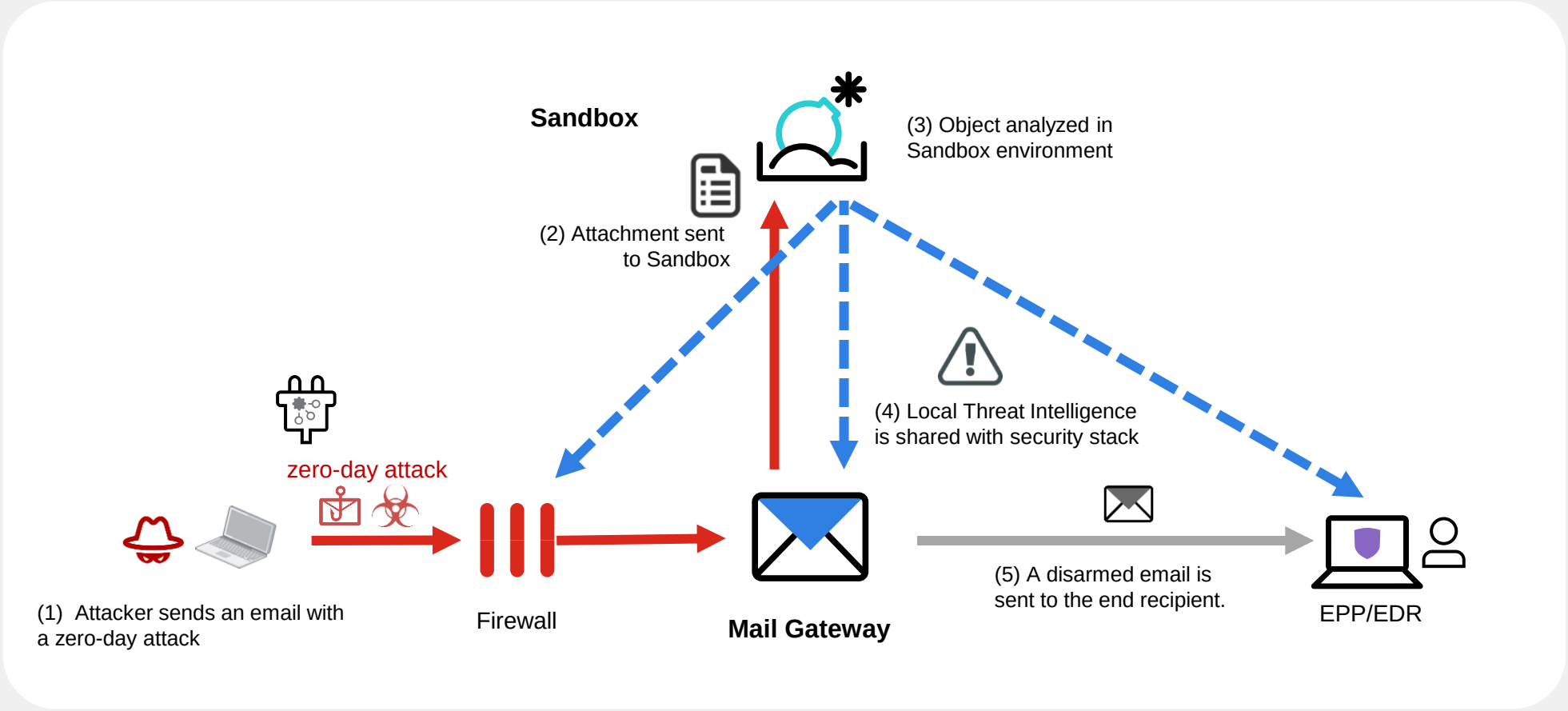
NGFWaaS

SASE,
Managed Firewall

Protect

Use Case: Fabric Based Protection

Malware via E-mail is Analyzed by Sandbox



Endpoint Security for APT Defense

Unified Security Infrastructure

NG-SOC

NGFW, Mail
WAF/ADC

1
Perimeter

Machine Learning,
Sandboxing, Outbreaks

2
Advanced
Threats

EPP
EDR

3
Endpoint
Behavior

Pain point

Network
Blind Spots

Skills
Gap

Automation
Gap

Managed Service Options

NGFWaaS

SASE,
Managed Firewall

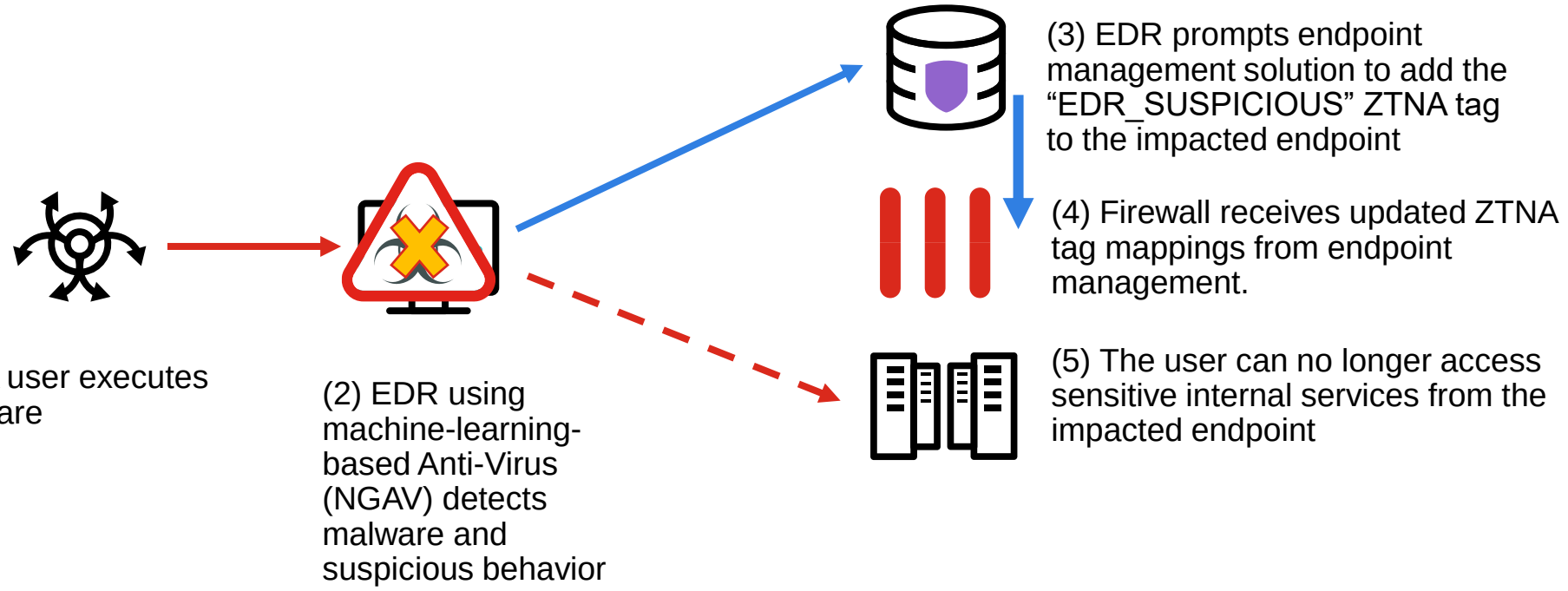
EPaaS

Managed Endpoint,
MDR, MXDR

Protect

Use Case: Fabric Based Protection

Integrated Response to Malware Execution



Network Offense using Deception and NDR

Unified Security Infrastructure

NG-SOC

NGFW, Mail WAF/ADC	Machine Learning, Sandboxing, Outbreaks	EPP EDR	NDR Deception
1 **Perimeter**	2 **Advanced** Threats	3 **Endpoint** Behavior	4 **Network** Behavior

Pain point

Skills Gap	Automation Gap
	

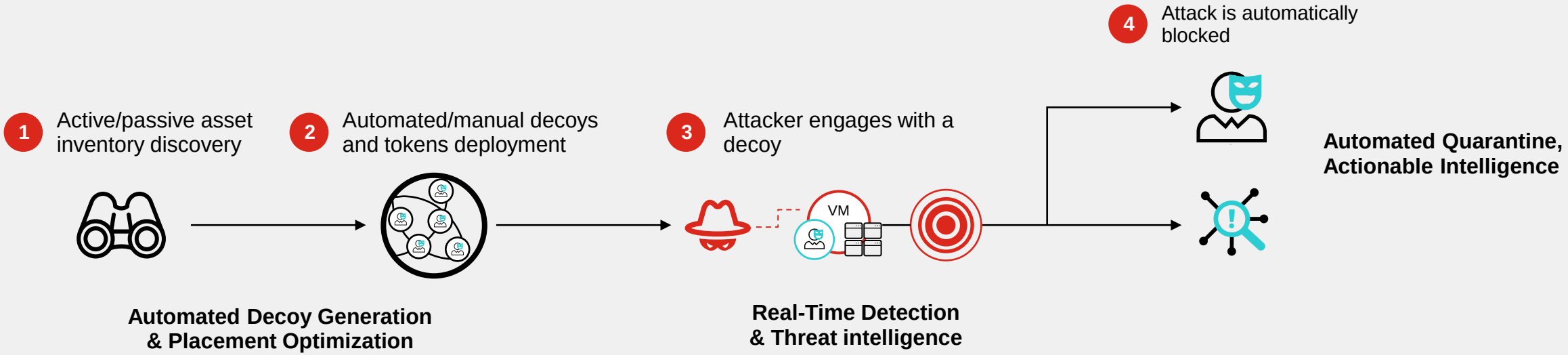
Managed Service Options

NGFWaaS	EPaaS
SASE, Managed Firewall	Managed Endpoint, MDR, MXDR

Protect

Deception Technology in Action…

Detect early. Contain cyberattacks. Reduce risk.



Comprehensive detection, closing visibility gaps, diverts attackers from sensitive assets to shift the balance to defender's advantage

Analytics, Reports & Compliance across Fabric

Unified Security Infrastructure

NG-SOC

NGFW, Mail WAF/ADC	Machine Learning, Sandboxing, Outbreaks	EPP EDR	NDR Deception	Analyzer SIEM
1 **Perimeter**	2 **Advanced Threats**	3 **Endpoint Behavior**	4 **Network Behavior**	5 **SIEM**

Pain point

Automation Gap

Managed Service Options

NGFWaaS	EPaaS	SOCaaS
FortiSASE, Managed Firewall	Managed Endpoint, MDR, MXDR	SOCaaS

Protect **Detect**

SOAR, XDR and Fabric add extended Automation

Unified Security Infrastructure

NG-SOC

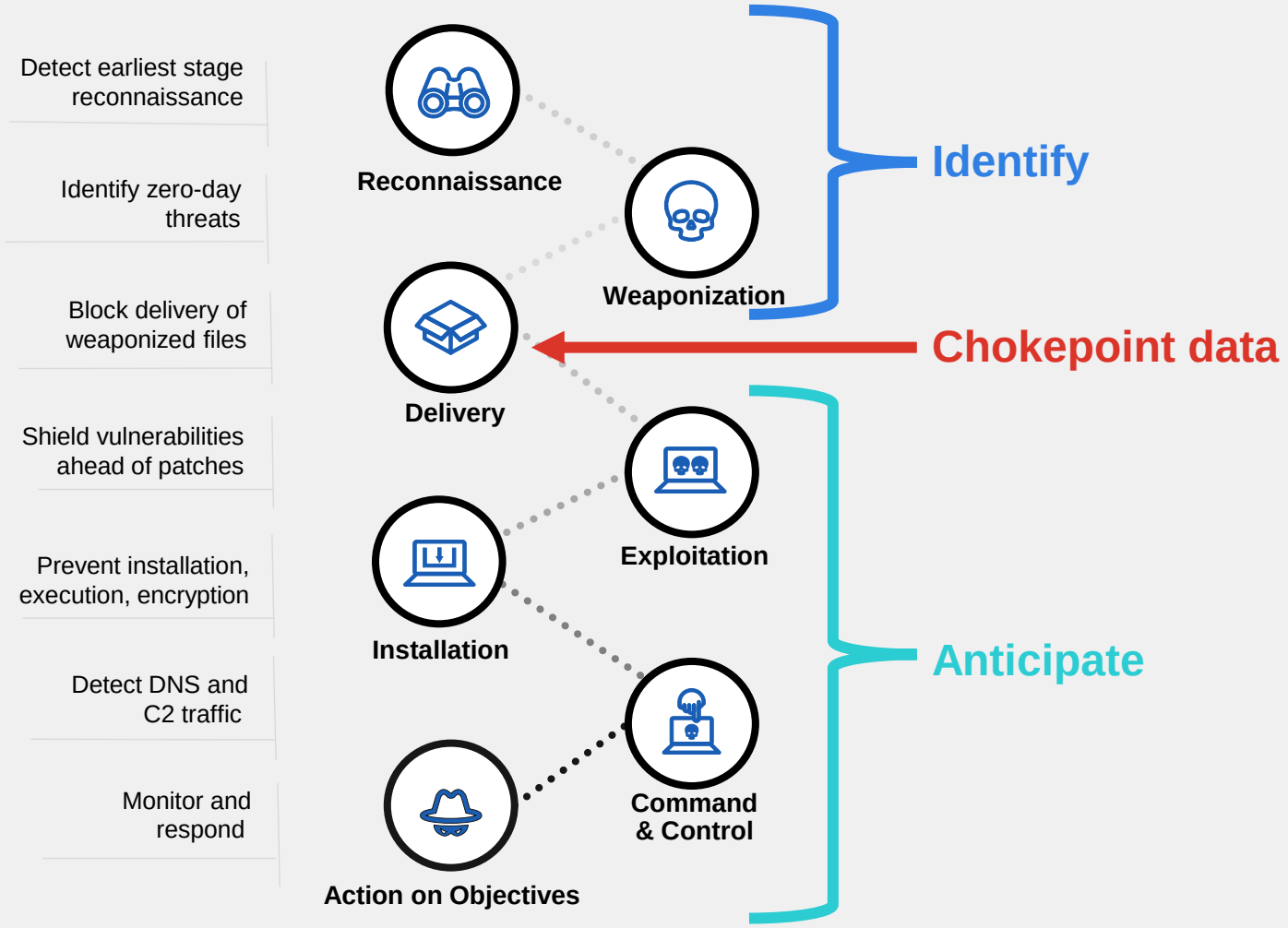
NGFW, Mail WAF/ADC	Machine Learning, Sandboxing, Outbreaks	EPP EDR	NDR Deception	Analyzer SIEM	SOAR, XDR Fabric
1 Perimeter	2 Advanced Threats	3 Endpoint Behavior	4 Network Behavior	5 SIEM	6 SOAR

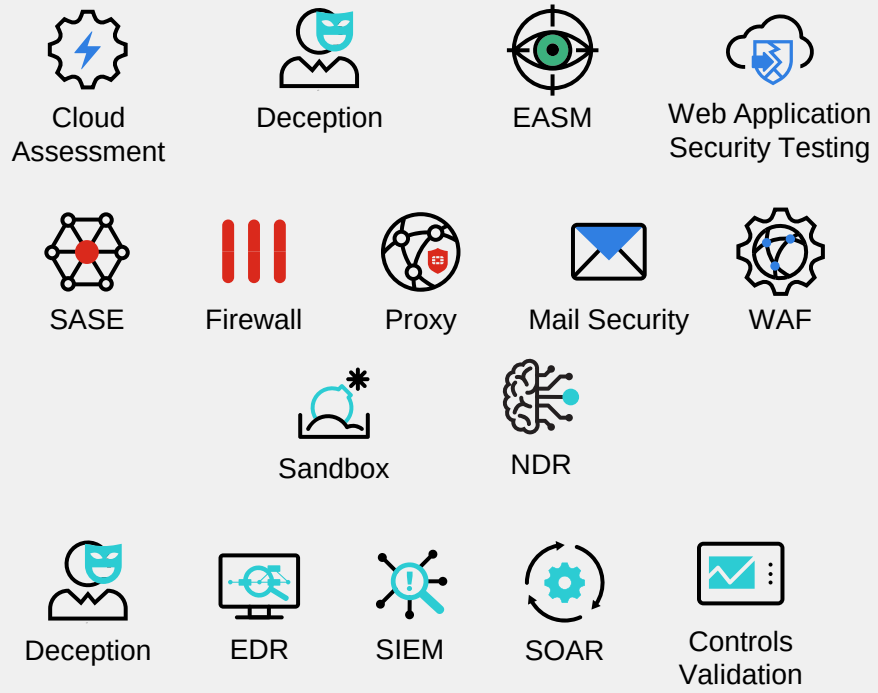
Managed Service Options

NGFWaaS	EPaaS	SOCaaS
FortiSASE, Managed Firewall	Managed Endpoint, MDR, MXDR	SOCaaS Forensics & Emergency Response Services

Protect | Detect | Respond

The Security Fabric Improves Detection & Prevention





Validate Your Ability to Observe & Block Threats

Critical Cyber Systems Protection Act

Principal Requirements

Reputable Vendors / Services / Suppliers

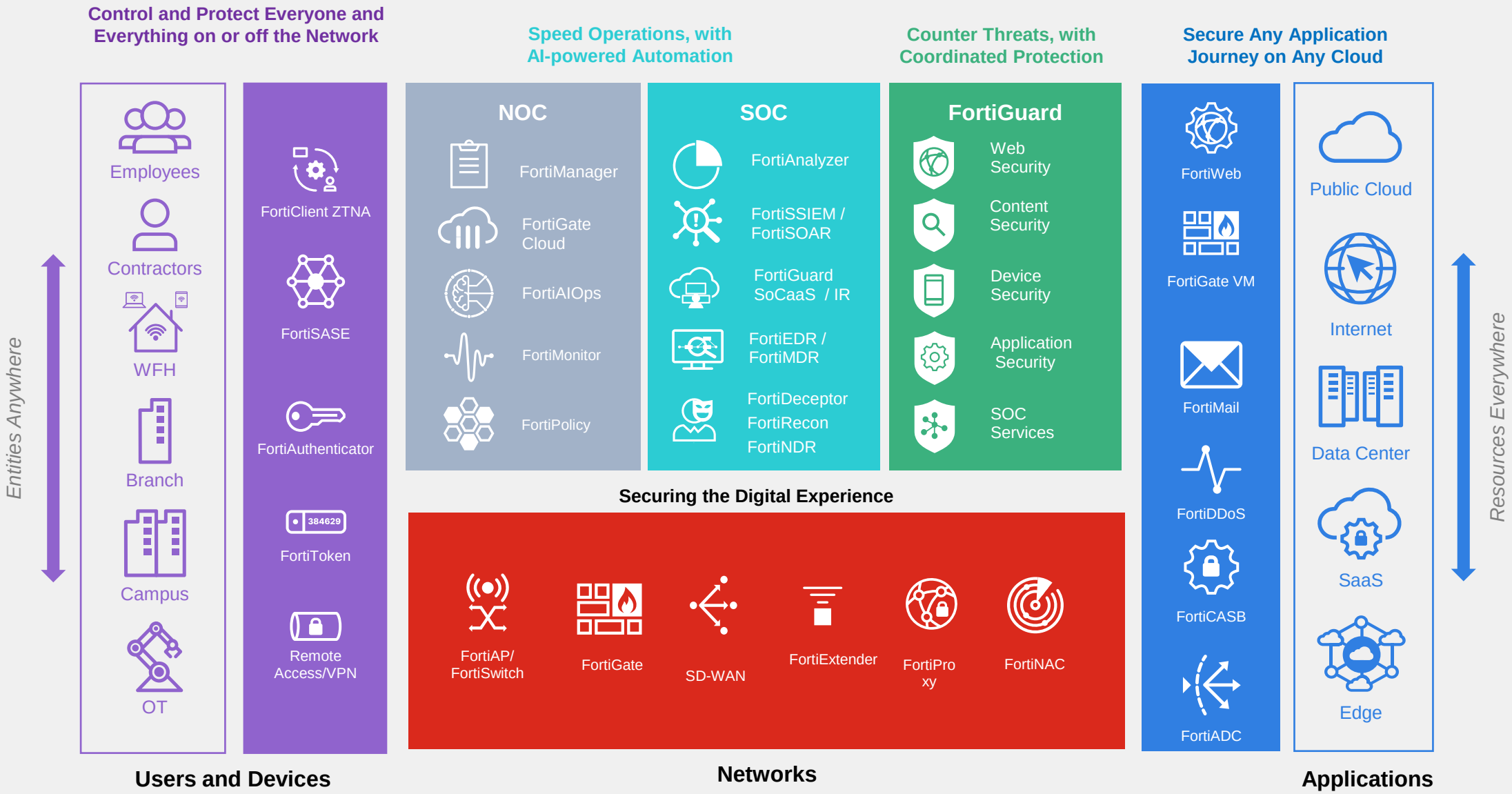
Cybersecurity Plan

Mitigate 3rd Party & Supply Chain Risk

Protection, Monitoring, Detection, and Response

Reporting, Audit, and Assessment

Fortinet Security Fabric Expansion




FORTINET