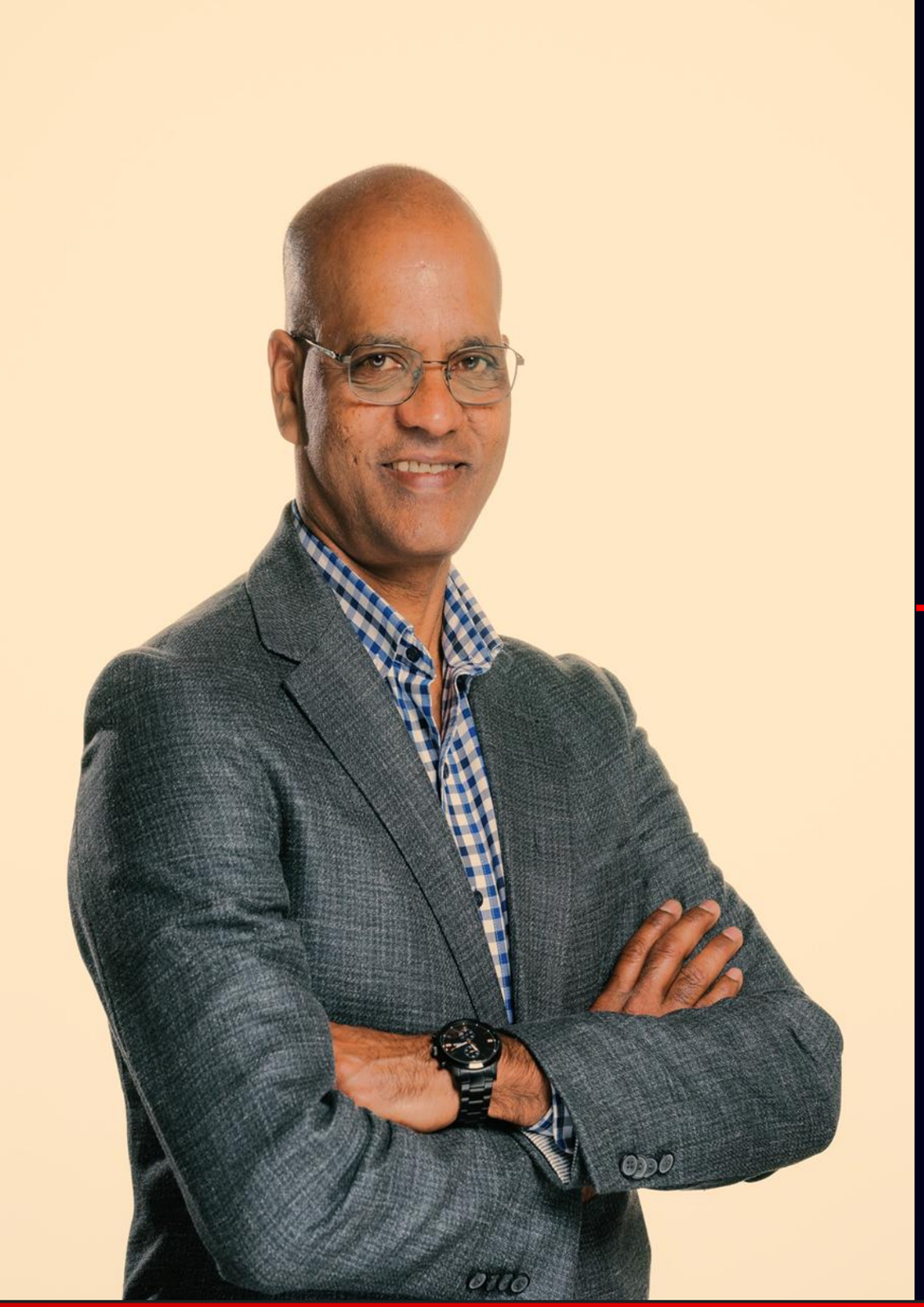


Building a Resilient Digital Caribbean: Beyond CyberSecurity: Assembling Resiliency for the inevitable Breach

Building cyber resilience and strengthening the ICT sector across the Caribbean region. Let’s explore how Hitachi Vantara's comprehensive solutions can address the unique challenges facing Caribbean nations in their digital transformation journey.

- BJ Deonarain
- Global Alliance Cyber Security Solutions Director
- Cyber Security and Resiliency

Contents and Agenda

1 Who is Hitachi
Data Driven Innovation for sustainable Future

2 What to look out for 2025
The Cyber Prowl

3 The Cyber Attack Sequence
The Kill Chain

4 Quantum
Are we there YET

5 Artificial Intelligence
Wake up one morning, and there it is

6 The Cyber Security Landscape
How it appears in the Caribbean

7 The Breaches
And the Adventure Begin

8 The Threat Actors
Evasive Chaps

9 Cyber Resiliency
Be Prepare to be operationally resilient

10 Fortify with Technology
Stay consistent with changes- Mitigate Risks

WHO IS HITACHI?

Hitachi's Focus

"...development of superior, original technology and products."

IT **60+ years**
of digital enablers and disruptive technologies

OT **110+ years**
of operational excellence and industry knowledge

Mission
Contribute to society through the development of superior, original technology and products.

Vision
Hitachi delivers innovations that answer society's challenges. With our talented team and proven experience in global markets, we can inspire the world.

Values
Hitachi founding spirit: Harmony, Sincerity and Pioneering Spirit.

Hitachi Leadership
Current & Historic

Namihei Odaira
Hitachi Founder

Toshiaki Tokunaga
President & CEO
Hitachi, Ltd.

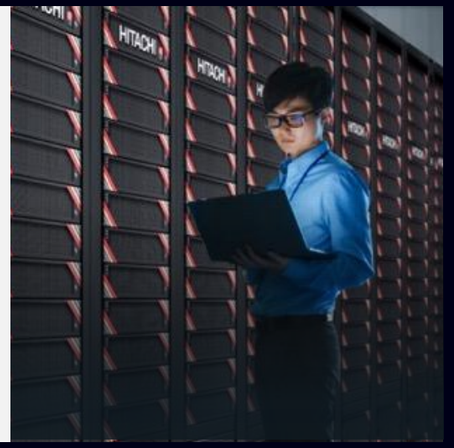
Jun Abe
CEO, DEAI business unit and DSS, and Chairman
Hitachi Vantara

Hitachi Global Business Revenue

25%
Digital Systems & Services

Including:

- Hitachi Vantara
- GlobalLogic
- Hitachi Digital Services
- Hitachi Solutions



29%
Green Energy & Mobility

Including:

- Hitachi Energy
- Hitachi Rail

30%
Connective Industries

Including:

- Hitachi High-Tech
- Hitachi Global Life Solutions
- JR Automation

16%
Others

Hitachi *Global multi-industry conglomerate*

Heritage of *Innovation*

- **$2.4B** annual R&D
- **$3.7B** 3-year investment in AI and digital
- **$18B** revenue from IT sector
- **182,000** global patents

Fortune 500
Top 11 global tech company by revenue

19
Customer co-creation centers

$300M
Corporate venture fund for digital and AI

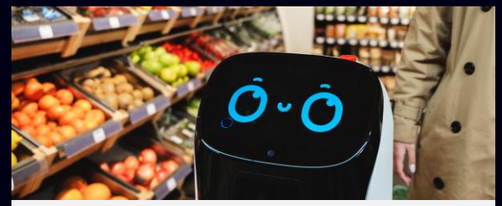
Top 100
Clarivate Global Innovators

268k
Employees

$67B
Consolidated revenue

Co-Create with

The Hitachi Ecosystem

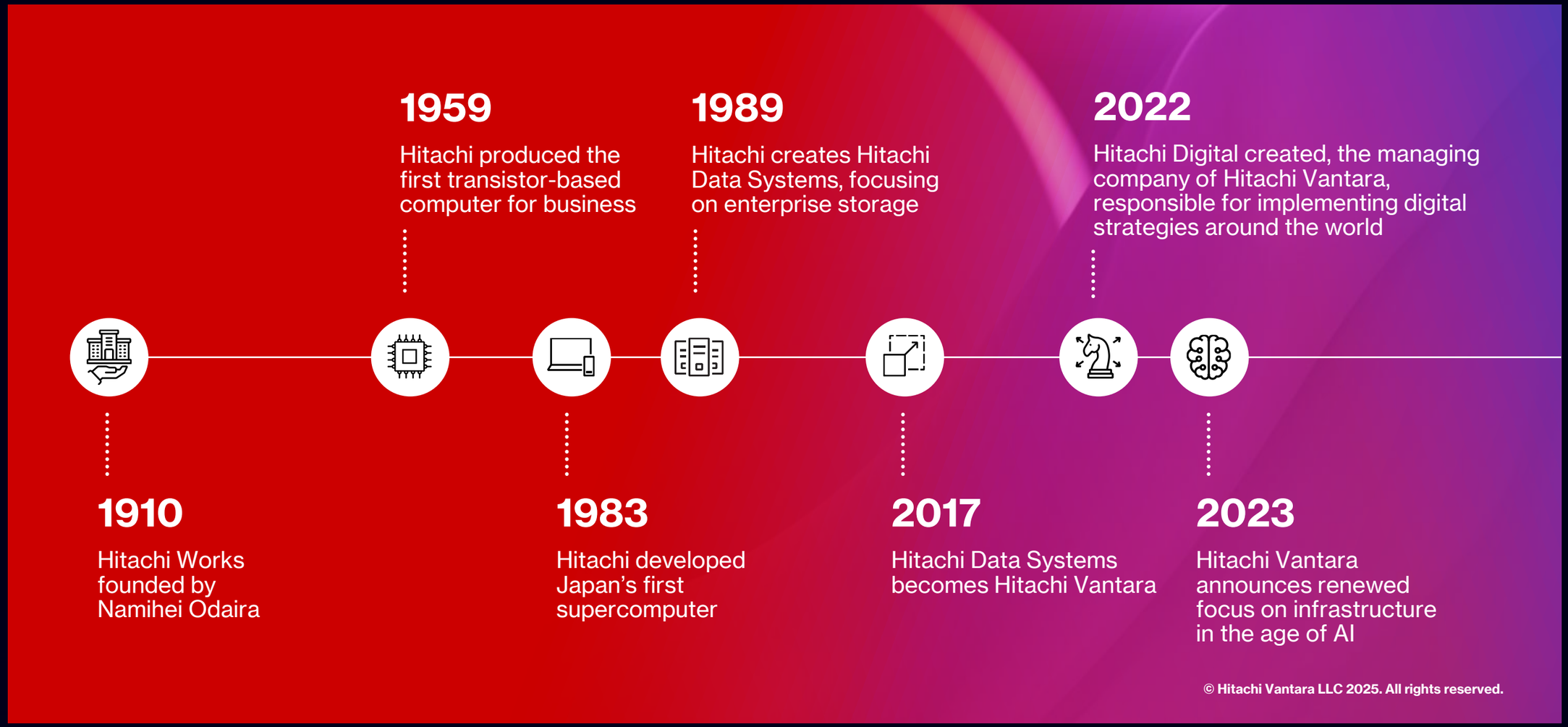


Software Innovation
GlobalLogic + Hitachi Vantara

Grid Intelligence
Hitachi Energy + Hitachi Vantara

Smart Urban Mobility
Hitachi Rail + Hitachi Vantara

Hitachi Vantara Timeline



Our Customers *Trusted by industry leaders worldwide*

Our Portfolio

Digital Transformation Experience

ITOps

Unmatched Efficiency, Reliability, and Security Aligned to Customers Business, Data and Services

AI/GenAI

Hitachi iQ: Integrated AI Solution Portfolio
Embedded Intelligence Across Hybrid Cloud
Developer Community of GenAI Companions

Consumption Services

Solutions Through Ecosystem of Integrated ISVs Guaranteed IT Ops SLAs

Intelligent Data Management

Data Orchestration

API-first Open Data and Control Planes
Automaton and Storage-as-code

Data Protection, Governance

Data Compliance, Data Privacy,
Data Lifecycle Management
Security and Unbreakable Guarantees

AIOps

Automation and Efficiencies at Scale
Sustainability Observability

Data Infrastructure Foundation

Hybrid Cloud Storage Platform

One Data Plane, One Control Plane Appliance, SWDS, and Cloud Sustainability by Design

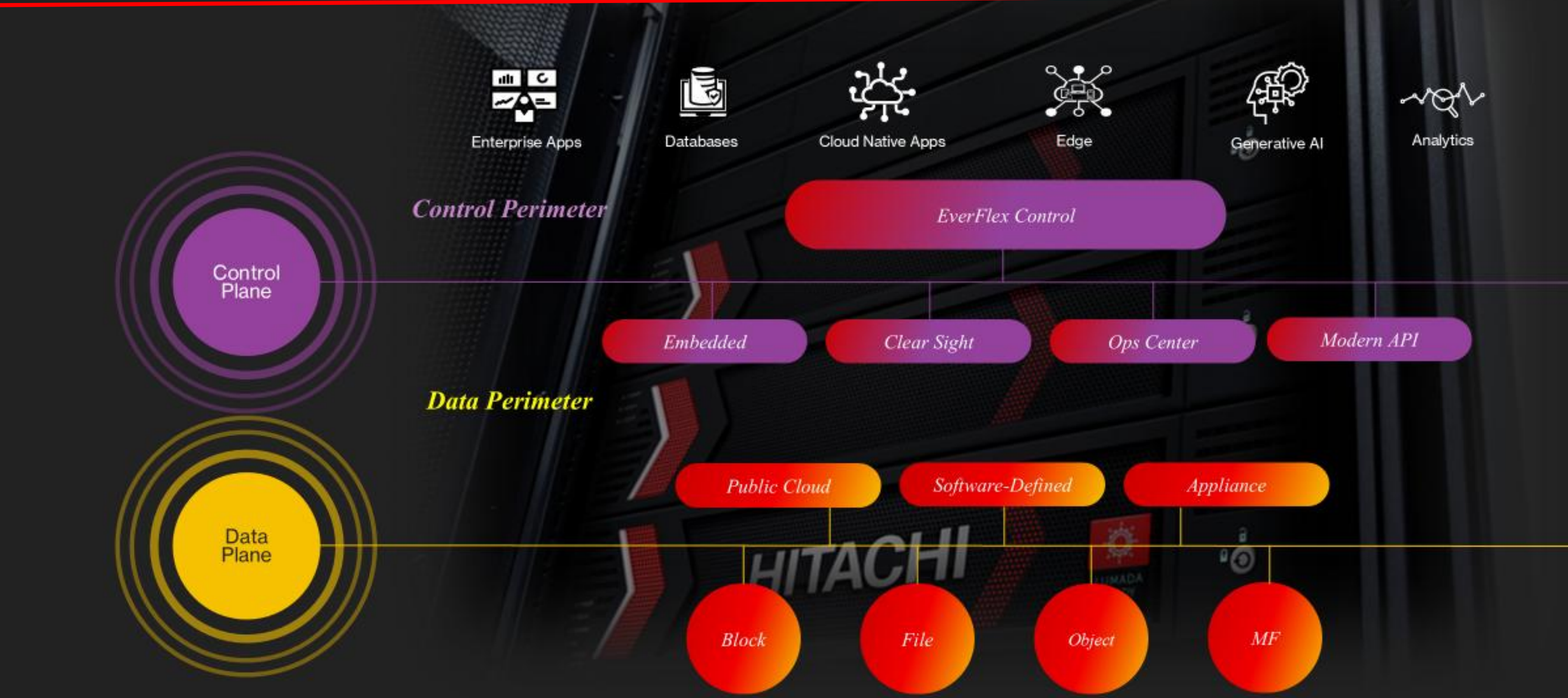
Integrated Solutions

Storage, Compute, Networking Architectures and Applications with ISV Ecosystem

IaaS – EverFlex

Consumption and Deployment Choice
Ensuring Scalable Flexibility Across Hybrid Cloud *Managed, On-Demand, Custom*

Virtual Storage Platform One Ecosystem



Hitachi CyberSecurity: Offering Comprehensive Cybersecurity Solutions

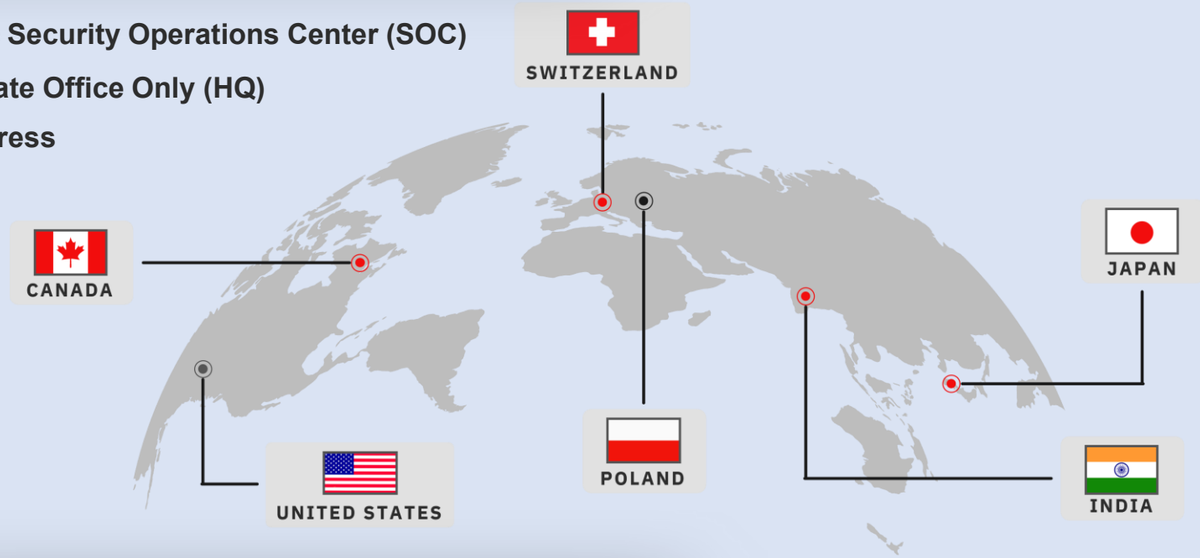
Who We Are

With over 25 years of experience, Hitachi Cyber has established itself as a trusted partner, delivering tailored cybersecurity solutions to organizations of all sizes and across various industries.

- **Global Leader in Cybersecurity**
- **Promoting Secure Growth**
- **Innovative Approach to Security**
- **24/7 Operations**

Our Footprint

- On-Site Security Operations Center (SOC)
- Corporate Office Only (HQ)
- In Progress



Our Top Tier Certifications & Expertise

Our Services

24/7 Managed Security Services

Vigilant threat detection, investigation, and response round the clock, every day of the year.

Professional Services

Guidance, accompaniment, and training on cybersecurity, privacy, and GRC.

Cyber Threat Intelligence

Actionable intelligence powered by AI and human expertise to safeguard digital assets.

CYBER PROWL

WHAT TO LOOK OUT FOR IN 2025

What to look out for in 2025

An increasingly sophisticated threat landscape that demands vigilance and adaptation. These are the most pressing cybersecurity challenges confronting organizations globally.

Identity Theft & Cloud Vulnerabilities

Sophisticated credential theft targeting cloud infrastructures has increased 70% since 2022, with attackers leveraging identity-based attack vectors to bypass traditional security controls.

Nation-State & Geopolitical Threats

State-sponsored cyber operations have expanded beyond traditional espionage to include critical infrastructure targeting, with 35% of critical sectors reporting attempted breaches linked to foreign actors.

Advanced Ransomware & Data Weaponization

Threat actors now combine encryption with exfiltration in 83% of ransomware attacks, creating dual extortion scenarios that leverage sensitive data as weapons against organizations.

Deepfakes & Misinformation

AI-generated content has enabled highly convincing social engineering attacks, with executive impersonation attempts increasing 247% in the past year.

Supply Chain Vulnerabilities

Cross-border dependencies create cascading risk, with 62% of breaches now originating through third-party access points and international vendor relationships.

Emerging Technology Challenges

The proliferation of AI and quantum computing introduces novel threat vectors that outpace traditional security paradigms and regulatory frameworks.

Ethical and Security Challenges of Emerging Technologies – The Quantum ERA

The Quantum-AI Convergence Threat

The combination of quantum computing capabilities with AI acceleration presents an unprecedented risk to classical encryption systems. As quantum processors become more accessible through cloud services, we face a new era of cryptographic vulnerability.

Current estimates suggest that 78% of today's encryption standards will be compromised when quantum computers reach sufficient qubits – a milestone potentially achievable within 5-7 years.

GPU-accelerated AI systems are already being used to identify patterns in encrypted traffic without decryption, creating a preview of quantum-enabled threats to come.

1 Key Vulnerability Factors

- Post-quantum cryptography adoption lags behind quantum development
- AI systems can identify cryptographic weaknesses at unprecedented scale
- GPU clusters enable brute-force approaches previously considered impractical
- Hybrid attack vectors combining multiple technologies bypass layered defenses

Organizations must balance the competitive advantages of adopting emerging technologies with the ethical implications and security risks they introduce. This requires a fundamental rethinking of security architecture to incorporate quantum-resistant algorithms and AI-aware defense strategies.

Ethical and Security Challenges of Emerging AI Technologies

Critical AI Security Vulnerabilities

As AI systems become more integrated into critical infrastructure, they present novel attack surfaces that traditional security approaches fail to address adequately.

1 Model Poisoning & Backdoors

Adversaries can compromise AI systems during training phases, introducing subtle manipulations that trigger malicious behaviors under specific conditions.

2 Prompt Injection Attacks

Crafted inputs can manipulate AI systems to bypass security guardrails, potentially extracting sensitive data or executing unauthorized actions.

3 AI-Enhanced Social Engineering

Machine learning enables unprecedented personalization of attacks, making detection of fraudulent communications increasingly difficult.

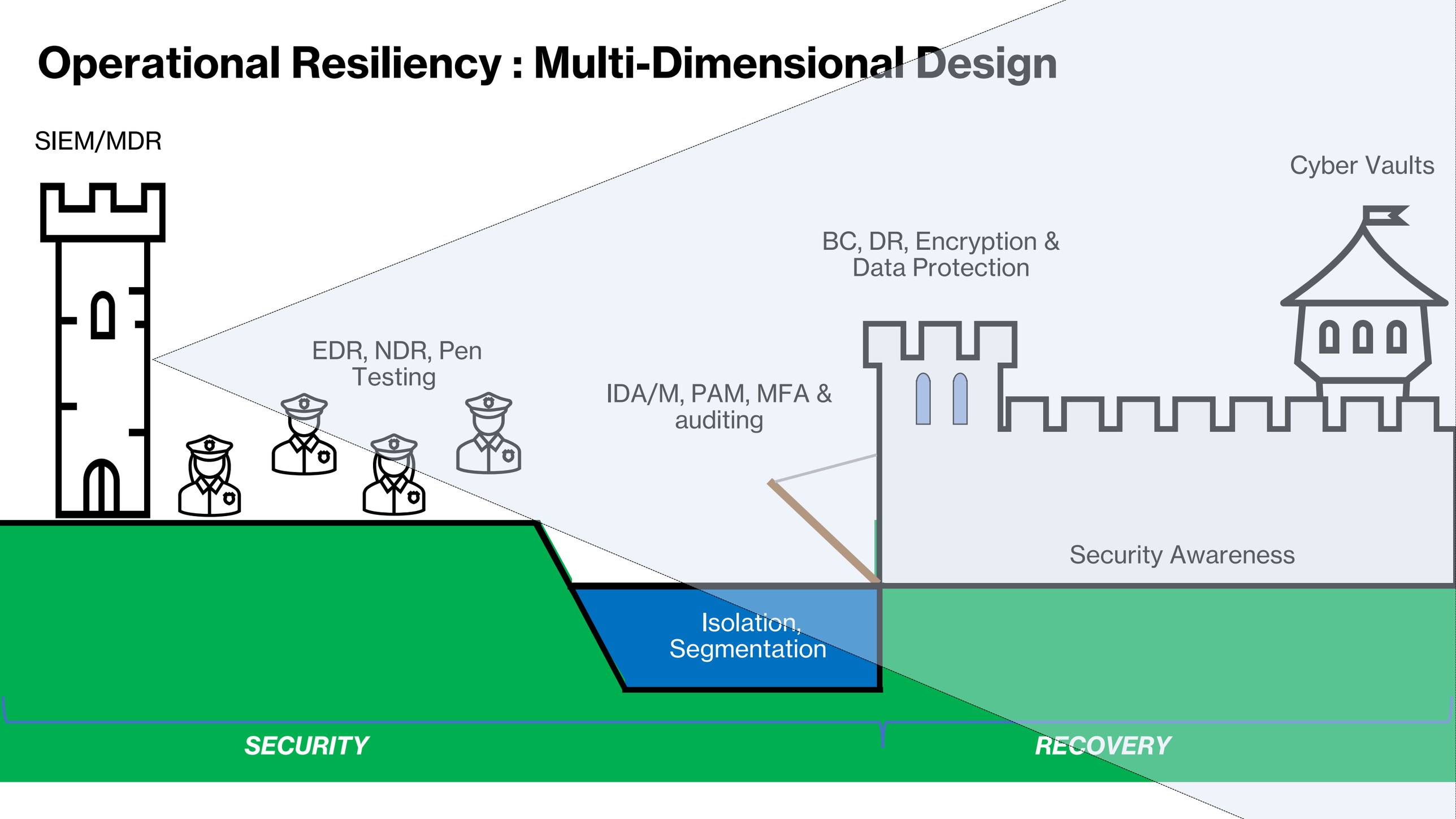
Ethical Dimensions

The deployment of AI in security contexts raises profound ethical questions that organizations must address proactively:

- Surveillance capabilities that threaten privacy and civil liberties
- Algorithmic bias that may disproportionately impact vulnerable populations
- Accountability gaps when automated systems make security decisions
- Dual-use concerns as defensive AI tools can be repurposed for attacks

Organizations must establish robust AI governance frameworks incorporating ethical review processes, transparent documentation, and continuous monitoring.

Operational Resiliency : Multi-Dimensional Design



The Cyber Attack Sequence

Anatomy of an Attack Sequence: How does it Happen

Reconnaissance

Attackers gather information about targets through OSINT, social engineering, and network scanning. In 2025, AI-assisted reconnaissance has increased target identification efficiency by 78%.

Weaponization

Malware is tailored to exploit specific vulnerabilities. Modular malware kits allow attackers to customize payloads based on reconnaissance data with 63% greater effectiveness.

Delivery

Malware is transmitted via phishing, compromised websites, or supply chain attacks. Spear-phishing remains the primary delivery method with a 42% success rate among targeted users.

Exploitation

The malware executes, exploiting vulnerabilities to gain access. Zero-day exploits increased by 31% in 2025, with an average time-to-patch of 43 days.

Installation

Malware establishes persistence on the target system. Fileless malware techniques evade 62% of traditional security controls and are used in 47% of attacks.

Command & Control

Attackers establish remote control channels. Encrypted C2 traffic using legitimate services like DNS and HTTPS makes detection difficult, with dwell times averaging 24 days.

Actions on Objectives

Attackers execute their goals (data theft, ransomware, etc.). The average time from initial breach to ransomware deployment is now just 3.5 days, down from 7 days in 2023.

Cyber Resiliency vs Cyber Security

Hitachi Vantara

The important difference between them and why you need for both

Cyber Security

Keep the bad guys out

Cybersecurity focuses on creating defenses to prevent cyberattacks from happening in the first place. This involves things like firewalls, anti-virus software, data encryption, and employee training on spotting phishing attempts. It's like building a strong wall around your castle to keep invaders out

- Focuses on prevention of cyberattacks.
- Implements tools and measures to block unauthorized access, like firewalls, antivirus software, and encryption.
- Ensures systems are patched and up-to-date to minimize vulnerabilities.
- Educates users on safe practices to avoid phishing attempts and social engineering.

Cyber Resilience

Be prepared to adapt and recover

Cyber Resilience is all about your organization's ability to bounce back after a cyberattack does occur. This includes having a disaster recovery plan in place, regularly backing up data, and having the ability to identify and contain an attack quickly. It's like having a well-drilled army and a stocked armory inside your castle in case the walls get breached

- Deals with an organization's ability to bounce back from a cyberattack.
- Involves planning for incident response, data recovery, and minimizing downtime.
- Considers broader threats beyond hacking, including natural disasters and power outages.
- Emphasizes business continuity to ensure core functions remain operational.

Why you need both:

Think of cybersecurity as your organization's first line of defense, and cyber resilience as your backup plan. No security system can be treated as a Nintendo box and is foolproof, so having a strong cyber resilience strategy ensures you can handle unexpected situations and get back on operational resiliency mode quickly.

Cyber Recovery vs Cyber Resiliency

The important difference between them and why the need for both

Cyber Resiliency

Be prepared to adapt and recover

Cyber Resilience is all about your organization's ability to bounce back after a cyberattack does occur. This includes having a disaster recovery plan in place, regularly backing up data, and having the ability to identify and contain an attack quickly. It's like having a well-drilled army and a stocked armory inside your castle in case the walls get breached

- Deals with an organization's ability to bounce back from a cyberattack.
- Involves planning for incident response, data recovery, and minimizing downtime.
- Considers broader threats beyond hacking, including natural disasters and power outages.
- Emphasizes business continuity to ensure core functions remain operational.

Cyber Recovery

Be prepared to recover system state

Cyber recovery is a specialized aspect of cybersecurity that focuses on the processes and technologies needed to restore an organization's critical data and systems after a cyberattack. It goes beyond traditional data backup and disaster recovery methods

- Specifically targeting recovery from attacks like ransomware, which can corrupt or encrypt data.
- Creating secure, isolated "vaults" where backup data is stored in a way that cannot be altered or deleted by attackers.
- Ensuring that critical systems and data can be quickly restored to a known good state, minimizing downtime.
- Scanning backups for malware and verifying that recovered data is clean and uncompromised.

Why you need both:

Cyber resilience and cyber recovery are two sides of the same coin when it comes to cybersecurity. They both play a vital role in protecting your organization from cyberattacks, but they focus on different aspects. In short, cyber resilience helps you prevent attacks and minimize damage, while cyber recovery helps you get back on your feet after an attack. Both are essential for a comprehensive cybersecurity strategy.

Cyber Security – NIST 2.0 Framework

Key Functions

Governance Risk & Compliance

Governance & Policy

- Exec Security Committees
- Policies
- Key Controls
- SOP/ Governance

Risk Management

- Risk Framework
- Risk Assessment
- Asset Classification
- Asset Handling
- Risk Management Strategy
- 3rd Party Security Reviews

Compliance & Regulatory

- Audit/ Site Reviews
- SOC1, SOC2, SOX
- Legal/ Regulatory
- Security Awareness Training

Business Continuity & DR

Customer Assurance

- Annual Penetration Testing
- Sales Enablement
- Customer Escalations
- Security Collaterals
- White Papers
- Contract Negotiations

Identity & Access Management

IAM

- Business Requirements
- User Access Mgmt.
- Privileged Access Mgmt. (PAM)
- System/App Access Control
- Single Sign On (SSO)
- Multifactor Auth. (MFA)
- Enterprise Mobility Mgmt (EMM)/MDM Security
- Identity Governance
  - User Roles/Responsibilities
  - Authorization/Minimum Necessary Privilege

Venerability Mgmt.

- Vulnerability Mgmt.
- Asset Discovery & Compliance
- Patch Mgmt. Compliance
- Ensure SOC Functionality
- Automation

Data Security

Data At-Rest & In-Transit

- Cryptographic Controls
- Encryption at Rest
- Cryptographic Standards
- Certificate Authority/ PKI/HSM
- HSM Support and Management
- Key Custodian

Privacy

Privacy Ops

- Evidence Collection And Support of Certifications
- Business Impact Assessment of New Guidance From Legal Privacy Team
- Ensuring Appropriate Privacy Safeguards Are Implemented
- Maintain Privacy Certifications (Technical Certs)
- Enforcing Data Life-cycle Management
- Data Governance
- Data Loss Prevention Policies & Governance
- Privacy & Framework
  - Implement
  - Manage & Enhance
  - Validate
  - Compliance

Infrastructure Security

Proactive Monitoring

- Infrastructure Security
- Secure Hardening Requirements
- Security Standards
- Security Tool Implementation, Care & Feeding
- SIEM & SOAR Provider
- Security Architecture And Design
- Host Security

Operations

- Data Loss Prevention (DLP) enforcement
- Cloud Security
- Operational Software Control
- Vulnerability Mgmt.
- Asset Discovery & Compliance
- Patch Mgmt. Compliance
- Ensure SOC functionality
- Automation

Security Assurance

- Testing Security Open Readiness
- Red Team

Cyber Defense

Security Operations

- Downstream Logging/ Monitor/Reporting & SOAR Functionality
- Legal eDiscovery
- Threat Hunting
- Security Operational Readiness
- Onboarding/ Offboarding
- Event Monitoring
- Tier 1 Alert Triage

Incident Management

- Incident Response Plan
- IR playbooks
- Investigations
- Forensic Analysis
- Containment
- Recovery
- Remediation
- Metrics and Reporting
- IR Tabletop & Live Tests
- BCP/DR Alignment

Application Security

AppSec

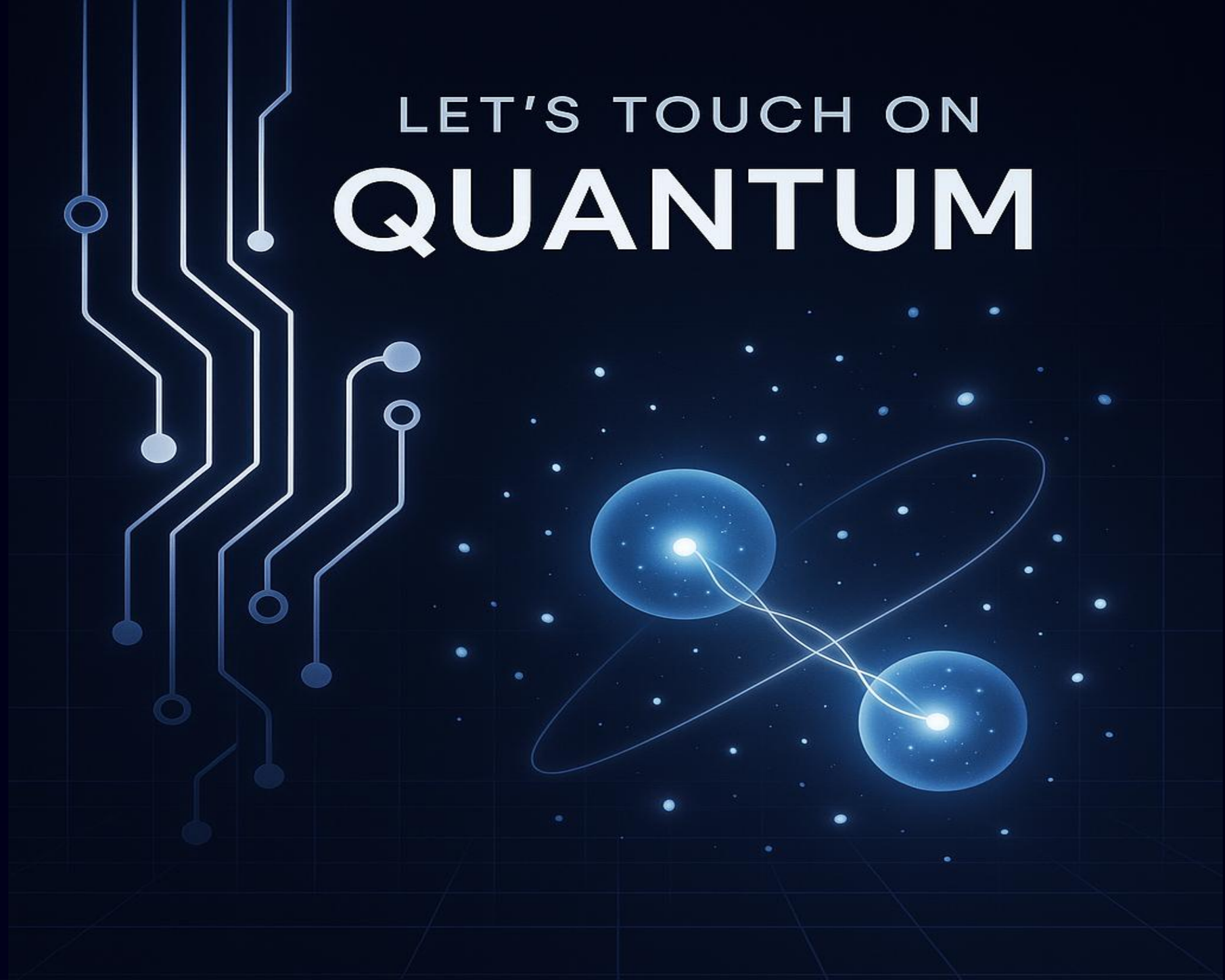
- Security Reviews
- Engg Architecture And Design
- Secure Development Requirements
- SSDLC Program And Support Processes (OSAMM / AppSec)
- Security Bug Tracking And Closing
- Standards And Guidance
- Engg Training And Education Program
- R& D Penetration Testing Program

DevSecOps

- Software Composition Analysis
- Statistic Application Security testing
- Dynamic Application Security Testing
- Additional Tooling (Fuzzing Etc.)
- Secrets Mgmt.
- Container Security
- Code Signing

LET'S TOUCH ON

QUANTUM



The Threat - Quantum Computing: A New Paradigm for Computation

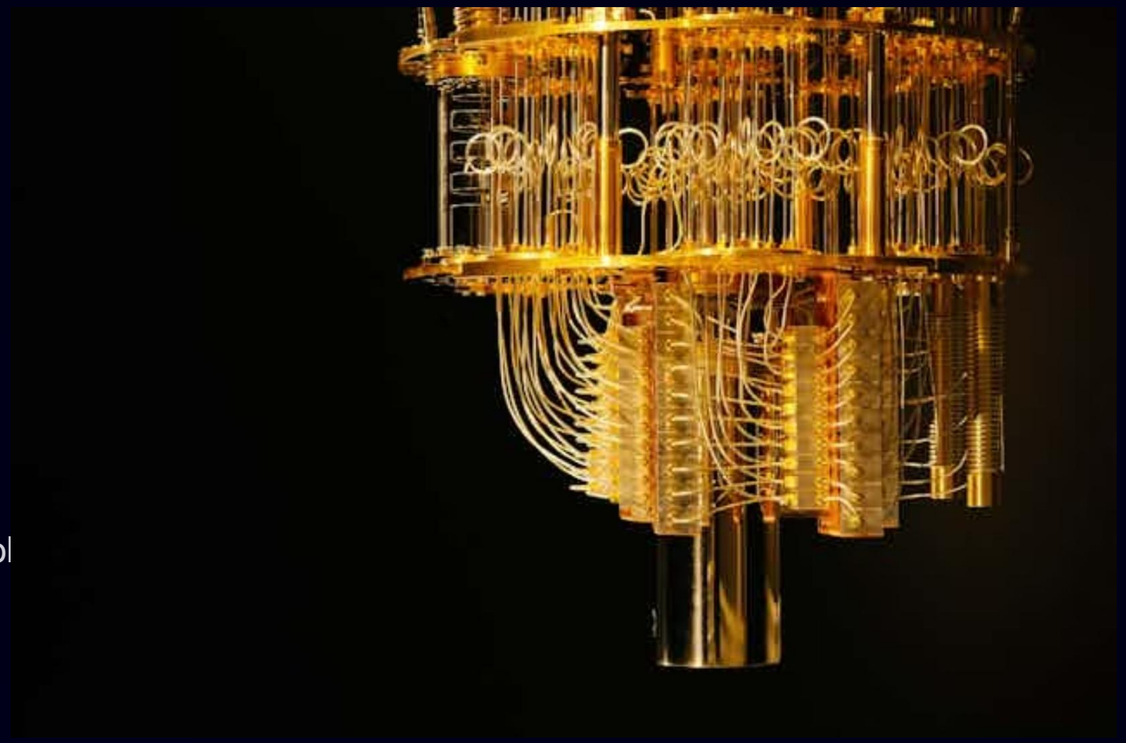
Cryptography is a foundational pillar of cybersecurity

What is Quantum Computing?

- Computation with qubits instead of binary bits
- Builds coherent superposition of states
- Behaves like a massively parallel computer

Why It Matters for Security

Quantum computers can break current public key cryptograph
primitives that secure our digital infrastructure



Quantum Computing is rewriting the rules of cryptography

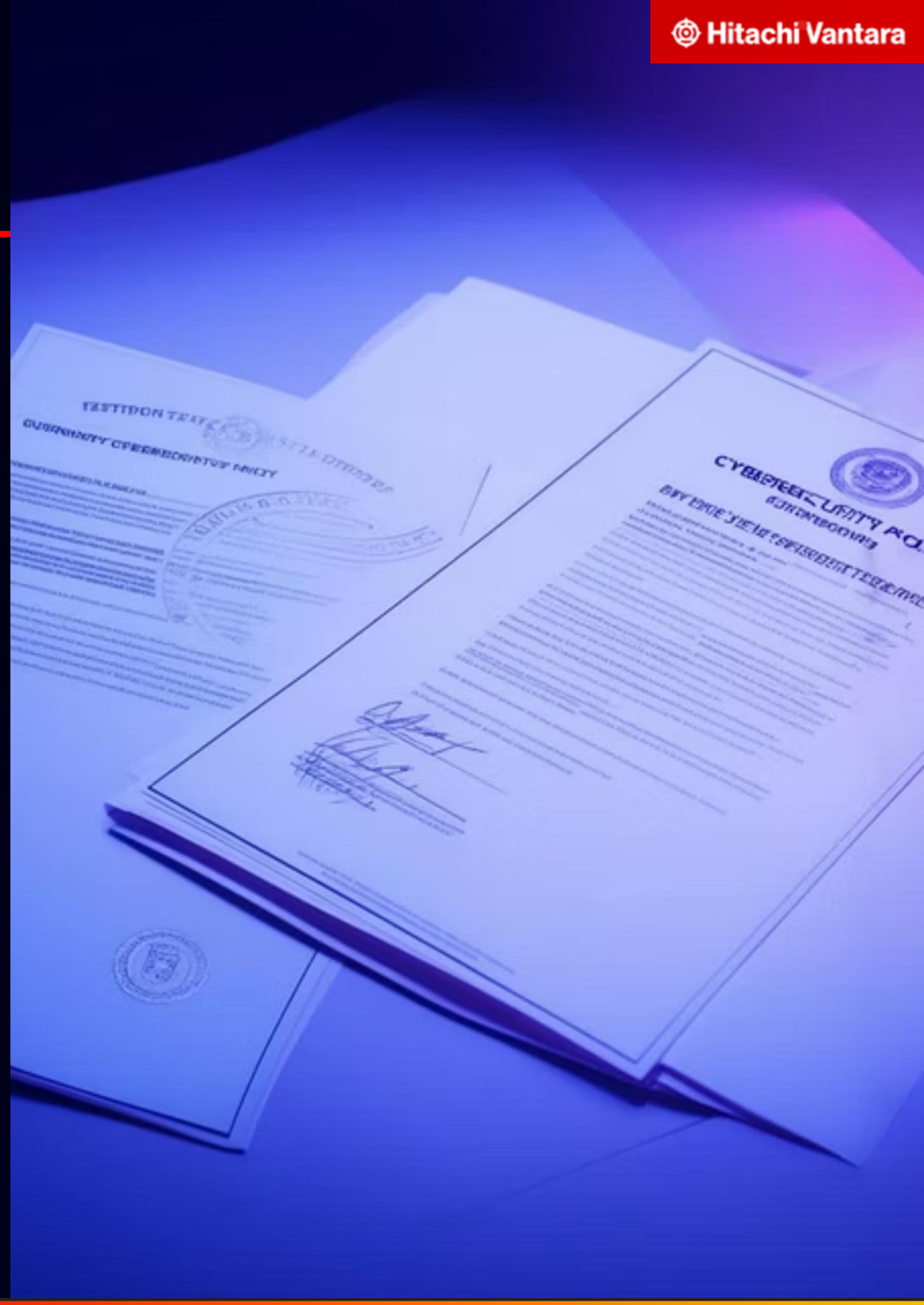
Quantum-Safe Risk is Officially Recognised

United States National Security Memorandum

"To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

European Union Strategy

"This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution."

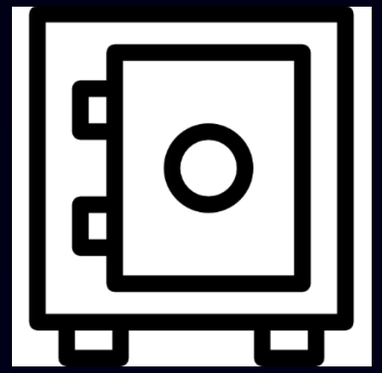


Major governments worldwide have recognised the quantum threat and are mandating transitions to quantum-resistant cryptography

Cryptographic Toolbox: Simplified Overview

Symmetric Cryptography

(Secret Key)



- Same key used for encryption and decryption
- Examples: AES, 3DES
- Relatively resistant to quantum attacks

Asymmetric Cryptography

(Public Key)

- Different keys used for encryption and decryption
- Examples: RSA, ECC, Diffie-Hellman
- Vulnerable to quantum attacks

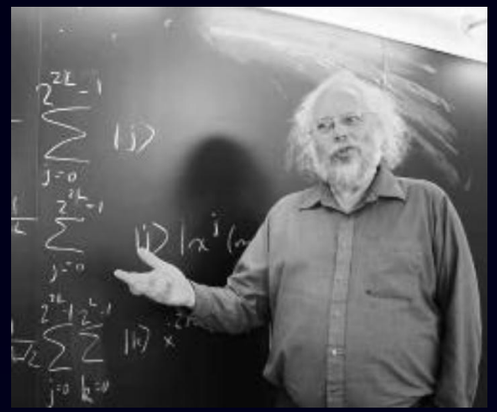
Quantum Computing and Cryptography

1

Shor's Algorithm

Developed by Peter Shor in 1994

- Quantum algorithm for integer factorization
- Can break public key cryptography like RSA, Elliptic Curve & Diffie Hellman
- Complexity: O((log N)³) vs. classical O(e^1.9 (log N)^1/3 (log log N)^2/3)



2

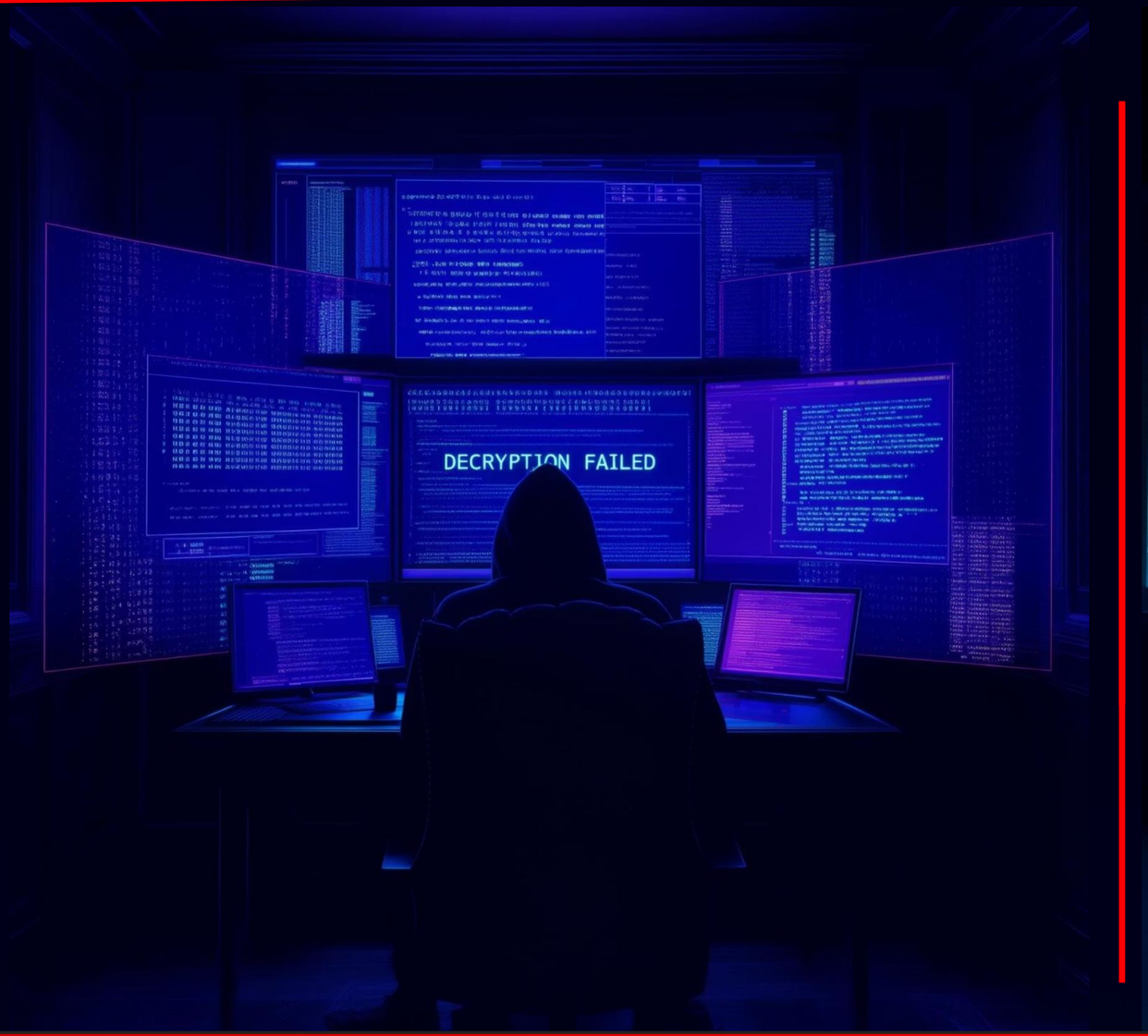
Grover's Algorithm

Developed by Lov Grover in 1996

- Quantum algorithm to perform search in an unsorted database
- Reduces security of symmetric encryption
- Complexity: O(n^½) vs. classical O(n)

Cryptography Before and After Quantum Computing

The Hacker's Point of View Today



After the Quantum Computer

Quantum-Safe Encryption Solution for Critical Networks

The next level of security for critical infrastructure

Hitachi quantum-safe solutions provide:

Enhanced Security

Protection against both current and quantum-based threats

Operational Reliability

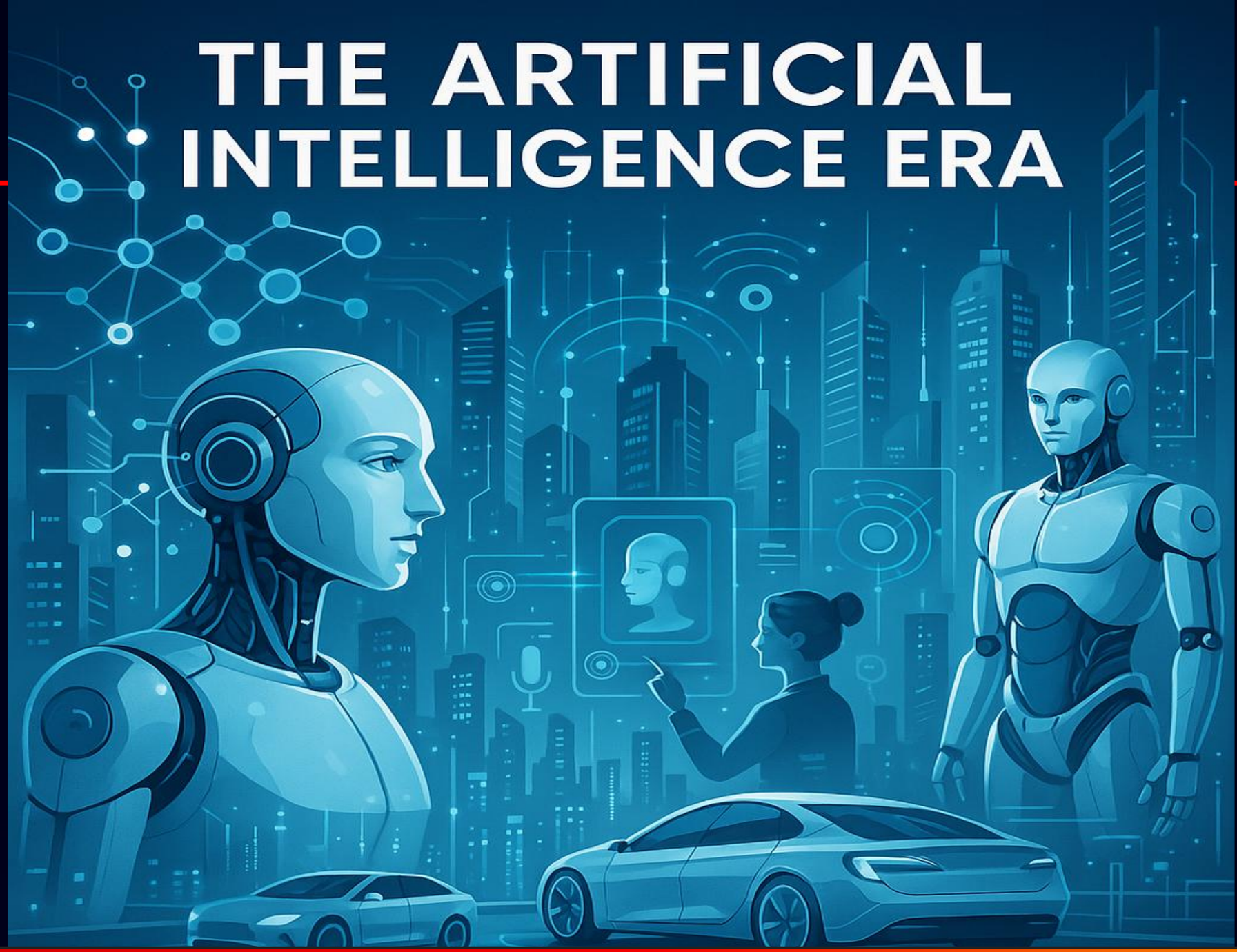
Maintaining critical system performance while implementing advanced security

Future-Proofed Investment

Long-term protection that evolves with emerging standards

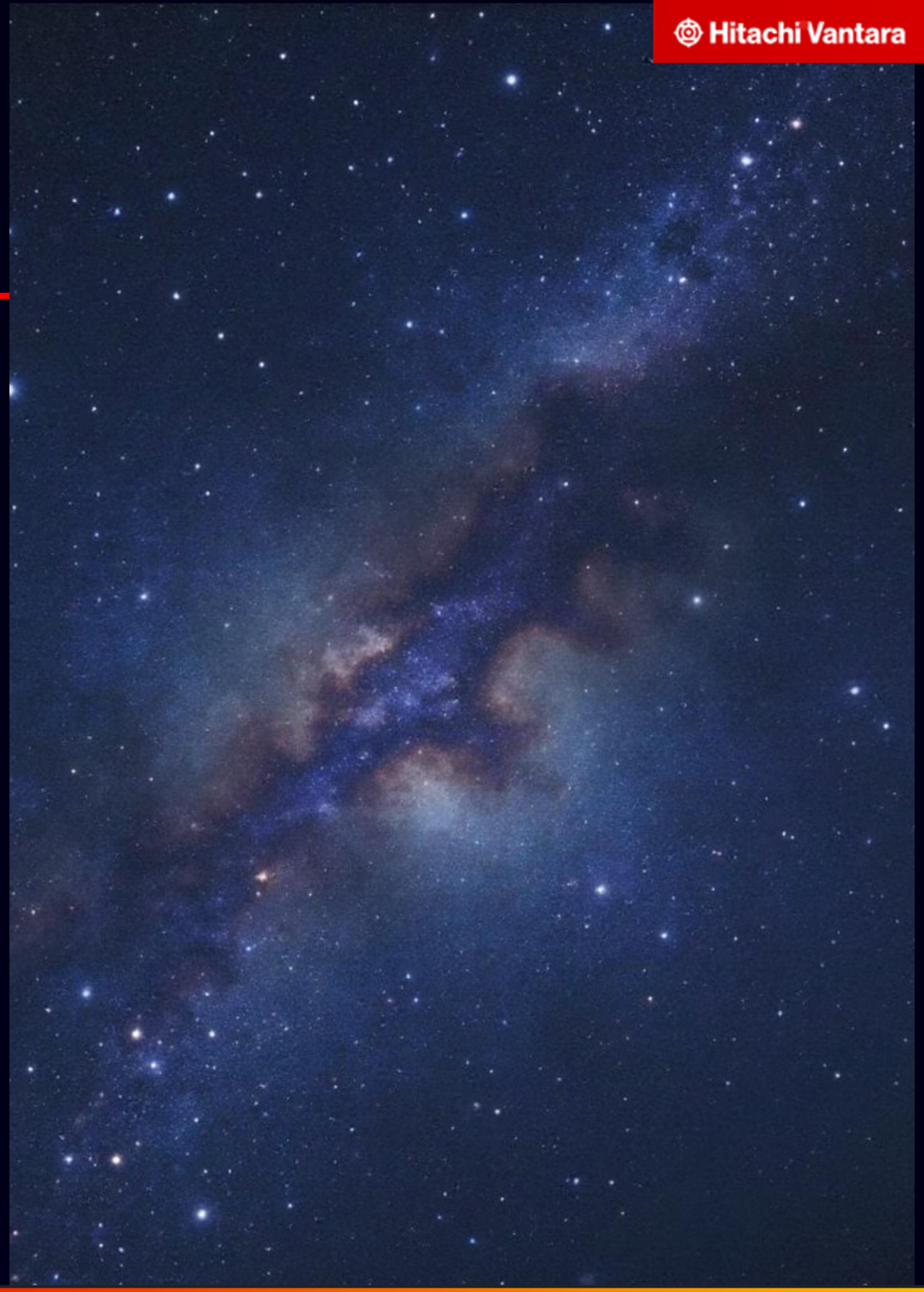
Quantum Computing in the Rear View – Don’t loose sight

Quantum Computing in the Mirror – Don’t loose sight



Decipher the Concept behind Artificial Intelligence

Unraveling the forces driving AI's explosive growth and understanding its diverse forms in today's business landscape. This presentation explores why AI has suddenly become ubiquitous and the various types of AI technologies transforming our world.



The AI Revolution: An Overview

Unprecedented Growth

AI adoption has accelerated at a staggering pace across industries, transforming how businesses operate and compete

Technological Convergence

Multiple technological advances have converged to create the perfect conditions for AI's rapid expansion

Widespread Impact

From healthcare to finance, retail to manufacturing, AI is fundamentally reshaping business processes and customer experiences

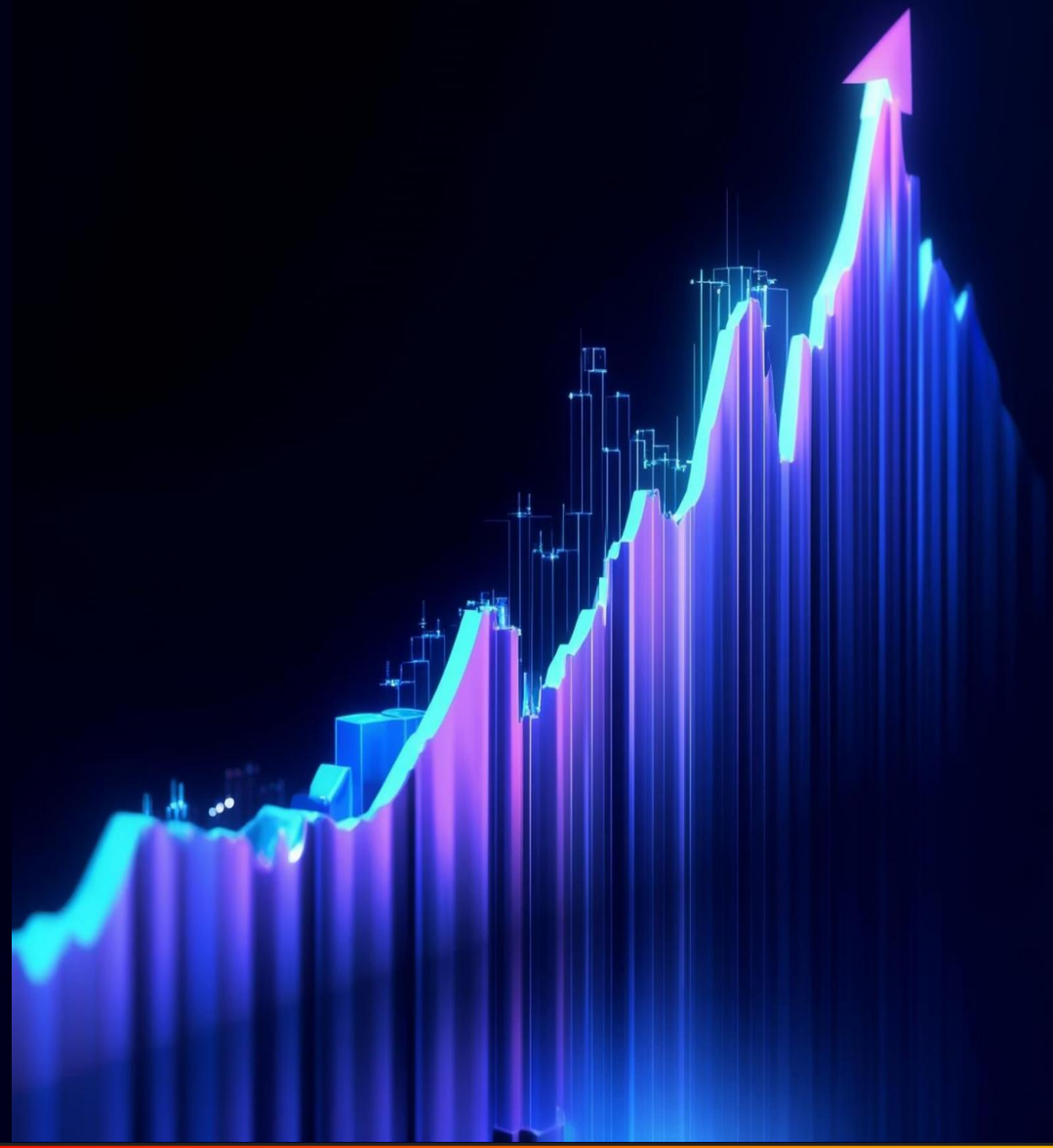
Exponential Growth in Data

Why it matters: AI models, especially machine learning and deep learning, require massive amounts of data to train effectively.

Key Examples:

- Social media platforms generate terabytes of user data daily
- IoT devices collect real-time data from billions of sensors
- Businesses leverage customer data for personalization and analytics

Impact: The availability of big data has enabled AI systems to learn complex patterns and make increasingly accurate predictions.



Advancements in Computing Power

Why it matters: Training AI models, especially deep neural networks, requires immense computational resources.

GPUs

Graphics Processing Units originally designed for gaming are now widely used for parallel processing in AI, offering significant speedups for matrix operations.

TPUs

Google's custom Tensor Processing Units are specifically optimized for AI workloads, providing 15-30x higher performance and 30-80x higher performance-per-watt than CPUs and GPUs.

Cloud Computing

Platforms like AWS, Google Cloud, and Azure provide scalable computing power for AI development, democratizing access to high-performance resources.

Impact: Faster training times and the ability to handle exponentially more complex models, enabling breakthroughs in AI capabilities.

Breakthroughs in Machine Learning Algorithms

Why it matters: Innovations in algorithms have made AI more efficient, accurate, and versatile across applications.

Transformers

Revolutionized natural language processing through attention mechanisms, enabling models like GPT and BERT to understand context and generate human-like text with unprecedented fluency.

Generative Adversarial Networks

GANs use competing neural networks to create realistic synthetic images, videos, and audio that can pass for human-created content, revolutionizing creative industries.

Reinforcement Learning

Powers systems like AlphaGo and autonomous vehicles by enabling AI to learn optimal behavior through trial-and-error and reward maximization in complex environments.

Open-Source Movement and Collaboration

Why it matters: Open-source tools and frameworks have democratized AI development, allowing global participation in advancing the field.

Key Examples:

1 Frameworks

TensorFlow, PyTorch, and Keras provide accessible libraries that simplify complex AI implementation

2 Pre-trained Models

Hugging Face's Transformers and OpenAI's GPT offer ready-to-use models that eliminate the need for resource-intensive training

3 Communities

GitHub, Kaggle, and conferences like NeurIPS and ICML foster knowledge sharing and collaborative innovation

Impact: Lowered barriers to entry have enabled startups, researchers, and hobbyists to contribute to AI advancements, accelerating innovation globally.

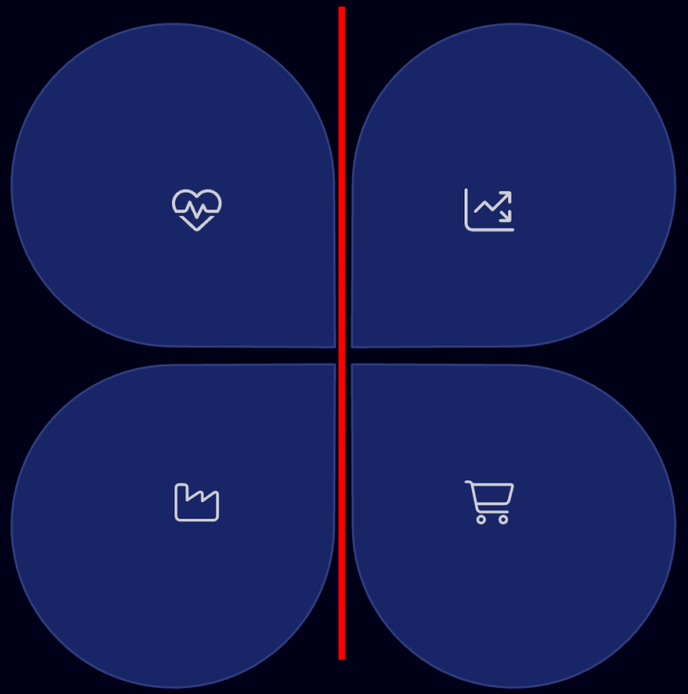
Real-World Applications and Success Stories

Healthcare

AI-powered cancer detection systems achieve 99% accuracy in identifying malignancies in medical images, while drug discovery algorithms have reduced development timelines from years to months.

Manufacturing

Predictive maintenance AI has reduced equipment downtime by 45% and maintenance costs by 25% in smart factories, while quality control AI has improved defect detection by 90%.



Finance

AI fraud detection systems have reduced financial crimes by 35% at major banks, while algorithmic trading now accounts for over 70% of all U.S. equity trades.

Retail

Personalized recommendation engines drive 35% of Amazon's revenue, while inventory management AI has reduced stockouts by 30% and warehousing costs by 25% for major retailers.

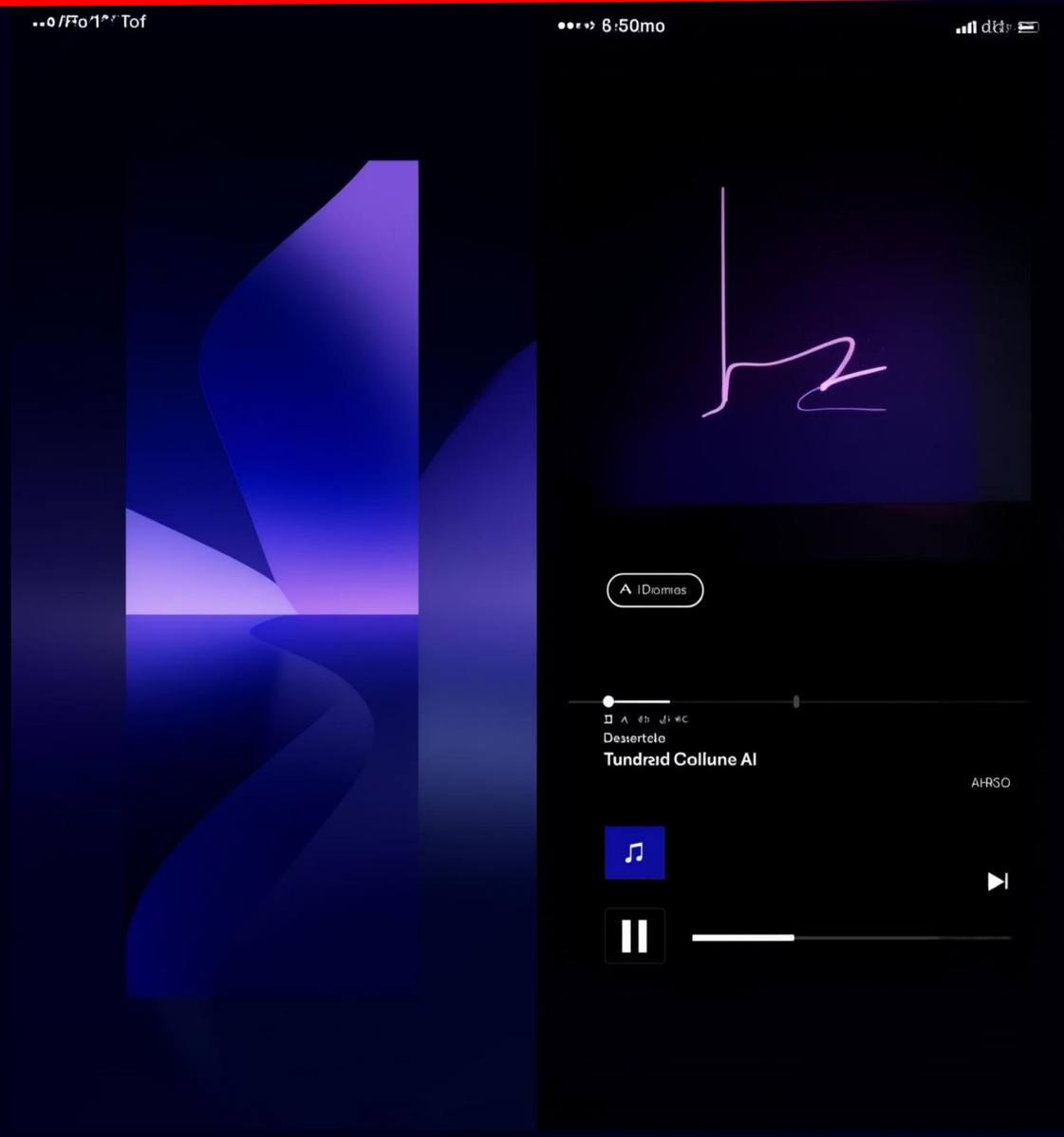
Impact: These tangible benefits are driving widespread business adoption and continuous investment in AI technologies.

Generative AI and ChatGPT

Why it matters: Generative AI has captured public attention and showcased AI's creative potential, making artificial intelligence accessible and relevant to everyday users.

Key Advancements:

- **ChatGPT**: OpenAI's conversational model gained 100 million users in just 2 months, setting records as the fastest-growing consumer application in history
- **DALL·E and Stable Diffusion**: Image generation models that create stunning visuals from text prompts, revolutionizing creative workflows
- **Media Generation**: AI tools creating music, videos, and animations that rival professional
- human-created content



Competition Among Tech Giants

1

Google

Leading with DeepMind's groundbreaking research (AlphaGo, AlphaFold) and developing Bard to compete in the conversational AI space. Investing $30B+ annually in AI R&D.

2

Microsoft

Formed a $10B partnership with OpenAI, integrating ChatGPT into Bing and Microsoft 365 products. Building an AI-first ecosystem across consumer and enterprise products.

3

Meta

Investing heavily in AI for content moderation, recommendation systems, and the metaverse. Released LLaMA model to compete in the foundation model space.

4

Amazon

Leveraging AI throughout e-commerce, cloud services, and logistics. AWS offers comprehensive AI/ML services and recently launched Amazon Bedrock for generative AI.

Impact: This intense competition is driving rapid innovation cycles and massive investment, accelerating AI advancement across all sectors.

Policy and Ethical Considerations

Regulatory Landscape

- EU's **AI Act**: First comprehensive regulatory framework for AI with risk-based approach
- U.S. **AI Bill of Rights**: Non-binding guidelines emphasizing safe and transparent AI systems
- China's **AI governance**: Focused on algorithmic transparency and data security

Ethical Focus Areas

- **Bias mitigation**: Preventing discrimination in AI outputs and decisions
- **Transparency**: Making AI systems explainable and accountable
- **Privacy**: Protecting personal data while enabling AI advancement

Cultural Shift and Awareness

Media Influence

Films like *Ex Machina*, *Her*, and *The Social Dilemma* have shaped public perception of AI's potential and risks

News Coverage

AI has moved from technology sections to front-page headlines, with mainstream media regularly covering AI developments

Public Discourse

Widespread debates about AI's impact on jobs, creativity, privacy, and society have entered everyday conversation

Education Transformation

Schools and universities are rapidly adapting curricula to include AI literacy and skills development

Impact: This cultural mainstreaming of AI has increased both curiosity and acceptance of AI technologies, creating a more receptive market for AI products and services while also raising the bar for responsible development.

Pandemic Acceleration

Why it matters: The COVID-19 pandemic served as a powerful catalyst for digital transformation, dramatically accelerating AI adoption across sectors.

1

Remote Work Revolution

AI-powered collaboration tools, virtual assistants, and workflow automation became essential as organizations transitioned to distributed work models

2

Healthcare Innovation

AI accelerated vaccine development, enabled remote diagnostics, and powered pandemic tracking and prediction models

3

E-commerce Surge

The explosion in online shopping created unprecedented demand for AI-driven logistics, recommendation engines, and customer service solutions

Impact: The pandemic compressed years of digital transformation into months, permanently altering business models and demonstrating AI's critical role in business resilience and adaptation.

AI Democratization

Why it matters: AI tools and platforms have become accessible to non-experts, expanding the pool of AI creators and users beyond technical specialists.

Key Enablers:

1. No-Code AI Platforms

   Tools like Google AutoML and DataRobot allow users to build machine learning models through visual interfaces without writing code

2. API-First AI Services

   OpenAI, Google Cloud, and AWS offer powerful AI capabilities as simple API calls that can be integrated into applications with minimal technical knowledge

3. Affordable Compute

   Cloud platforms have dramatically reduced the cost of accessing AI-grade computing resources, eliminating hardware barriers

Impact: Small businesses, educators, creative professionals, and entrepreneurs can now leverage sophisticated AI capabilities without specialized expertise, driving innovation across industries and use cases.

Types of AI: By Capability

1

Narrow AI (ANI)

Task-specific intelligence designed for singular purposes. Examples include virtual assistants like Siri, recommendation engines like Netflix, and specialized tools like weather prediction models.

Status: Widely deployed and constantly improving

2

General AI (AGI)

Human-like intelligence capable of understanding, learning, and applying knowledge across domains. Would possess reasoning, problem-solving, and adaptability comparable to humans.

Status: Theoretical and under active research

3

Superintelligent AI (ASI)

Intelligence that surpasses human capabilities across all domains. Would potentially solve problems beyond human comprehension and innovate in unprecedented ways.

Status: Theoretical with no immediate path to creation

Most current business applications use various forms of Narrow AI, while research continues toward more general capabilities.

Types of AI: By Technology

Machine Learning

Systems that learn patterns from data to make predictions and decisions. Powers applications from fraud detection to customer segmentation.

Natural Language Processing

AI that understands, interprets, and generates human language. Enables chatbots, translation services, sentiment analysis, and content generation.

Computer Vision

AI that processes and analyzes visual information. Used in facial recognition, medical imaging, autonomous vehicles, and quality control.

Robotics

Physical machines enhanced with AI for sensing, decision-making, and action. Deployed in manufacturing, logistics, healthcare, and exploration.

Expert Systems

Rule-based decision engines that emulate human expertise. Used in medical diagnostics, financial planning, and regulatory compliance.

Generative AI

Systems that create new content like text, images, audio, and video. Transforming creative industries, content production, and design.

Types of AI: By Learning Method

Key Considerations for Business Leaders

- Different learning methods are appropriate for different business problems and data availability
- Supervised learning requires high-quality labeled data, which can be expensive to create
- Reinforcement learning excels in dynamic environments with clear feedback signals
- Self-supervised learning is transforming AI by enabling learning from vast amounts of unlabeled data
- Many production AI systems combine multiple learning approaches for optimal results

Understanding these learning methods helps business leaders make informed decisions about AI investments and implementation strategies.

Supervised Learning

Learns from labeled data to make predictions. Used in spam detection, image classification, and predictive analytics.

Unsupervised Learning

Finds patterns in unlabeled data. Enables customer segmentation, anomaly detection, and recommendation systems.

Reinforcement Learning

Learns via rewards/punishments in an environment. Powers game-playing AI, robotics, and autonomous systems.

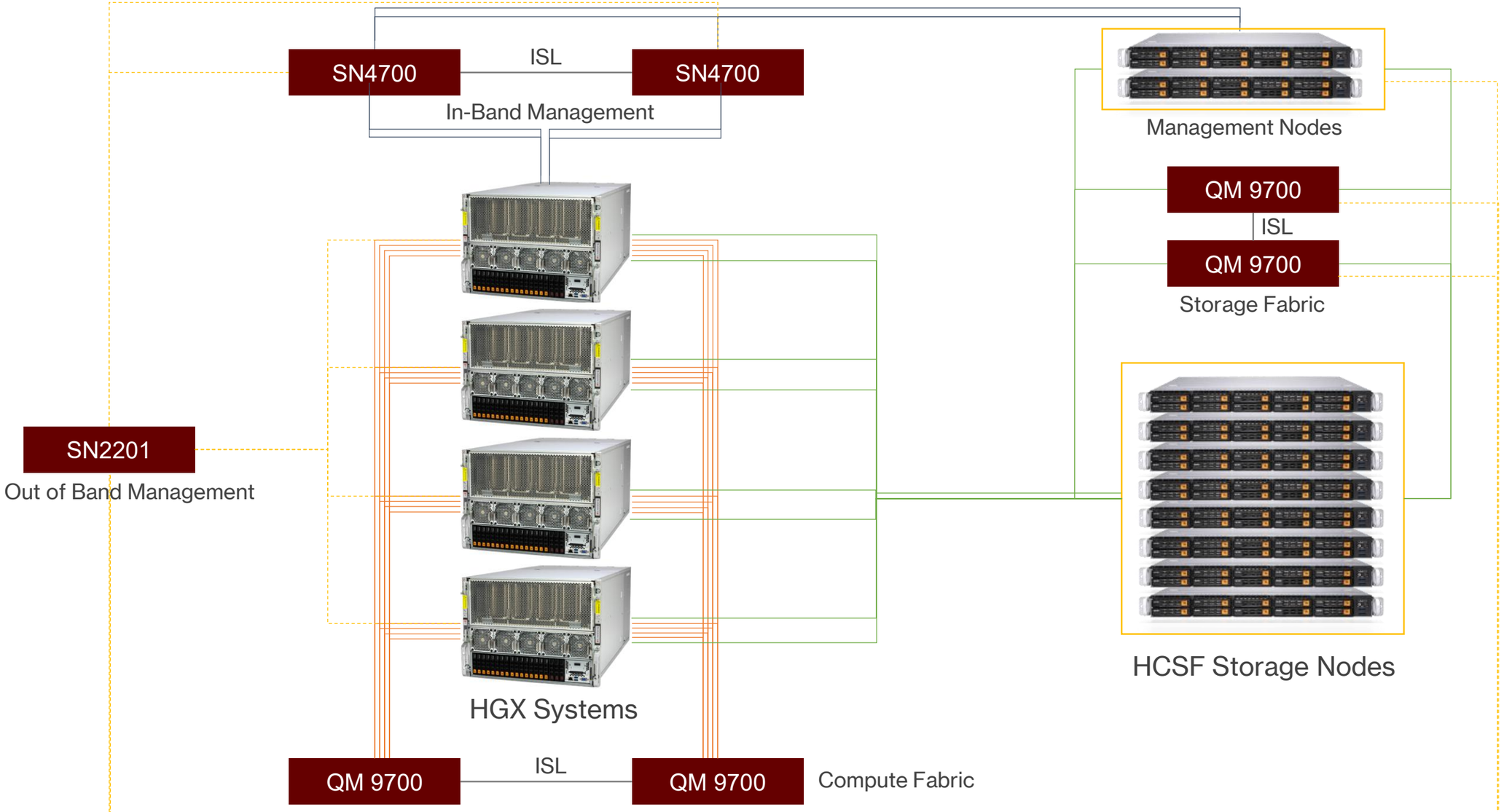
Semi-Supervised Learning

Uses mixed labeled/unlabeled data. Applied in speech recognition, medical imaging, and natural language processing.

Self-Supervised Learning

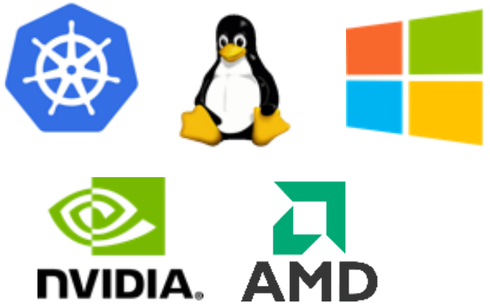
Generates its own labels from data. Foundation of large language models like GPT and emerging visual models.

Hitachi iQ AI Reference Architecture

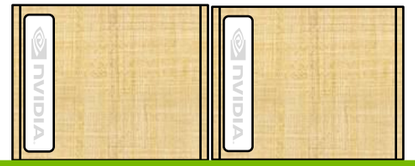


Data Platform Architecture

AI/ML/HPC Applications



GPU Resources



HPC Apps

Containerized Apps

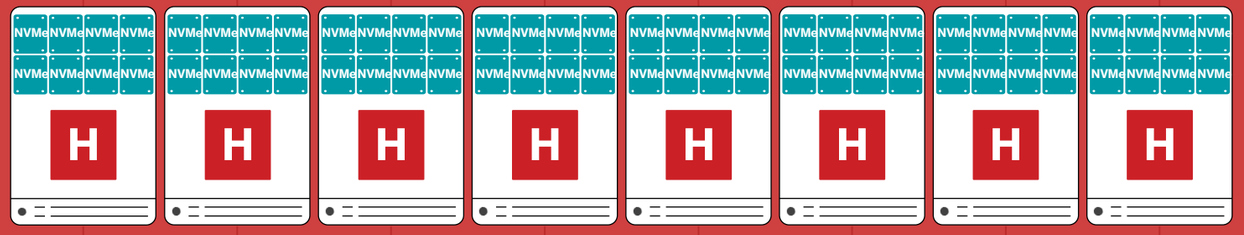
Traditional Interfaces

InfiniBand/Ethernet Network

- ✓ Separate tenants for application and scratch space
- ✓ GPU Direct Storage (GDS)
- ✓ S3, NFS, SMB and POSIX access
- ✓ Cloud Bursting to Hyper scalers
- ✓ Unified namespace with tiered file system

Unified Namespace

High Performance NVMe Tier



25gbE Private Back-end Ethernet Network

HCP for Cloud Scale, On-Prem Object Storage

High Performance NVMe Tier

Exa Scale Capacity Tier

H HCSF Client

H HCSF Server

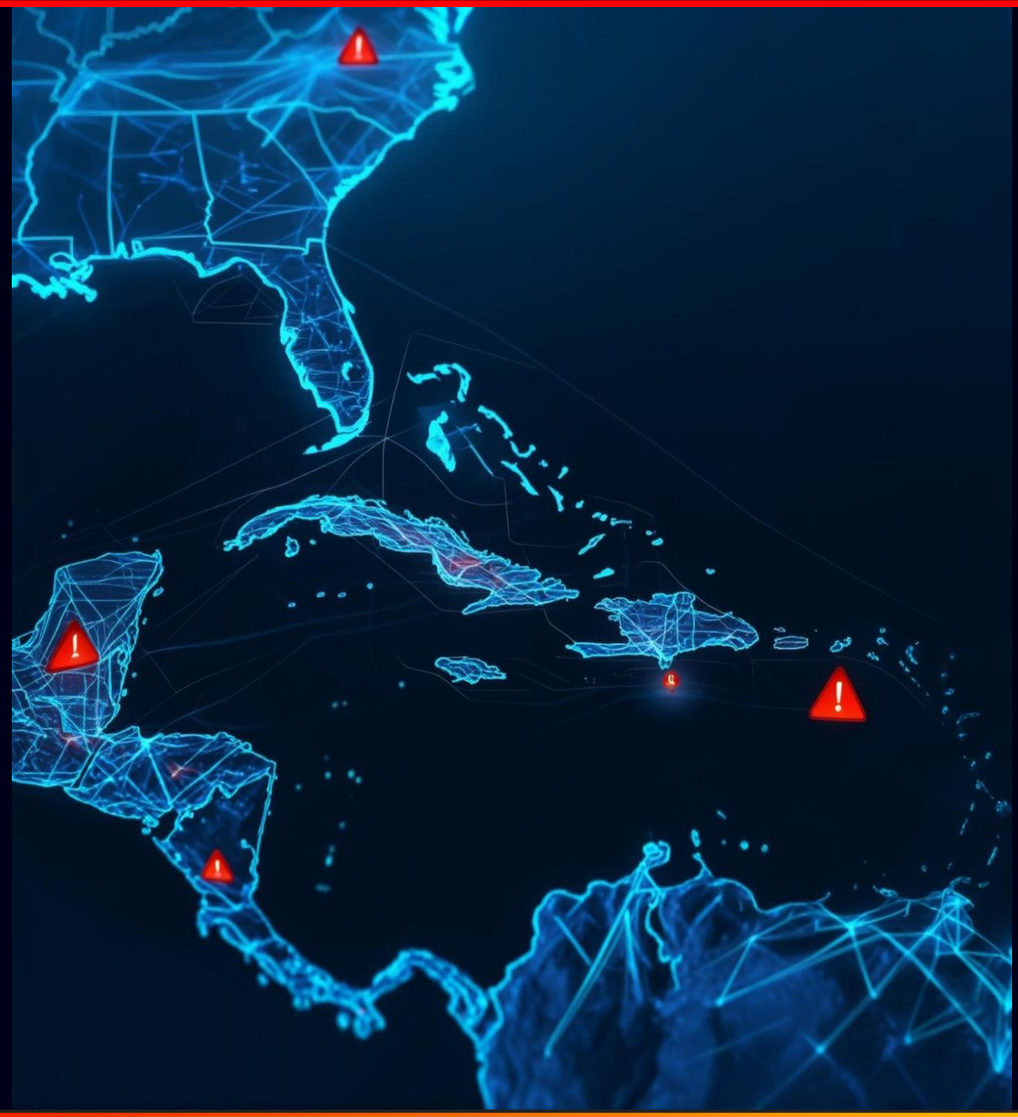
The CyberSecurity Landscape

The Cybersecurity Landscape in the Caribbean

The Caribbean region is experiencing rapid digital transformation, creating new vulnerabilities that cybercriminals are actively exploiting. Regional cybersecurity maturity remains concerning, with an average score of just 10.2 out of 20 as of 2024 assessments.

This digital security gap has led to alarming statistics:

- 144 million cyberattack attempts documented in the first half of 2022 alone
- Ransomware emerging as the dominant attack vector
- Double extortion tactics becoming increasingly prevalent
- Critical infrastructure particularly vulnerable due to outdated systems



Cybersecurity Threat Landscape: 2025 By The Numbers

343M

Victims

Individuals affected by cyberattacks in 2023, with projections showing this number reaching 500M by the end of 2025

126%

Ransomware Growth

Year-over-year increase in ransomware attacks, with healthcare and critical infrastructure as primary targets

1,925

Weekly Attacks

Average number of attacks per organization each week, a 37% increase from 2024 figures

$4.88M

Breach Cost

Average cost of a data breach, with regulatory fines accounting for 23% of total costs

16B

Leaked Credentials

Total credentials exposed on dark web markets, a 42% increase from previous year

Critical Insights

Human error remains the primary vulnerability vector, involved in 74% of successful breaches. Meanwhile, global cybercrime costs are projected to reach $10.5 trillion annually by the end of 2025, representing the largest transfer of economic wealth in history.

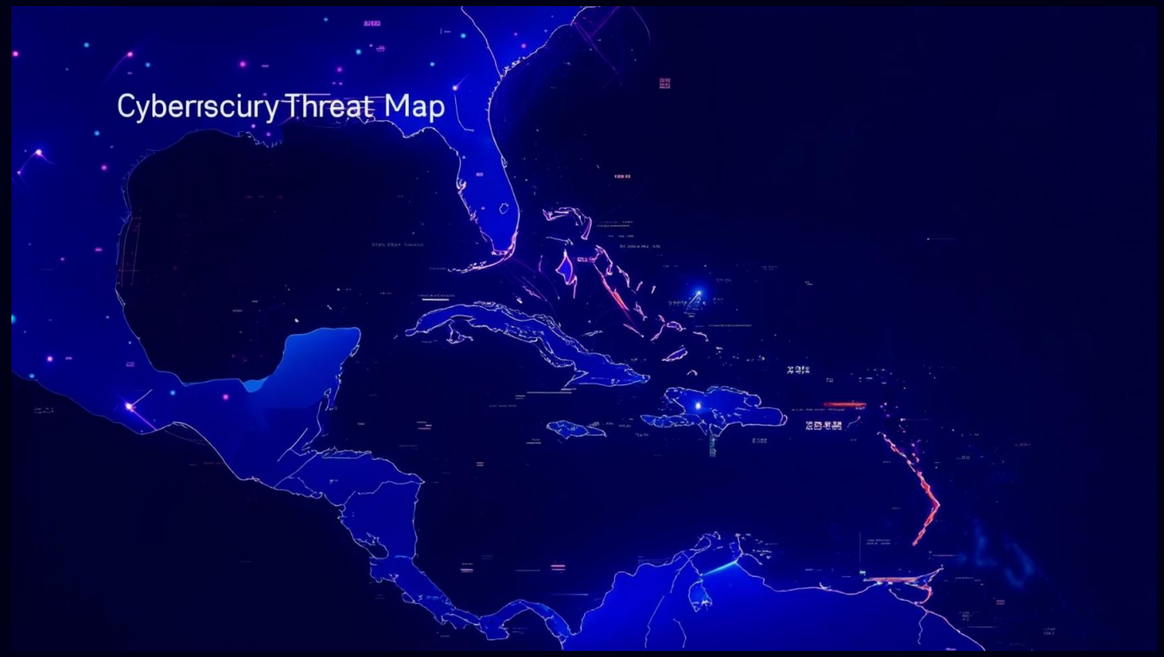
The most concerning trend is the democratization of advanced attack techniques. Nation-state level capabilities landscape are now available to criminal groups through Malware-as-a-Service platforms, dramatically expanding the threat or organizations of all sizes.

Caribbean Cybersecurity Landscape: Rising Threats

The Caribbean region faces an escalating cybersecurity crisis, with Jamaica alone experiencing **over 4 million cyberattack attempts** in the first half of 2024. These attacks predominantly target:

- Critical financial infrastructure and tourism systems
- Government services and healthcare networks
- Telecommunications providers and internet service operations

Regional challenges are compounded by underinvested infrastructure, fragmented cybersecurity policies across different islands, and heavy dependence on third-party and foreign hosting services.



62%

Increase in ransomware attacks (YOY)

73%

Organizations lacking incident response plans

41%

Attacks targeting telecommunications

Digital Economy Growth & Vulnerabilities

Rapid Digital Adoption

Financial services, healthcare, tourism, and e-government sectors rapidly digitizing across the Caribbean

Mobile-First Region

~70% mobile internet penetration with mobile connections exceeding population in many islands

SME Vulnerability

Small businesses (~95% of regional companies) lack resources for adequate cybersecurity protection

Resource Constraints

Limited regional cybersecurity service providers and significant affordability challenges

Comprehensive Caribbean Cybersecurity Regulations – A Summary

Country	Legal System	Key Cybersecurity Legislation(s)	Year Enacted
Antigua & Barbuda	Common Law	Electronic Crimes Act, Data Protection Act	2013
Bahamas	Common Law	Cybercrime Act, Data Protection Act	2018
Barbados	Common Law	Cybercrime Act, Data Protection Act	2019
Belize	Common Law	Cybercrime Act, National Cybersecurity Strategy (2020-2023)	
Bermuda	Common Law	Computer Misuse Act, Data Protection Act	2014
British Virgin Islands	Common Law	Computer Misuse Act, Data Protection Act	2015
Cayman Islands	Common Law	Computer Misuse Law, Data Protection Law	2017
Dominica	Common Law	Cybercrime Act	2016
Grenada	Common Law	Cybercrime Act	2017

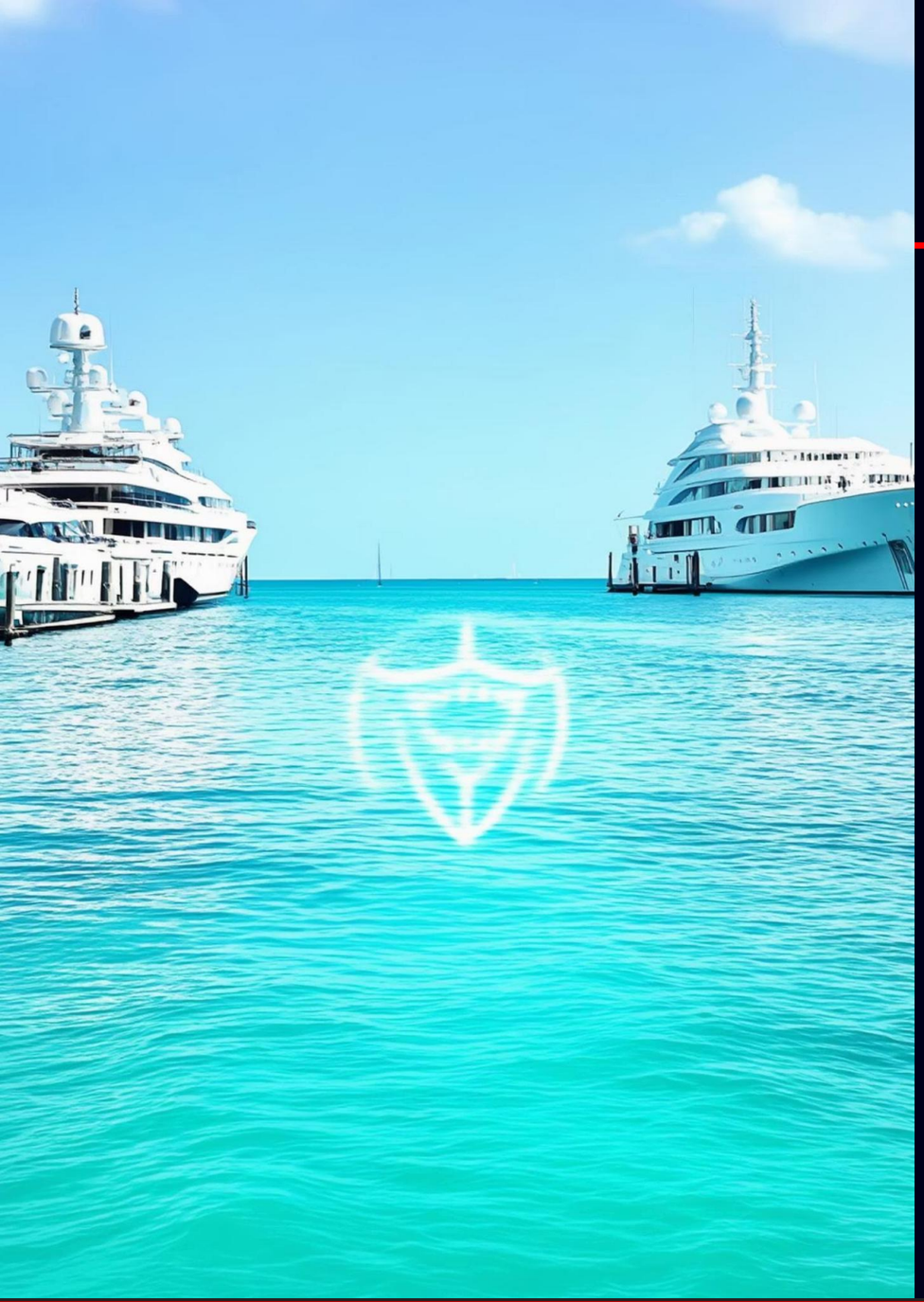
2018-2020

This comprehensive overview demonstrates the region's commitment to cybersecurity, with most nations adopting legislation between 2013-2020. Common Law dominates the regulatory landscape, with 15 of 17 specifically listed nations following this system. While all countries have enacted some form of cybercrime legislation, data protection frameworks remain inconsistent, highlighting an area for future regional harmonization.

Comprehensive Caribbean Cybersecurity Regulations – A Summary Con’t

Country	Legal System	Key Cybersecurity Legislation(s)	Year Enacted
Guyana	Common Law	Cybercrime Act, Data Protection Act	2018
Haiti	Civil Law	Cybercrime Law	2017
Jamaica	Common Law	Cybercrimes Act, Data Protection Act	2015, 2020
Saint Kitts and Nevis	Common Law	Computer Misuse Act, Data Protection Act	2014
Saint Lucia	Common Law	Cybercrime Act, Data Protection Act	2017
Saint Vincent & Grenadines	Common Law	Cybercrime Act	2018
Suriname	Civil Law	Cybercrime Law	2019
Trinidad and Tobago	Common Law	Cybercrime Act, Data Protection Act	2018
Others (e.g., Montserrat, Anguilla)	Common Law	Various Cybercrime and Data Protection Acts	2013-2020

This comprehensive overview demonstrates the region's commitment to cybersecurity, with most nations adopting legislation between 2013-2020. Common Law dominates the regulatory landscape, with 15 of 17 specifically listed nations following this system. While all countries have enacted some form of cybercrime legislation, data protection frameworks remain inconsistent, highlighting an area for future regional harmonization.



Bahamas Cybersecurity Regulations

Data Protection Act (2020)

Comprehensive legislation governing collection, processing, and storage of personal data with explicit security requirements. Established the Office of the Data Protection Commissioner with enforcement powers. Includes cross-border data transfer restrictions.

Computer Misuse Act (2018)

Addresses cybercrime offenses including unauthorized access, system sabotage, illegal interception, and computer-related fraud. Penalties include fines up to B$100,000 and imprisonment up to 10 years for serious offenses.

National Cybersecurity Strategy (2023)

Five-year plan focusing on critical infrastructure protection, digital economy security, and public awareness. Established the Bahamas Computer Incident Response Team (BahCIRT) with a B$4.7 million operational budget

Guyana Cybersecurity Regulations

Computer Crime Act (2018)

Criminalized unauthorized access, data interception, system interference, and computer-related fraud. Penalties include fines up to GYD$10 million and imprisonment up to 10 years for serious offenses involving critical infrastructure.

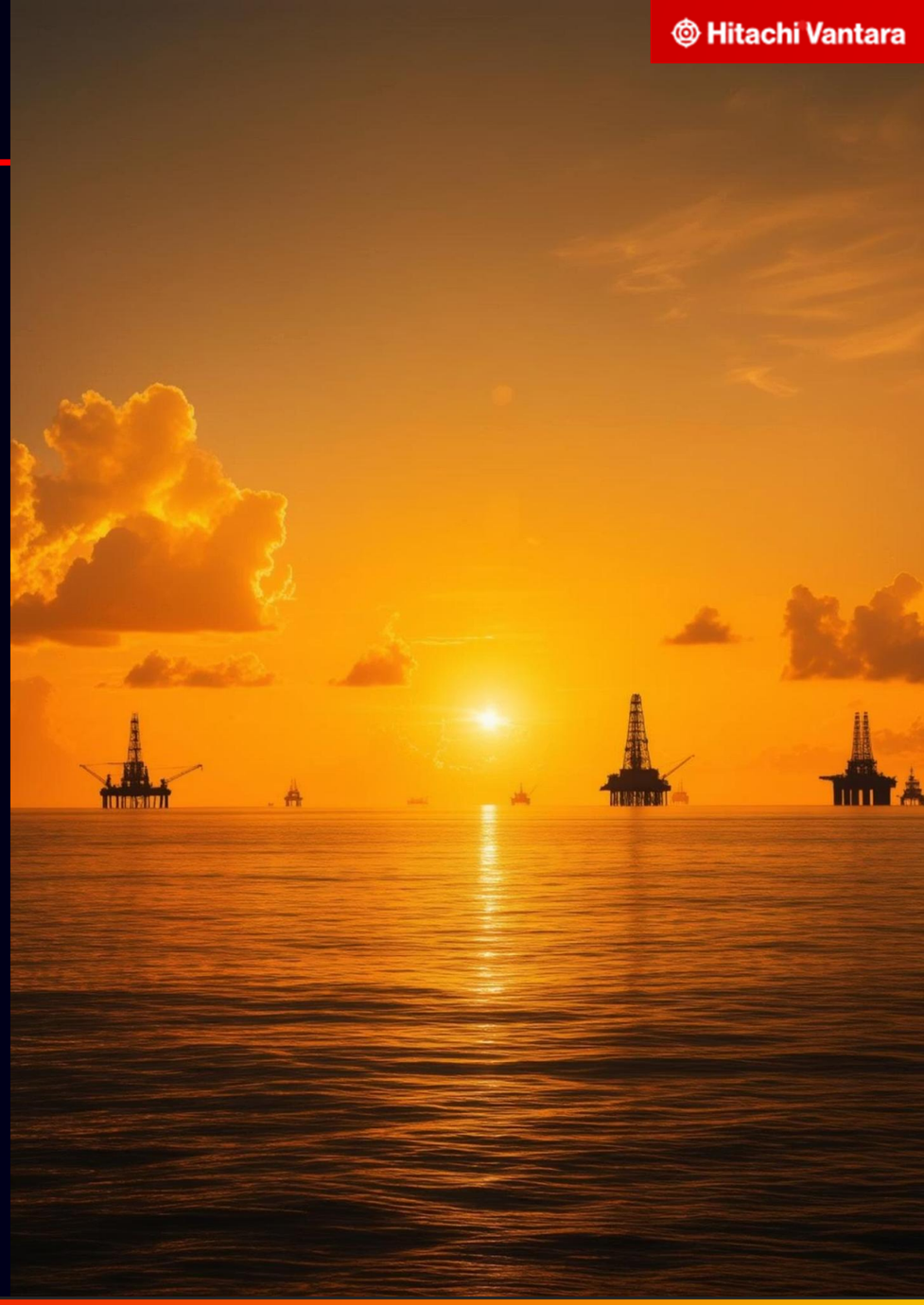
Data Protection Bill (Pending)

Comprehensive data protection legislation introduced to Parliament but not yet enacted as of 2025. The draft bill includes GDPR-influenced provisions for security requirements, breach notification, and data subject rights.

Sector-Specific Regulations

Bank of Guyana Cybersecurity Guidelines (2022) established mandatory security controls for financial institutions. The Telecommunications Agency issued Critical Infrastructure Security Directives (2023) for telecom operators.

Guyana is establishing a national Computer Emergency Response Team with expanded focus on protecting oil and gas infrastructure. Regional cooperation remains critical for enforcement capacity.



Hitachi Cyber Security Services Portfolio

HITACHI
Inspire the Next

Virtual CISO & Advisory Services

- Virtual CISO, Architect and/or Security Team
- Strategic Planning
- Risk Management
- Policy Development
- Compliance Assurance
- Vendor Management

Cyber Threat Intelligence

- External Attack Management
- Digital Risk Protection Services
- Brand Exposure Protection
- Data Leaks Identification
- Dark Web Monitoring

Penetration Testing

- Infrastructure Penetration Testing
- Application Penetration Testing
- Mobile Web Application Testing
- Wireless (WiFi) Penetration Testing
- Hardware Testing
- Static Code Analysis
- Code Review
- Objective-Based Testing
- Attack Surface Hunting

Architecture Security

- Network Architecture & Configuration Assessment & Design Support
- Cloud Migration - Security Architecture Design Support
- M365 Security Configuration Assessment + Deployment Support
- Azure Security Configuration + Virtual Architecture Assessment & Deployment Support
- Application Security Architecture & Risk Assessment
- OT Network Security Assessment - ISA/IEC 62443 Guidelines
- Identity Access Management Assessment
- Network Infrastructure Security
- Cloud Computing Considerations
- Application Security
- Endpoint Device Protection
- Data Security Measures
- User Authentication and Access Controls
- Addressing Security Challenges Across Domains
- Malware Resiliency Assessment

Governance, Risk & Compliance

- Enterprise Security Program Development
- IT/OT Risk Management
- Security Controls Gap Assessment (ISO, NIST, CObIT, SANS)
- Compliance Assessments (HIPAA, SOC 1/2, NIST CSF, CSA CCM, CAN CIOSC, CIS) & Attestation (PCI DSS, ISO2700x, SWIFT)
- Security Policy & Procedures Development
- Training and Awareness
- Business Continuity and Disaster Recovery Advisory
- Business Impact Assessment
- Cybersecurity Governance
- Vulnerability Risk Management Program
- Threat Risk Assessment
- Cybersecurity Insurance Compliance

Virtual DPO & Privacy Services

- Virtual DPO Services/Support to Internal DPO
- Compliance Assurance
- Privacy Frameworks
- Data Protection Policies
- Privacy Impact Assessments
- Data Breach Response
- Vendor Management

Vulnerability Assessment

- Vulnerability Scanning
- Risk Assessment for IT and OT/IoT Technologies
- Vulnerability Patching Plans

Training, Social Engineering & Simulations

- Tailored Cybersecurity, Privacy & GRC Training
- Executive & Board Training
- Middle Management Empowerment
- Security-by-Design Training for Technical Staff
- General Employee Awareness
- Social Engineering & Phishing Campaigns
- Agency-Wide Simulations & Tabletop Exercises (Red Team-Blue Team and Purple Team Scenarios).

Cyber Resilience & Incident Response

- Proactive Resilience Strategies
- Business Continuity Planning
- Disaster Recovery Planning
- Trusted Defense Enhancement
- Incident Response Process and Playbook Development
- Security Incident Response (Retainer or Post-breach)
- Compromise Investigation and Assessment (May Include Subcontracted Digital Forensics)
- Vulnerability Management Audit
- Firewall Policy Audit
- Endpoint Protection Configuration Audit
- Environment Monitoring/Logging Audit
- Cyber Resiliency Assessment

24/7 Managed Security Services

- Managed Detection and Response Leveraging Microsoft Sentinel
- IT/OT Event Monitoring Without Response, Integrated with Microsoft Sentinel
- Vulnerability Management
- Managed Security for PCI-DSS Compliance, Including ASV Scanning
- Endpoint Detection and Response
- Network Detection and Response
- Cloud Security Monitoring: Managed Security for AWS, Azure, and M365

The Breaches

Trinidad and Tobago: TSTT Ransomware Attack (Nov 2023)

Initial Breach

Ransomexx ransomware group successfully infiltrated Telecommunications Services of Trinidad and Tobago (TSTT) network through phishing attack

Data Compromise

Attackers exfiltrated 6GB of sensitive data affecting over 1.2 million customers, including names, emails, national IDs, phone numbers, and Social Security Numbers

Aftermath

CEO terminated following widespread criticism of breach handling and transparency issues; Prime Minister declared the incident a "national security threat"

Jamaica: Surge in Ransomware Attacks (2024-2025)

Jamaica has faced an unprecedented wave of sophisticated ransomware attacks between 2024-2025, with two major threat actors dominating the landscape:

FOG Ransomware Group

- Primary target: education sector
- Notable breach: Northern Caribbean University
- Tactics: Initial phishing followed by lateral movement

Akira Ransomware Group

- Responsible for 300+ Jamaican victims in 2024
- Already claimed 200+ victims in early 2025
- Double extortion: data exfiltration plus encryption
- Demanded ransoms primarily in Bitcoin

Bahamas: Increasing Cyber Threats (2023-2025)

Financial Sector Targeting

Sophisticated ransomware campaigns specifically targeting Bahamian financial institutions, with multiple banks reporting breach attempts. Attackers exploited vulnerabilities in legacy banking infrastructure.

Government Systems

Several government departments faced prolonged service disruptions due to malware infections. Public reporting remained limited, but internal documents revealed extensive data access by unauthorized parties.

Identity Theft Surge

Following multiple data breaches, Bahamian citizens experienced a 340% increase in identity theft cases from 2023-2025. Financial fraud using stolen credentials became widespread.

Barbados and Guyana: Emerging Cyberattack Patterns

Barbados

Key government ministries suffered coordinated attacks in mid-2024, with attackers combining sophisticated social engineering with custom malware deployments. The Central Bank of Barbados reported multiple attempted breaches targeting financial data.

- Tourism sector particularly vulnerable
- Critical data compromised including citizen records
- Average system downtime: 9.2 days

Guyana

Emerging oil industry made Guyana an attractive target, with evidence of nation-state sponsored attacks alongside criminal enterprises. Multiple government portals experienced extended outages.

- Energy sector primary target
- Industrial control systems compromised
- Business disruptions affected GDP growth

Other Caribbean Nations: Attack Patterns

Cloud Exploitation

Attackers across Curacao, St. Maarten, and Bermuda exploited misconfigured cloud services to exfiltrate sensitive data. AWS S3 buckets and Azure storage were common targets with inadequate security controls.

Phishing Campaigns

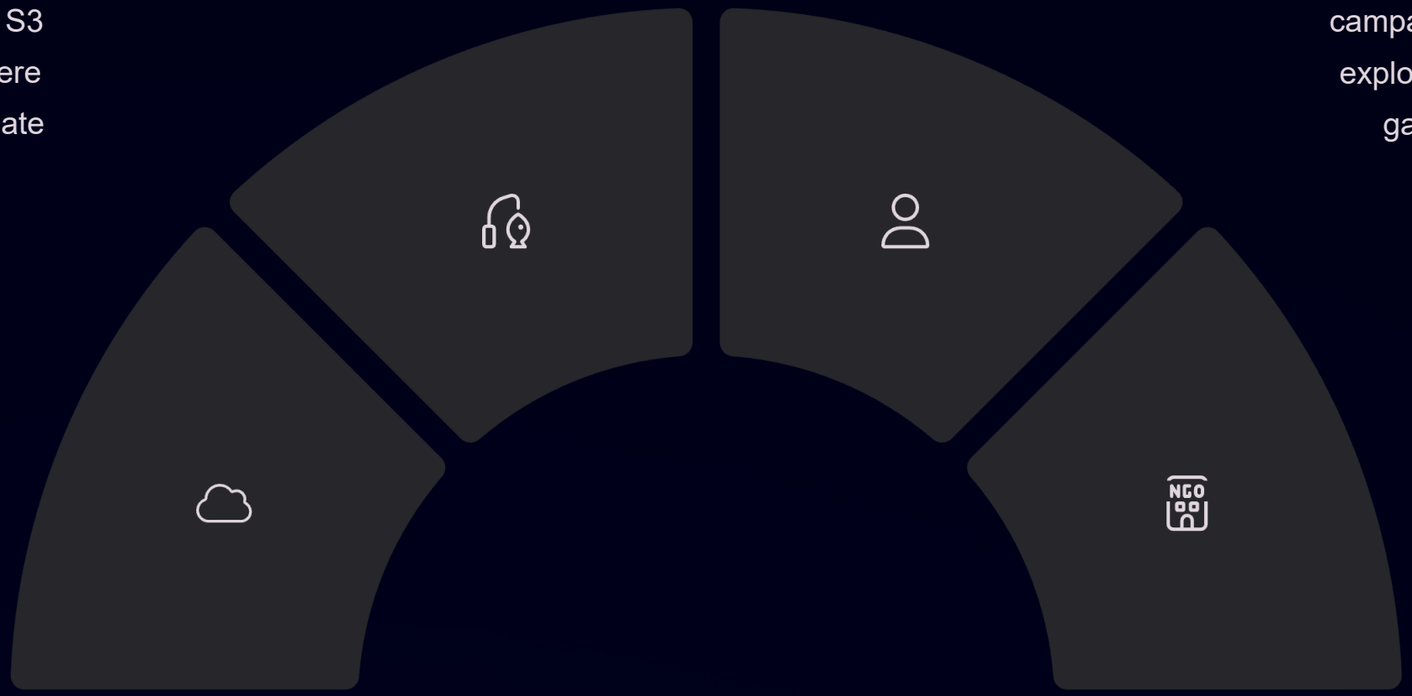
Montserrat, Grenada, and Antigua and Barbuda faced sophisticated phishing operations targeting government officials. Campaigns used local cultural references to improve effectiveness.

Ransomware

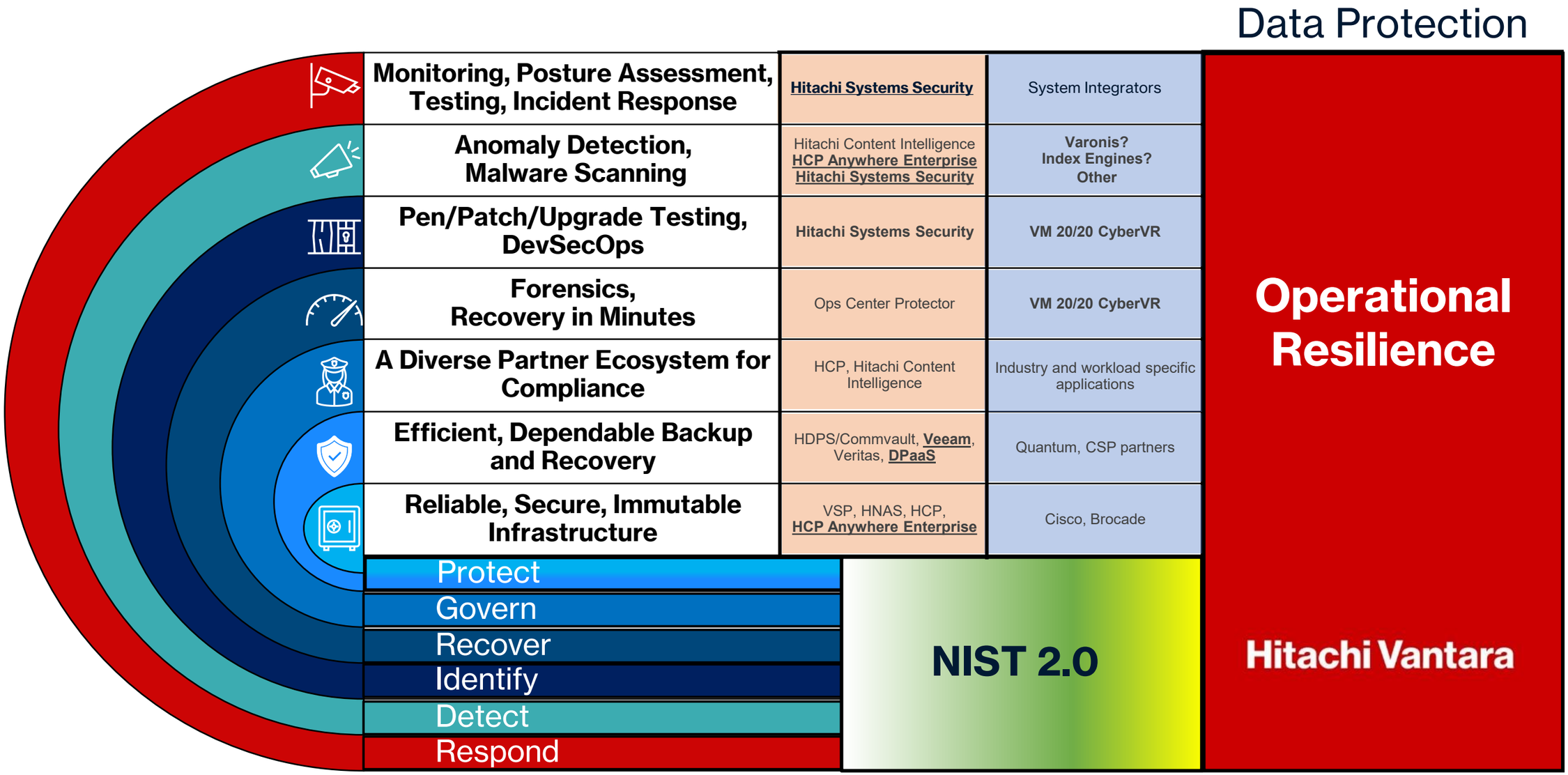
Tourism and hospitality sectors in Turks and Caicos and Anguilla suffered multiple ransomware incidents, with several luxury resorts forced to pay ransoms to recover critical reservation systems.

Criminal Organization

Evidence suggests coordinated campaigns by organized crime groups exploiting the region's digital security gaps and limited cybersecurity personnel resources.



Defense-in-Depth, A Layered Approach, HV 7-Layers of Data Resilience



The Threat Actors

Attack Methods and Threat Actors

Primary Threat Actors

- **Ransomexx:** Sophisticated double-extortion ransomware, hit TSTT
- **FOG:** Education sector specialist, active in Jamaica
- **Akira:** High-volume attacker, 500+ Caribbean victims
- **BlackCat:** Critical infrastructure targeting
- **Cl0p:** Financial sector focus with data exfiltration

Common Attack Vectors

- Social engineering (phishing, smishing) as primary initial access
- Unpatched vulnerabilities in public-facing applications
- Credential stuffing against weak authentication systems
- Living-off-the-land techniques to evade detection

Impact on Businesses and Governments

$2.09M

Average Breach Cost

Per incident cost for Caribbean businesses in 2022, representing a 17% increase from previous year

1.2M+

Identities Exposed

Personal records compromised in TSTT breach alone, creating long-term identity theft risks

19.4

Days Downtime

Average system downtime following ransomware attacks, severely disrupting operations

68%

Public Trust Decline

Percentage drop in public confidence following government data breaches

Beyond immediate financial impacts, Caribbean organizations suffer long-term reputational damage, customer churn, and regulatory scrutiny following successful cyberattacks.

Case Study: Northern Caribbean University (Jamaica)

1

October 4, 2024

FOG ransomware gang initiates phishing campaign targeting administrative staff with malicious Microsoft 365 links

2

October 5, 2024

Initial access gained through compromised administrator credentials; lateral movement begins across university network

3

October 6, 2024

Exfiltration of 2.3TB of data including student records, financial information, and research data

4

October 7, 2024

Encryption deployed across 83% of university systems; ransom demand of 45 Bitcoin (~$1.8M) delivered

5

October-December 2024

University rebuilds systems from backups; implements enhanced security protocols and awareness training

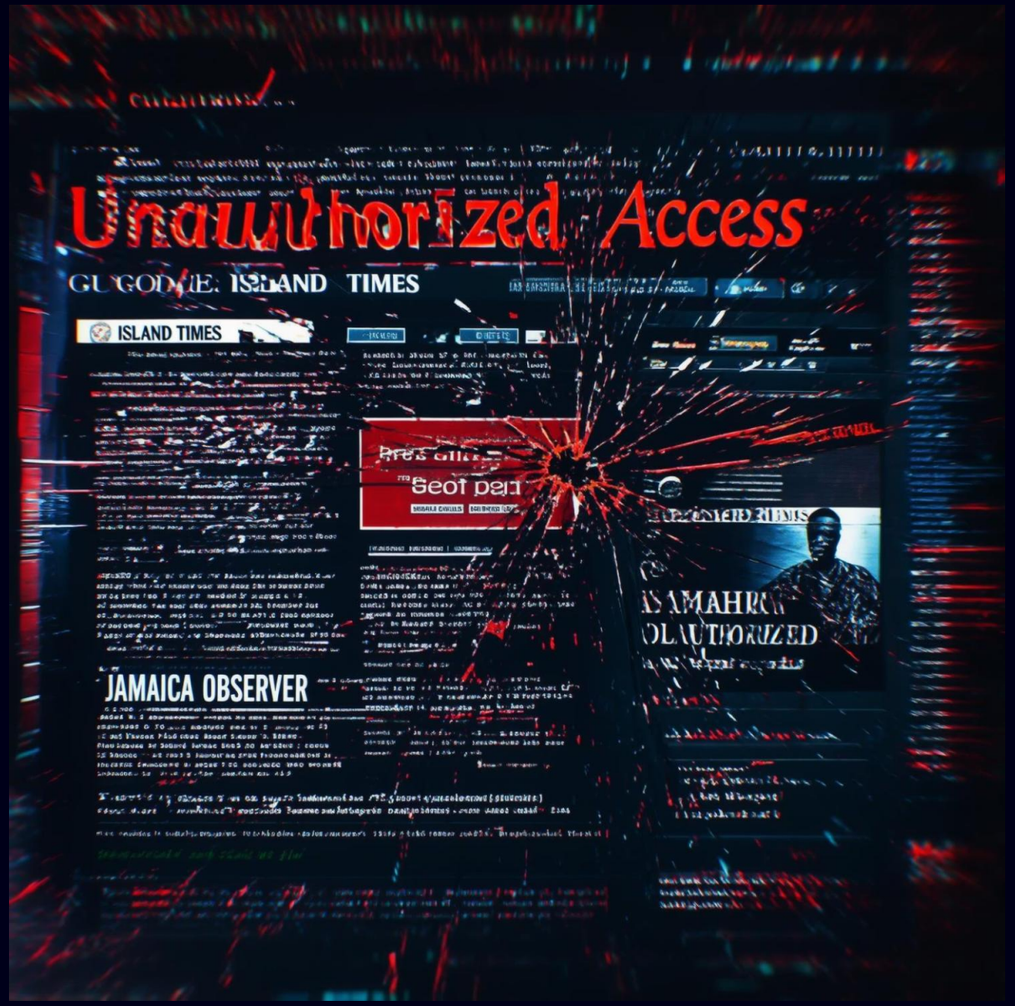
Case Study: Caribbean National Weekly Cyberattack

In March 2024, the Caribbean National Weekly media organization suffered a sophisticated cyberattack that highlighted the vulnerability of regional media outlets.

Attack Details

- Initial access via spear-phishing targeting senior editors
- Website defacement with politically motivated messages
- Complete theft of email archives and source materials
- Exposure of confidential journalist sources putting individuals at risk
- Publication disrupted for 17 days

The attack demonstrated the need for enhanced media cybersecurity and raised concerns about press freedom implications of such targeted campaigns.



Emerging Threats: Smishing and Mobile Attacks

Mobile-First Attack Landscape

The Caribbean region is experiencing a significant shift toward mobile-focused cyberattacks, with smishing (SMS phishing) campaigns increasing by 287% from 2023 to 2025.

Key trends include:

- Geographically targeted SMS campaigns impersonating local banks
- Malicious apps designed specifically for Caribbean users
- Mobile payment system exploitation
- SIM swapping attacks targeting high-net-worth individuals
- Banking trojans customized for regional financial institutions

With smartphone penetration exceeding 85% across most Caribbean nations, these attacks have a vast potential victim pool.

Cyber Resiliency

Cyber Resilience Pillars for the Caribbean

Prevention

- Next-generation firewalls
- Multi-factor authentication
- Endpoint protection systems
- User awareness training

Recovery

- Robust data backup systems
- Rapid restoration capabilities
- Legal and compliance guidance
- Post-incident analysis

Detection

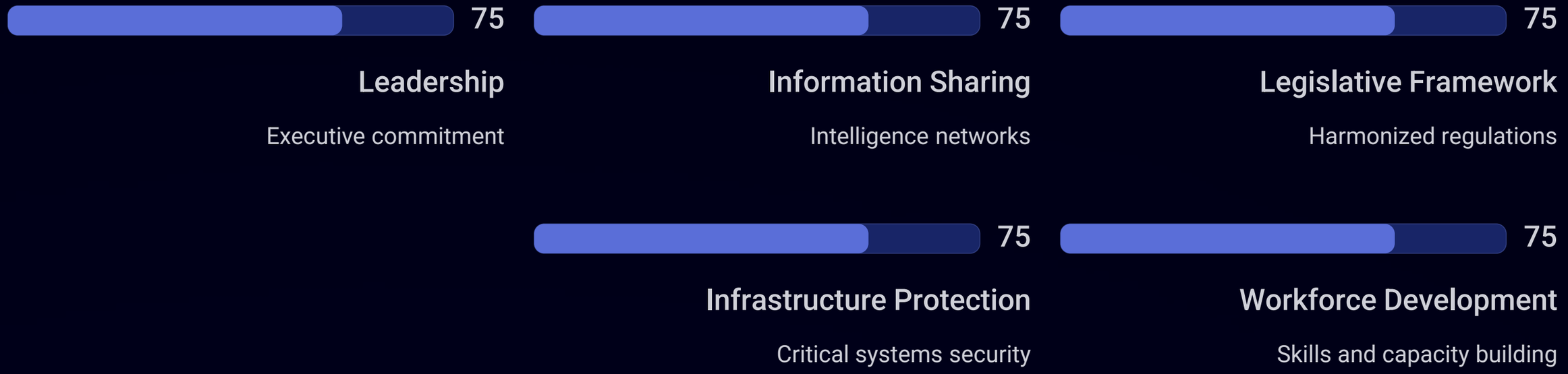
- Real-time network monitoring
- Behavioral anomaly detection
- Threat intelligence integration
- Vulnerability scanning

Response

- Incident response plans
- Business continuity protocols
- Crisis communication frameworks
- Stakeholder coordination

Effective cyber resilience requires a balanced investment across all four pillars, tailored to the unique context of Caribbean organizations and infrastructure.

Regional Cyber Resilience Strategy 2030 (CARICOM-USAID)



The CARICOM-USAID Regional Cyber Resilience Strategy 2030 represents the most comprehensive collaborative effort to date, addressing both individual nation-state needs and collective regional security. The multi-level approach strengthens information sharing mechanisms while addressing critical legislative gaps and infrastructure vulnerabilities.

Caribbean Digital Transformation Initiatives

OECS Caribbean Digital Transformation Project (CARDTP)

The CARDTP represents a comprehensive regional approach to digital development, with four key components:

1. Digital enabling environment enhancement through policy and regulatory reforms
2. Digital government infrastructure, platforms, and services development
3. Digital skills and technology adoption acceleration across public and private sectors
4. Project implementation support including monitoring, evaluation, and stakeholder engagement

Central to these initiatives is the establishment of national Computer Incident Response Teams (CIRTs) and development of robust cybersecurity policy frameworks, capacity building programs, and emergency planning tools.

Fortifying with Technology:

A Proactive Defense

Hitachi CyberSecurity: Offering Comprehensive Cybersecurity Solutions

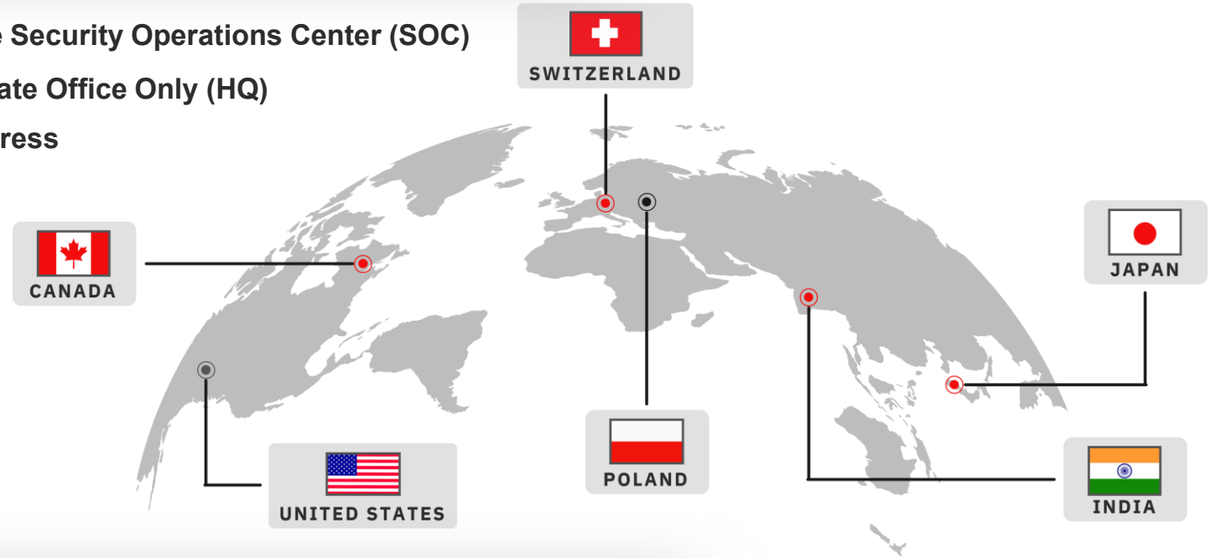
Who We Are

With over 25 years of experience, Hitachi Cyber has established itself as a trusted partner, delivering tailored cybersecurity solutions to organizations of all sizes and across various industries.

- **Global Leader in Cybersecurity**
- **Promoting Secure Growth**
- **Innovative Approach to Security**
- **24/7 Operations**

Our Footprint

- On-Site Security Operations Center (SOC)
- Corporate Office Only (HQ)
- In Progress



Our Top Tier Certifications & Expertise

PCI Qualified Security Assessor (QSA)
OHSAS 18001 SGS
afaq ISO 27001 Information Security
FIRST Improving Security Together
SWIFT CSSP
SOC 2 TYPE 2 AICPA SOC

Our Services

24/7 Managed Security Services

Vigilant threat detection, investigation, and response round the clock, every day of the year.

Professional Services

Guidance, accompaniment, and training on cybersecurity, privacy, and GRC.

Cyber Threat Intelligence

Actionable intelligence powered by AI and human expertise to safeguard digital assets.

Privacy and GRC Framework Expertise

Robust Privacy and GRC (Governance, Risk, Compliance) Frameworks

- Implementing comprehensive strategies for secure and compliant operations.

Compliance Ensured with a Range of Regulatory Frameworks

- Adherence to multiple regulations for enhanced business integrity.

Enhanced Data Protection and Regulatory Adherence

- Strengthening data security and regulatory compliance for trust and reliability.

Hitachi Cyber Security Services Portfolio

HITACHI
Inspire the Next

Virtual CISO & Advisory Services

- Virtual CISO, Architect and/or Security Team
- Strategic Planning
- Risk Management
- Policy Development
- Compliance Assurance
- Vendor Management

Cyber Threat Intelligence

- External Attack Management
- Digital Risk Protection Services
- Brand Exposure Protection
- Data Leaks Identification
- Dark Web Monitoring

Penetration Testing

- Infrastructure Penetration Testing
- Application Penetration Testing
- Mobile Web Application Testing
- Wireless (WiFi) Penetration Testing
- Hardware Testing
- Static Code Analysis
- Code Review
- Objective-Based Testing
- Attack Surface Hunting

Architecture Security

- Network Architecture & Configuration Assessment & Design Support
- Cloud Migration - Security Architecture Design Support
- M365 Security Configuration Assessment + Deployment Support
- Azure Security Configuration + Virtual Architecture Assessment & Deployment Support
- Application Security Architecture & Risk Assessment
- OT Network Security Assessment - ISA/IEC 62443 Guidelines
- Identity Access Management Assessment
- Network Infrastructure Security
- Cloud Computing Considerations
- Application Security
- Endpoint Device Protection
- Data Security Measures
- User Authentication and Access Controls
- Addressing Security Challenges Across Domains
- Malware Resiliency Assessment

Governance, Risk & Compliance

- Enterprise Security Program Development
- IT/OT Risk Management
- Security Controls Gap Assessment (ISO, NIST, CObIT, SANS)
- Compliance Assessments (HIPAA, SOC 1/2, NIST CSF, CSA CCM, CAN CIOSC, CIS) & Attestation (PCI DSS, ISO2700x, SWIFT)
- Security Policy & Procedures Development
- Training and Awareness
- Business Continuity and Disaster Recovery Advisory
- Business Impact Assessment
- Cybersecurity Governance
- Vulnerability Risk Management Program
- Threat Risk Assessment
- Cybersecurity Insurance Compliance

Virtual DPO & Privacy Services

- Virtual DPO Services/Support to Internal DPO
- Compliance Assurance
- Privacy Frameworks
- Data Protection Policies
- Privacy Impact Assessments
- Data Breach Response
- Vendor Management

Vulnerability Assessment

- Vulnerability Scanning
- Risk Assessment for IT and OT/IoT Technologies
- Vulnerability Patching Plans

Training, Social Engineering & Simulations

- Tailored Cybersecurity, Privacy & GRC Training
- Executive & Board Training
- Middle Management Empowerment
- Security-by-Design Training for Technical Staff
- General Employee Awareness
- Social Engineering & Phishing Campaigns
- Agency-Wide Simulations & Tabletop Exercises (Red Team-Blue Team and Purple Team Scenarios).

Cyber Resilience & Incident Response

- Proactive Resilience Strategies
- Business Continuity Planning
- Disaster Recovery Planning
- Trusted Defense Enhancement
- Incident Response Process and Playbook Development
- Security Incident Response (Retainer or Post-breach)
- Compromise Investigation and Assessment (May Include Subcontracted Digital Forensics)
- Vulnerability Management Audit
- Firewall Policy Audit
- Endpoint Protection Configuration Audit
- Environment Monitoring/Logging Audit
- Cyber Resiliency Assessment

24/7 Managed Security Services

- Managed Detection and Response Leveraging Microsoft Sentinel
- IT/OT Event Monitoring Without Response, Integrated with Microsoft Sentinel
- Vulnerability Management
- Managed Security for PCI-DSS Compliance, Including ASV Scanning
- Endpoint Detection and Response
- Network Detection and Response
- Cloud Security Monitoring: Managed Security for AWS, Azure, and M365

Hitachi Vantara

Maximizing Data Protection:
A Strategic Approach

Cyber Security – NIST 2.0 Framework

Key Functions

Governance Risk & Compliance

Governance & Policy

- Exec Security Committees
- Policies
- Key Controls
- SOP/ Governance

Risk Management

- Risk Framework
- Risk Assessment
- Asset Classification
- Asset Handling
- Risk Management Strategy
- 3rd Party Security Reviews

Compliance & Regulatory

- Audit/ Site Reviews
- SOC1, SOC2, SOX
- Legal/ Regulatory
- Security Awareness Training

Business Continuity & DR

Customer Assurance

- Annual Penetration Testing
- Sales Enablement
- Customer Escalations
- Security Collaterals
- White Papers
- Contract Negotiations

Identity & Access Management

IAM

- Business Requirements
- User Access Mgmt.
- Privileged Access Mgmt. (PAM)
- System/App Access Control
- Single Sign On (SSO)
- Multifactor Auth. (MFA)
- Enterprise Mobility Mgmt (EMM)/MDM Security
- Identity Governance
  - User Roles/Responsibilities
  - Authorization/Minimum Necessary Privilege

Venerability Mgmt.

- Vulnerability Mgmt.
- Asset Discovery & Compliance
- Patch Mgmt. Compliance
- Ensure SOC Functionality
- Automation

Data Security

Data At-Rest & In-Transit

- Cryptographic Controls
- Encryption at Rest
- Cryptographic Standards
- Certificate Authority/ PKI/HSM
- HSM Support and Management
- Key Custodian

Privacy

Privacy Ops

- Evidence Collection And Support of Certifications
- Business Impact Assessment of New Guidance From Legal Privacy Team
- Ensuring Appropriate Privacy Safeguards Are Implemented
- Maintain Privacy Certifications (Technical Certs)
- Enforcing Data Life-cycle Management
- Data Governance
- Data Loss Prevention Policies & Governance
- Privacy & Framework
  - Implement
  - Manage & Enhance
  - Validate
  - Compliance

Infrastructure Security

Proactive Monitoring

- Infrastructure Security
- Secure Hardening Requirements
- Security Standards
- Security Tool Implementation, Care & Feeding
- SIEM & SOAR Provider
- Security Architecture And Design
- Host Security

Operations

- Data Loss Prevention (DLP) enforcement
- Cloud Security
- Operational Software Control
- Vulnerability Mgmt.
- Asset Discovery & Compliance
- Patch Mgmt. Compliance
- Ensure SOC functionality
- Automation

Security Assurance

- Testing Security Open Readiness
- Red Team

Cyber Defense

Security Operations

- Downstream Logging/ Monitor/Reporting & SOAR Functionality
- Legal eDiscovery
- Threat Hunting
- Security Operational Readiness
- Onboarding/ Offboarding
- Event Monitoring
- Tier 1 Alert Triage

Incident Management

- Incident Response Plan
- IR playbooks
- Investigations
- Forensic Analysis
- Containment
- Recovery
- Remediation
- Metrics and Reporting
- IR Tabletop & Live Tests
- BCP/DR Alignment

Application Security

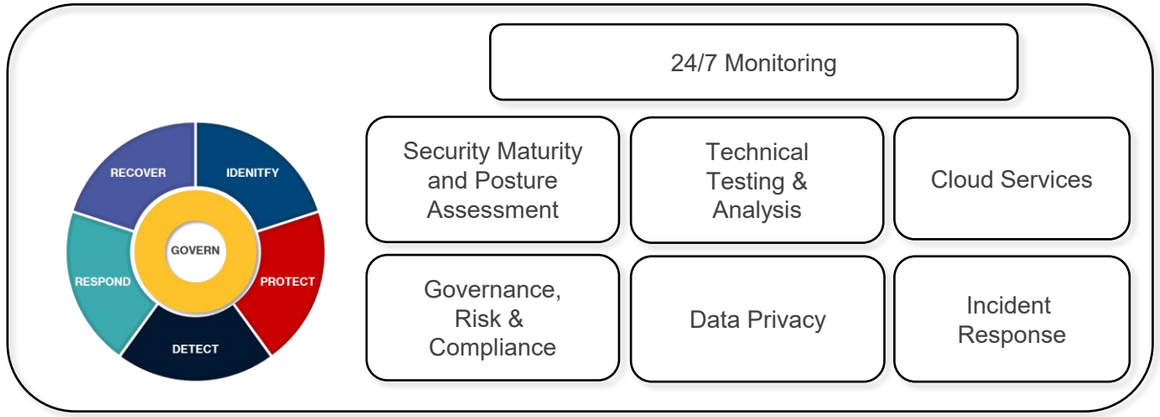
AppSec

- Security Reviews
- Engg Architecture And Design
- Secure Development Requirements
- SSDLC Program And Support Processes (OSAMM / AppSec)
- Security Bug Tracking And Closing
- Standards And Guidance
- Engg Training And Education Program
- R& D Penetration Testing Program

DevSecOps

- Software Composition Analysis
- Statistic Application Security testing
- Dynamic Application Security Testing
- Additional Tooling (Fuzzing Etc.)
- Secrets Mgmt.
- Container Security
- Code Signing

Hitachi Vantara Cyber Security & Resiliency

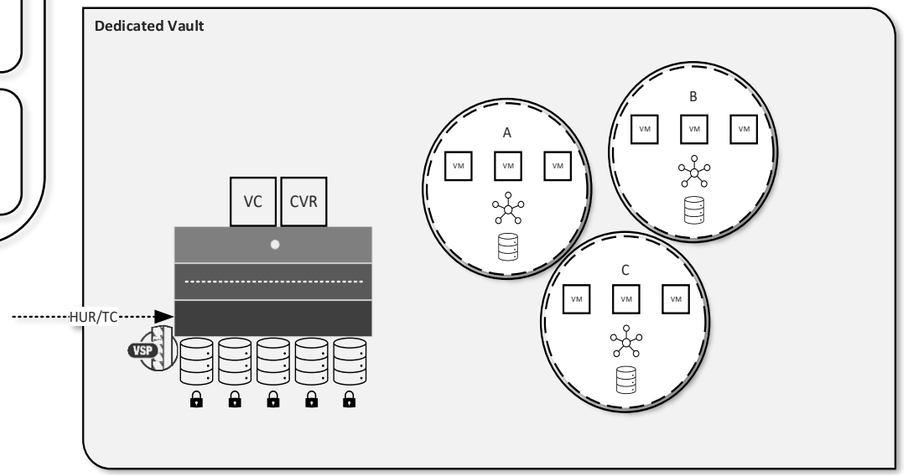


CyberVR **Ops Center Protector**

HITACHI OPS CENTER PROTECTOR · VERITAS · COMMVAULT · IBM Spectrum Protect · veeam · rubrik · actifio · ORACLE · SecureAgent Software · FalconStor · MODEL 9 · TRIBUTARY SYSTEMS

COMPUTE · NETWORKING

BLOCK · FILE · OBJECT · MAINFRAME · 3rd PARTY



Penetration Testing, Forensics, Control Validation

Test upgrades, patches, new applications

DevSecOps & ransomware recovery

Scalable Stay ahead of data growth

Affordable Reduce overall costs

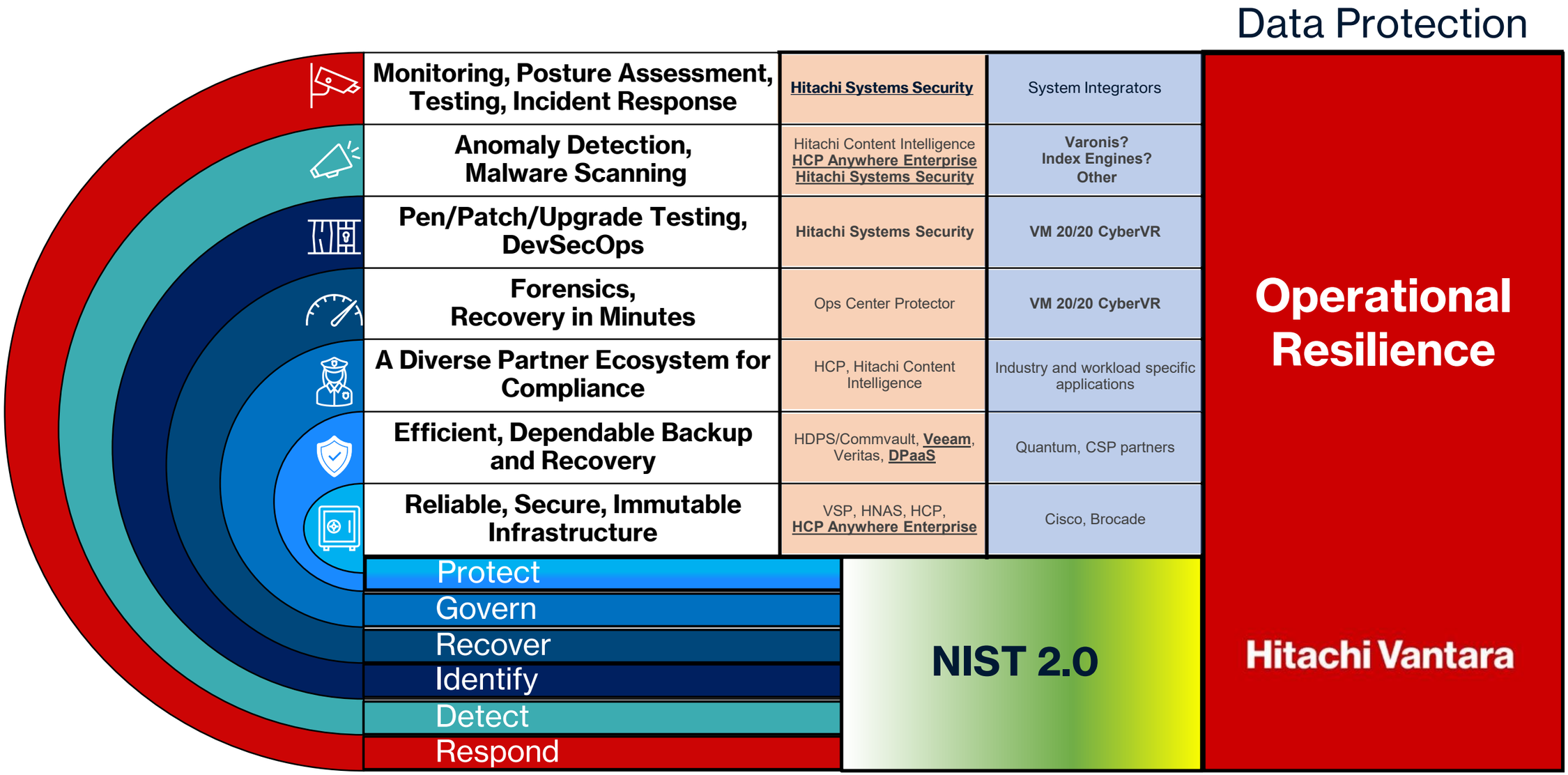
Fast Fulfill SLAs for RPO/RTO

Easy New capabilities for existing tools

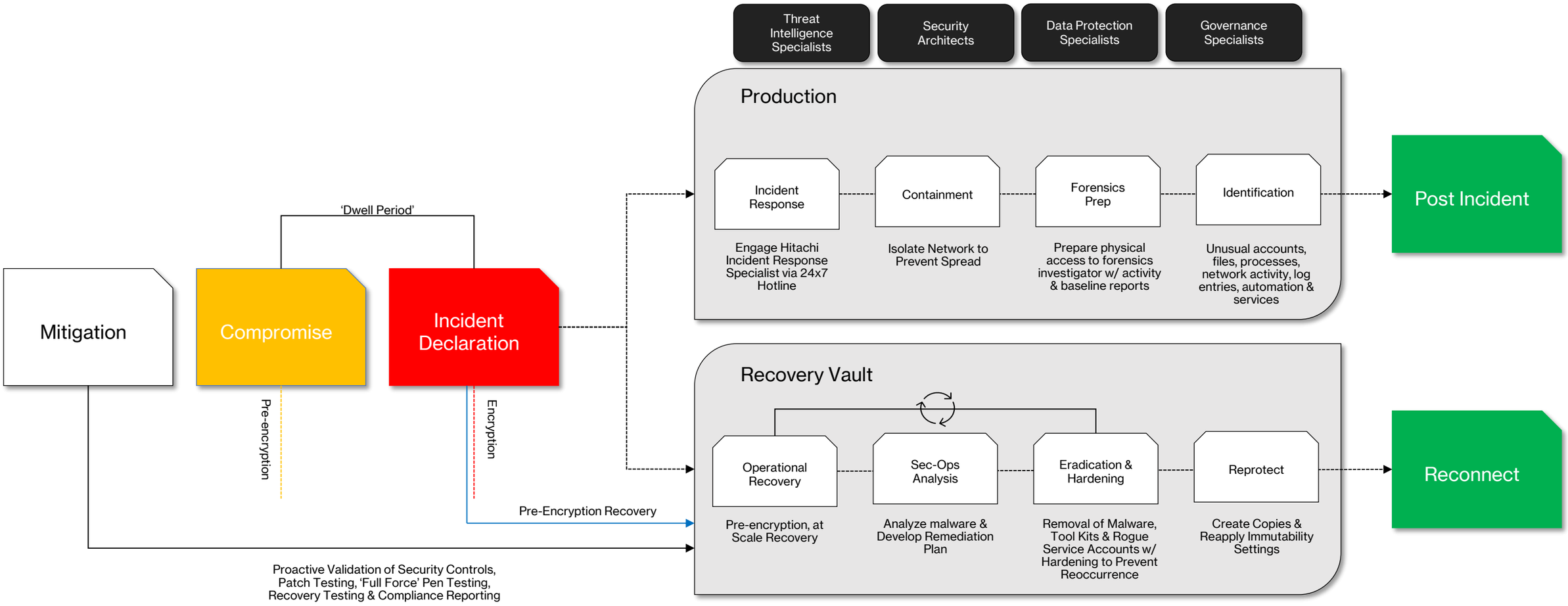
Reliable Recoverability and cyber-resiliency

Data Durability Self-Healing Objects	Rapid recovery at scale	Desktop & mobile clients	Cloud DR
Improve RTO / RPO	Multi-layer AV	VDI file services	100% private option
Integrates With Your Backups	Ransomware protection	SMB/NFS cloud caching	External Key mgt.
Long-term & Short-term Data Retention	Anomaly detection	Multi-site collaboration	DoD certified
Exabyte Scale			
Software-Defined No Vendor Lock-In			
Data In-Place Upgrades			
Ransomware Protection			
Hybrid Tier to Public Cloud			

Defense-in-Depth, A Layered Approach, HV 7-Layers of Data Resilience



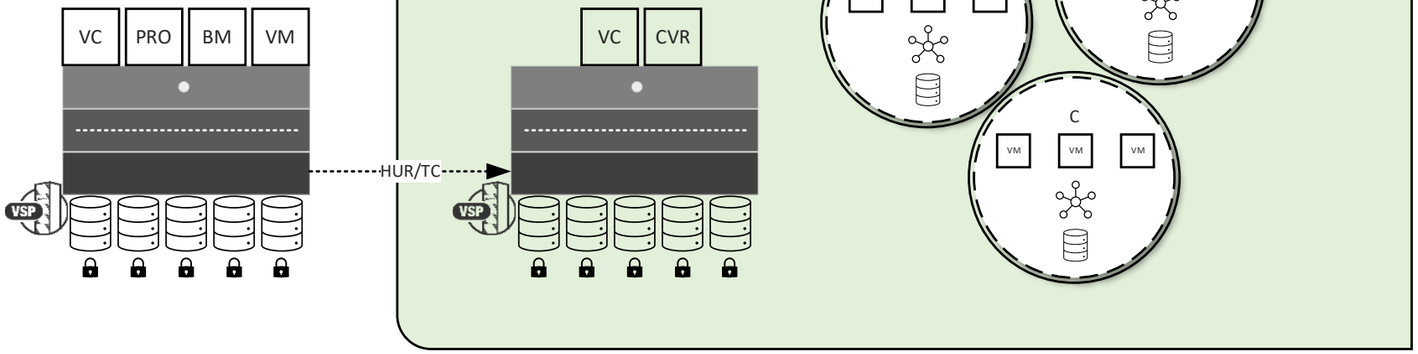
Hitachi Cyber Vault Value



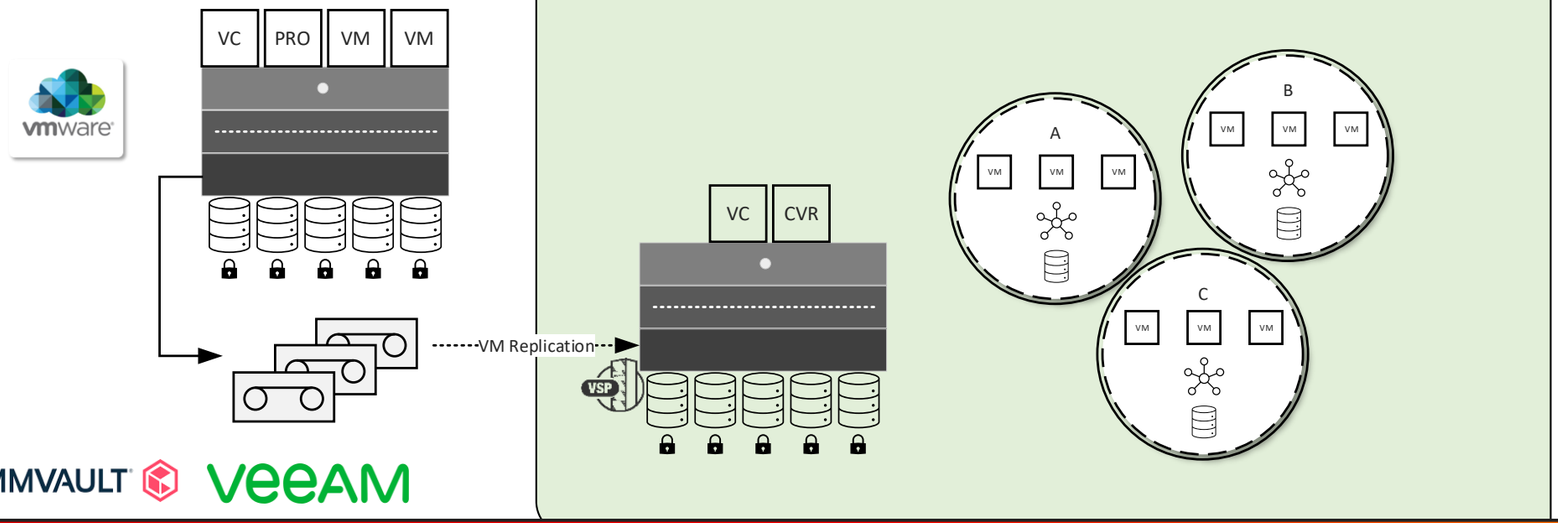
Recovery Vault Options

	Specifications					
	3XS	2XS	XS	SMALL	MEDIUM	LARGE
Storage VSP One Block 20	25TB NVME* 8x32FC ports	50TB NVME* 8x32FC ports	125TB NVME* 8x32FC ports	250TB NVME* 16x32FC ports	500TB NVME* 24x32FC ports	750TB NVME* 32x32FC ports
Compute HA810 G3 DS servers 40c/512GB	0	0	2	4	8	12
CyberVR Automation Software**	50 VMs	75 VMs	125 VMs	250 VMs	500 VMs	750 VMs
Networking Nexus 3524-XL, 48x10Gb	8 SFPs	8 SFPs	8 SFPs	16 SFPs	24 SFPs	32 SFPs
Penetration Testing***	20 IPs	30 IPs	50 IPs	50 IPs	100 IPs	150 IPs
Cyber Incident Response Retainer******	40 hours	40 hours	40 hours	40 hours	80 hours	120 hours

Vault Deployment Options



Provides protection and recovery for various workloads including Hyper-V, KVM, Oracle, SQL and AIX with the advantage of accelerated & predictable recovery of ESX and bare metal x86 servers.



Provides automated & predictable recovery for VMWare ESX machines from ANY storage

VERITAS COMMVAULT VEEAM