

Future Security for Future Networks

Sam Barker

VP, Telecoms Market Research

Juniper Research

MWOC24

Senthil Ramakrishnan

Assistant VP, Product Management & Development, Cybersecurity

AT&T

State of Cybersecurity 2024

Vendor Sprawl	3K+ cybersecurity vendors in US	Increasing Complexity
Alert Fatigue	75+ separate cyber tools managed	Limited Integration
Talent Shortage	3M+ cyber personnel shortfall	Lack of In-House Expertise
Regulation	280+ cyber bills in US	Sprawling Compliance Requirements
Cybercrime	\$1T+ cost of cybercrime	Growth in Malicious Activity

Top Priorities:

-  **Security is #1** concern for Customers
-  Threat landscape is intensifying
-  Cost of cyber breach is **>\$1B in 2023**
-  Security Controls are vastly distributed and complex
-  **43% of attacks target Small Business & Mid Market**

*Source : Gartner 2023 Global Security and Risk Management Survey

Customers and challenges



Cloud-first approach is fueling internet connectivity

As 5G and fiber are growing, your threat surface is also expanding

Digital transformation is top of mind

Need solutions that support growth strategies and the ability to scale quickly



Attacked from all sides*

The cyberthreat landscape is ever-evolving and expanding

Limited resources available to manage and maintain policies and controls

*Gartner 2021 Global Security and Risk Management Survey

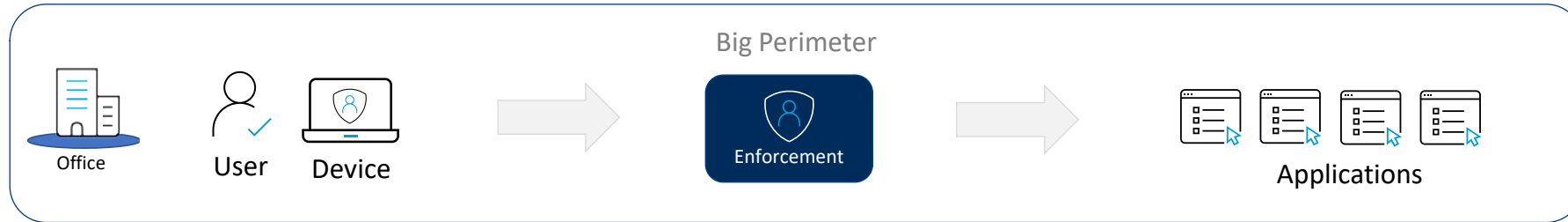


Complexity is a challenge

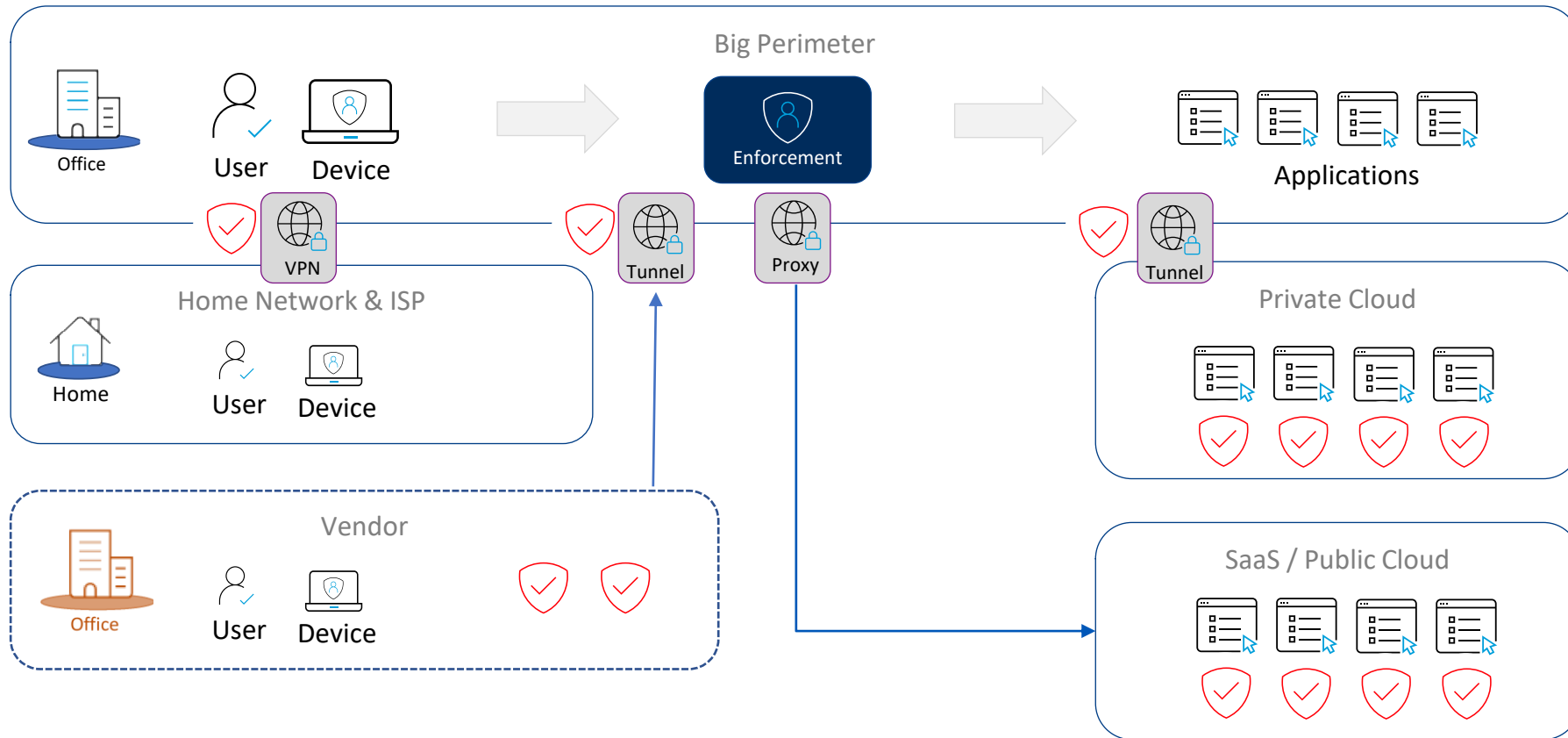
Lack of expertise to manage and maintain multiple security solutions from multiple vendors

Budget constraints make multiple security solutions too costly

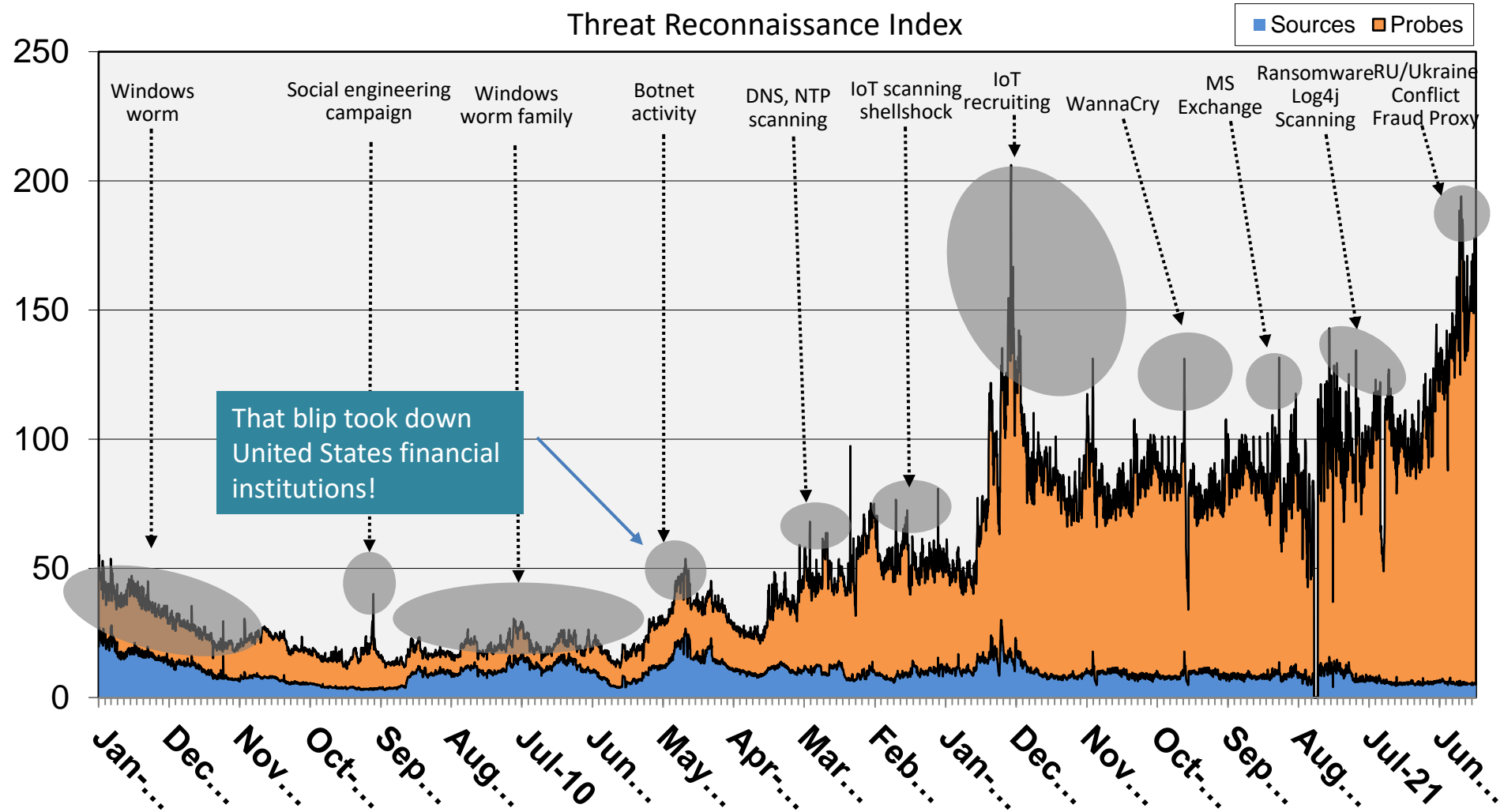
Remember when life was Simple....



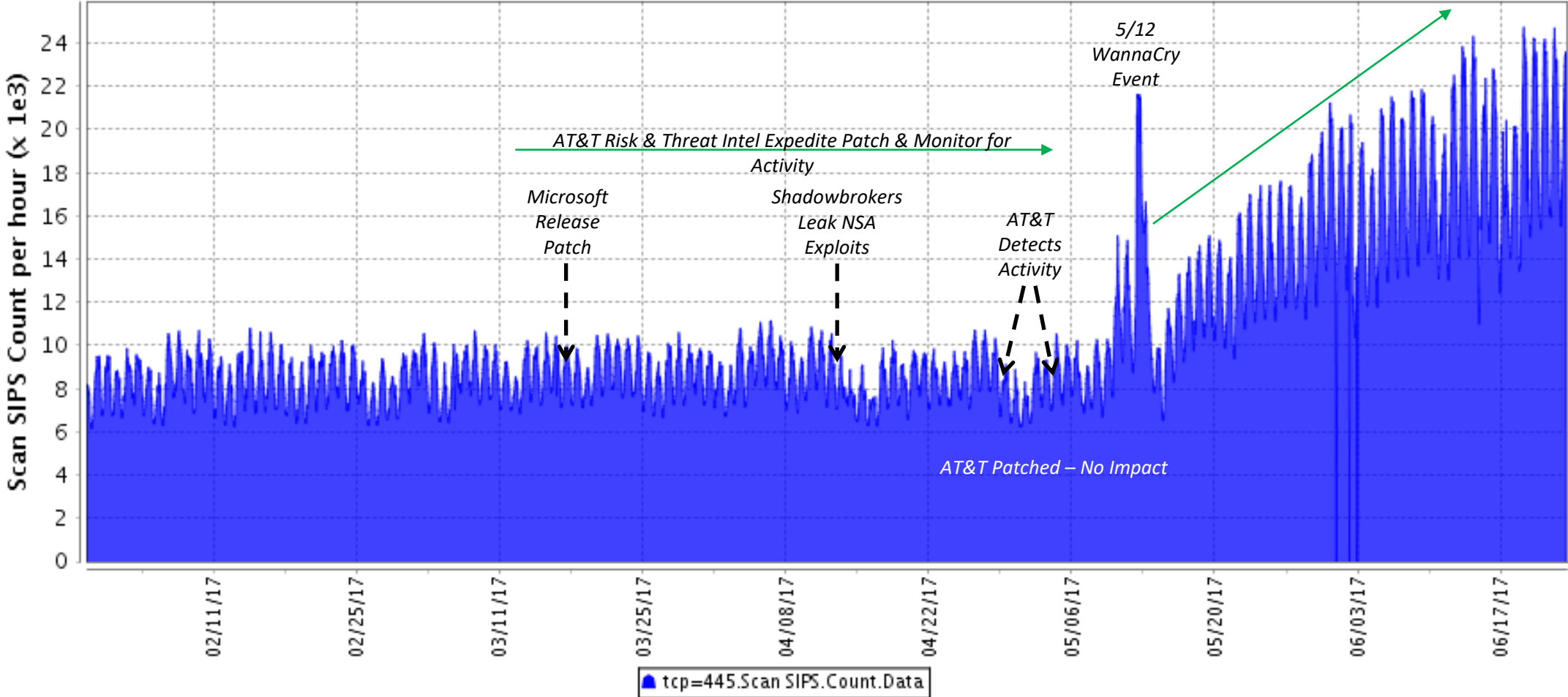
Security Has Become Complex and Hard to Manage



Visibility generates Valuable Insights



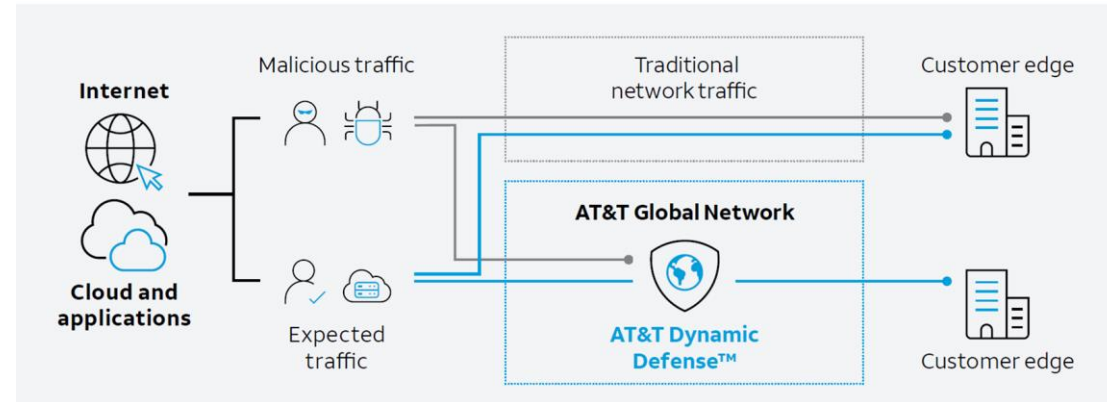
A deeper look at Exploit Activity - WannaCry



What is Network Embedded Security?

AT&T Network Embedded Security

a security platform embedded in AT&T's global network infrastructure that customers can utilize to detect threats, filter traffic, and execute security controls before the data reaches their network.



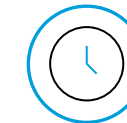
Unprecedented visibility
We see it first



Embedded security controls
Built in, not bolt on, included with AT&T Connectivity



Effortless
Better security at a better value



Near-real time
Same-day deployment in minutes, 24/7/365 network monitoring

Dynamic Defense



Filter



Detects threats BEFORE they reach customer



Defeat Reconnaissance and Initial Access Techniques



Executes security controls to mitigate threats



Impacted MITRE ATT&CK techniques are highlighted

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (2)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Adversary in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal
Gather Victim Host Information (2)	Acquire Infrastructure (2)	Exploit Public-Facing Application	Command and Scripting Interpreter (2)	BITS Jobs	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Application Window Discovery	Internal Spearfishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Accounts (2)	External Remote Services	Container Administration Command	Boot or Logon Suboptimal Execution (2)	Boot or Logon Suboptimal Execution (2)	BITS Jobs	Credentials from Password Storm (2)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Exploitation of Removable Media	Data Encrypted for Impact	Data Encrypted for Impact
Gather Victim Network Information (2)	Compromise Infrastructure (2)	Hardware Additions	Container Administration Command	Boot or Logon Suboptimal Execution (2)	Boot or Logon Suboptimal Execution (2)	Build Image on Host	Debugger Creation	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Data Manipulation (2)	Data Manipulation (2)
Gather Victim Org Information (2)	Develop Capabilities (2)	Flashing (2)	Deploy Container	Boot or Logon Suboptimal Execution (2)	Boot or Logon Suboptimal Execution (2)	Debugger Creation	Exploitation for Credential Access	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Browser Session Hijacking (2)	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Manipulation (2)
Phishing for Information (2)	Establish Accounts (2)	Replication Through Removable Media	Exploitation for Client Execution	Browser Extensions	Browser Extensions	Deobfuscate/Decode File or Information	Forge Web Credentials (2)	Cloud Service Discovery	Remote Service (2)	Clipboard Data	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Search Closed Sources (2)	Obtain Credentials (2)	Supply Chain Compromise (2)	Inter-Process Communication (2)	Compromise Client Software Binary	Create or Modify System Process (2)	Direct Volume Access	Forge Web Credentials (2)	Cloud Storage Object Discovery	Remote Service (2)	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (2)	Endpoint Denial of Service (2)
Search Open Technical Databases (2)	Stage Capabilities (2)	Trusted Relationship	Native API	Create Account (2)	Domain Policy Modification (2)	Direct Volume Access	Host Capture (2)	Container and Resource Discovery	Replication Through Removable Media	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Other Network Medium (2)	Fireware Compromise
Search Open Websites/Domains (2)	Valid Accounts (2)	Scheduled Task/JOB (2)	Scheduled Task/JOB (2)	Create or Modify System Process (2)	Domain Policy Modification (2)	Escape to Host	Modify Authentication Process (2)	Device Driver Discovery	Application Windows Discovery	Data from Configuration Repository (2)	Feedback Channels	Exfiltration Over Physical Medium (2)	Inhibit System Recovery
Search Victim-Owned Websites	Serverless Execution	Shared Modules	Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery	File and Directory Discovery	Data from Information Repositories (2)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
	System Services (2)	User Execution (2)	Windows Management Instrumentation	System Services (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)	Request Generation	File and Directory Discovery	File and Directory Discovery	Data from Local System	Non-Standard Port	Scheduled Transfer	Resource Hijacking
	Windows Management Instrumentation	Modify Authentication Process (2)	Valid Accounts (2)	Modify Authentication Process (2)	Scheduled Task/JOB (2)	Scheduled Task/JOB (2)	Indicator Removal (2)	Group Policy Discovery	Group Policy Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot

MWOC24

Louis Lou

Executive Assistant Director, Global Cyber Security & Privacy

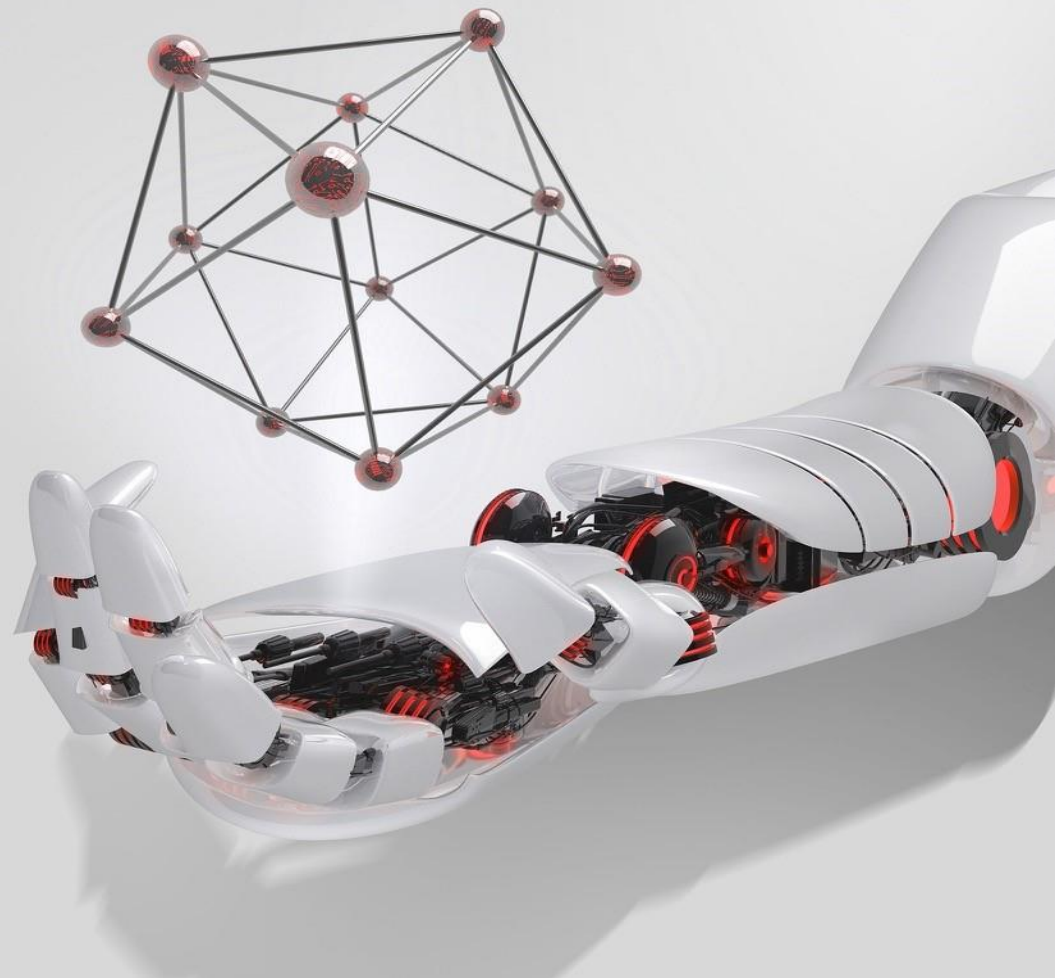
Huawei

FUTURE SECURITY

FOR FUTURE NETWORKS

Louis Lou

Executive Assistant Director for Global Cyber Security & Privacy



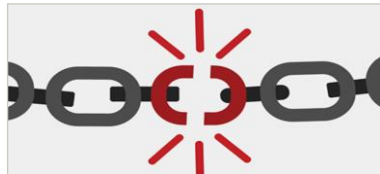
Future Security Challenges | More Cyber Attacks and EDTs bring new challenges

Cyber Attacks



Ransomware Attack

Ransom attacks occur every 11 seconds
It can cause losses of billions of dollars to enterprises.



Supply chain attacks

45% of organizations worldwide have experienced one or more software supply chain attacks



DDoS attack

More than 10 million DDoS attacks per year
398 million RPS attack



Data breach

The average cost of a data breach is up to \$4+ million.

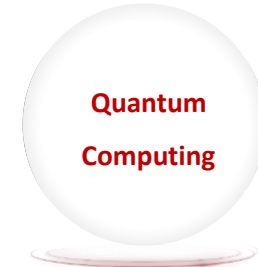
According to Cybersecurity Ventures, the global economy is expected to lose up to \$10.5 trillion by the end of 2024.

Emergent Disruptive Technologies (EDTs)



AI/Large Model

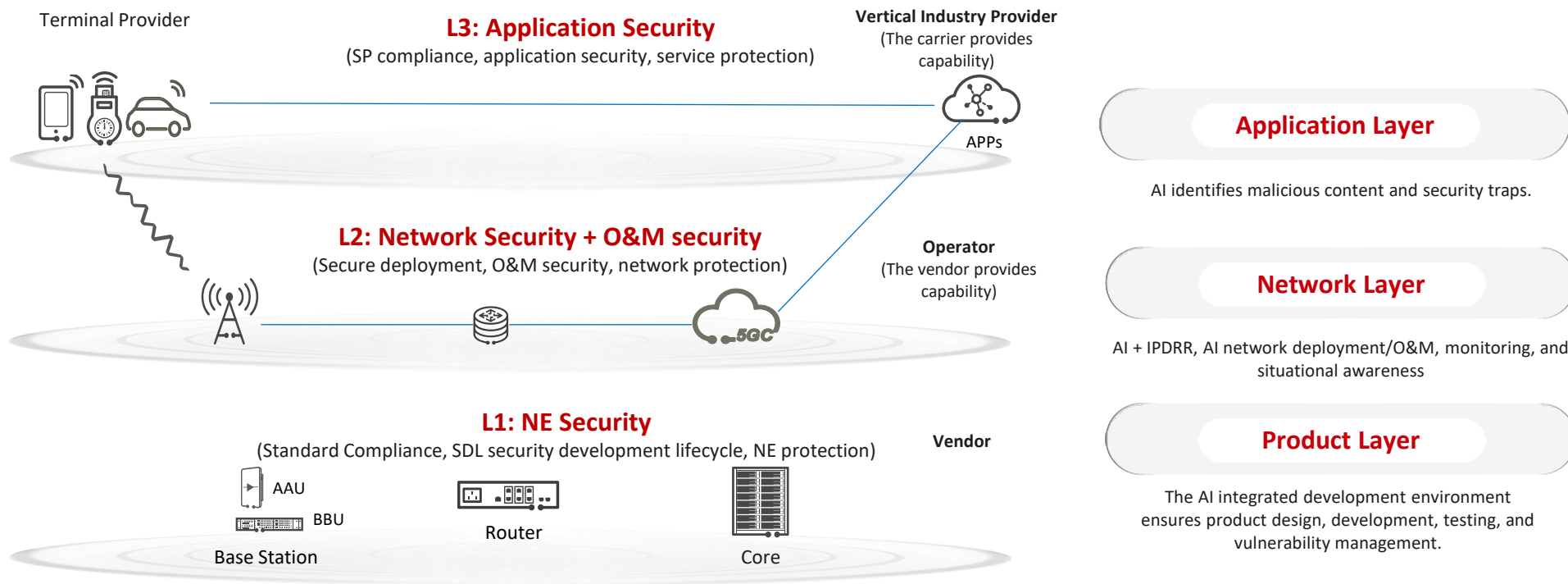
AI Security
AI for Attack (Attacker)
AI for Security



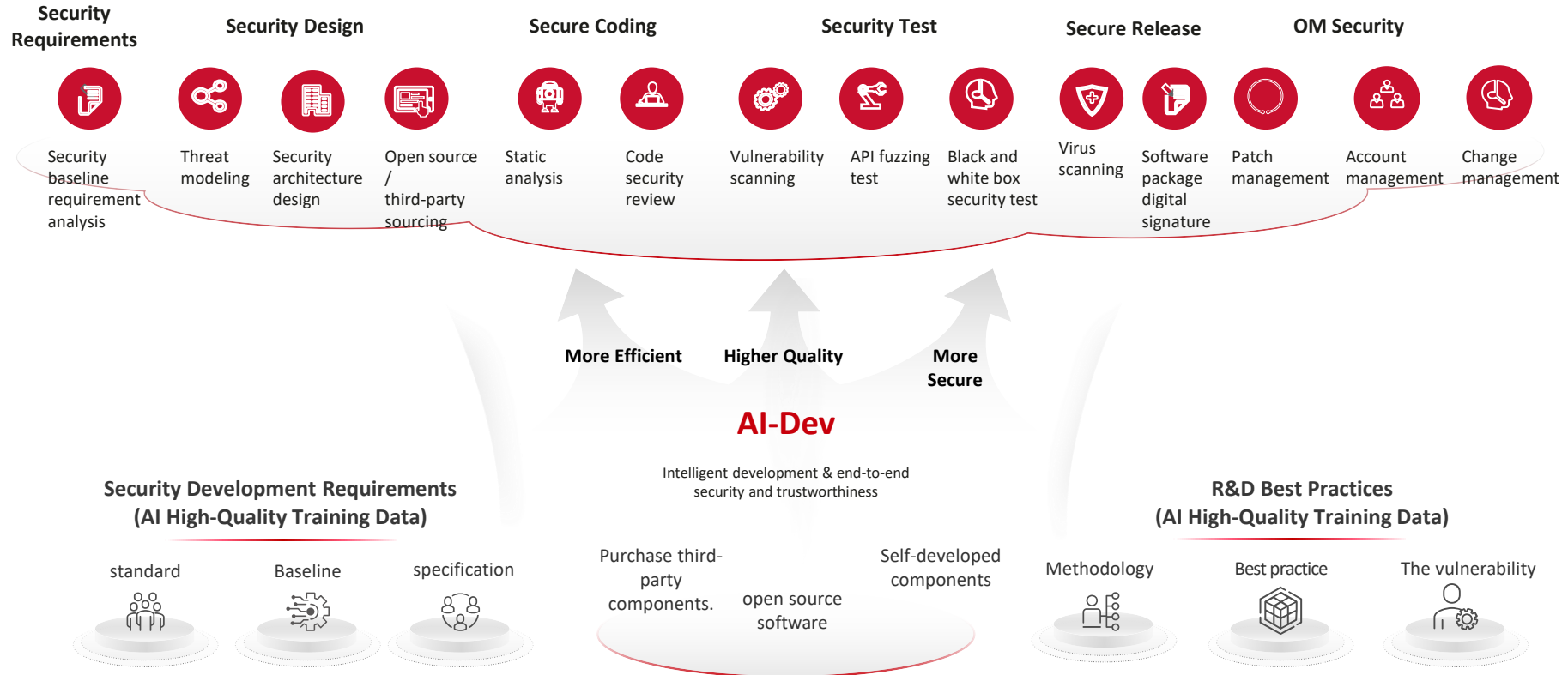
Quantum Computing

Quantum computing breaks asymmetric cryptosystems and subverts existing cryptosystems.

Future Security Technologies and Applications | AI integrated development environment, AI network O&M, and AI malicious content identification

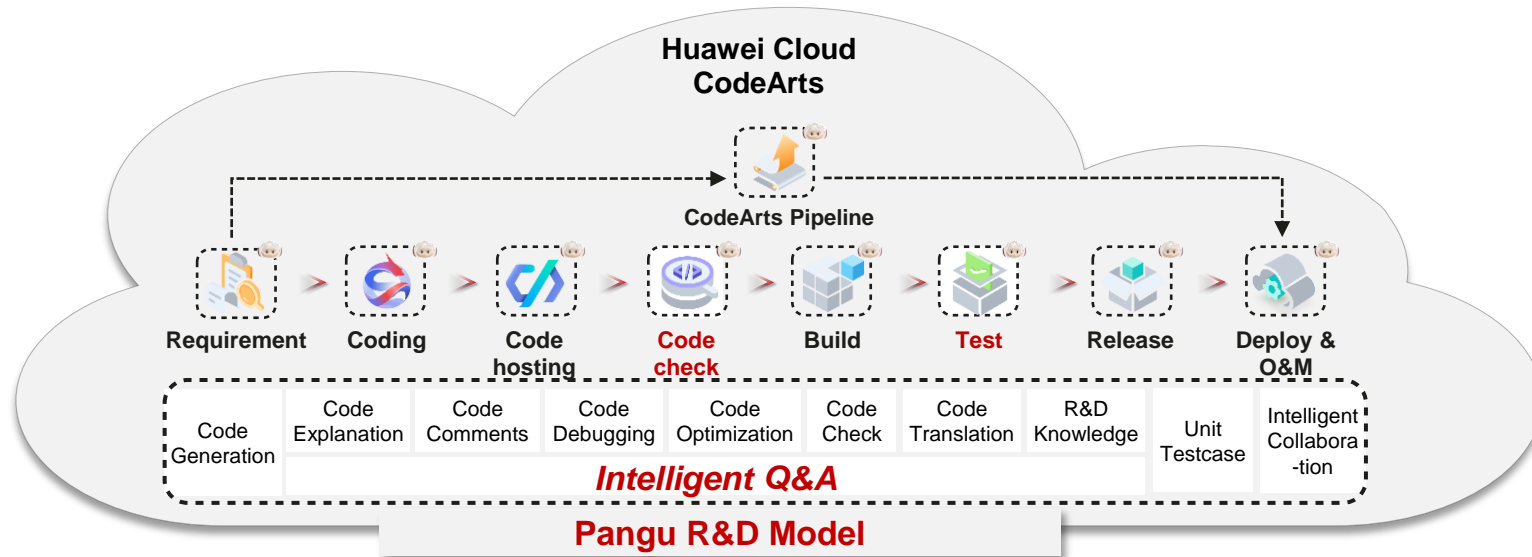


AI-enabled Product Development | AI-DEV Integrates the Tool Chain to Ensure Product Design, Development, Testing and Vulnerability Management, Helping Suppliers Develop More Secure Products



AI-DEV | CodeArts Absorbed Huawei R&D Engineering/Tool Capabilities, and is Offered to Business Customers to Improve their Product Quality and Development Productivity

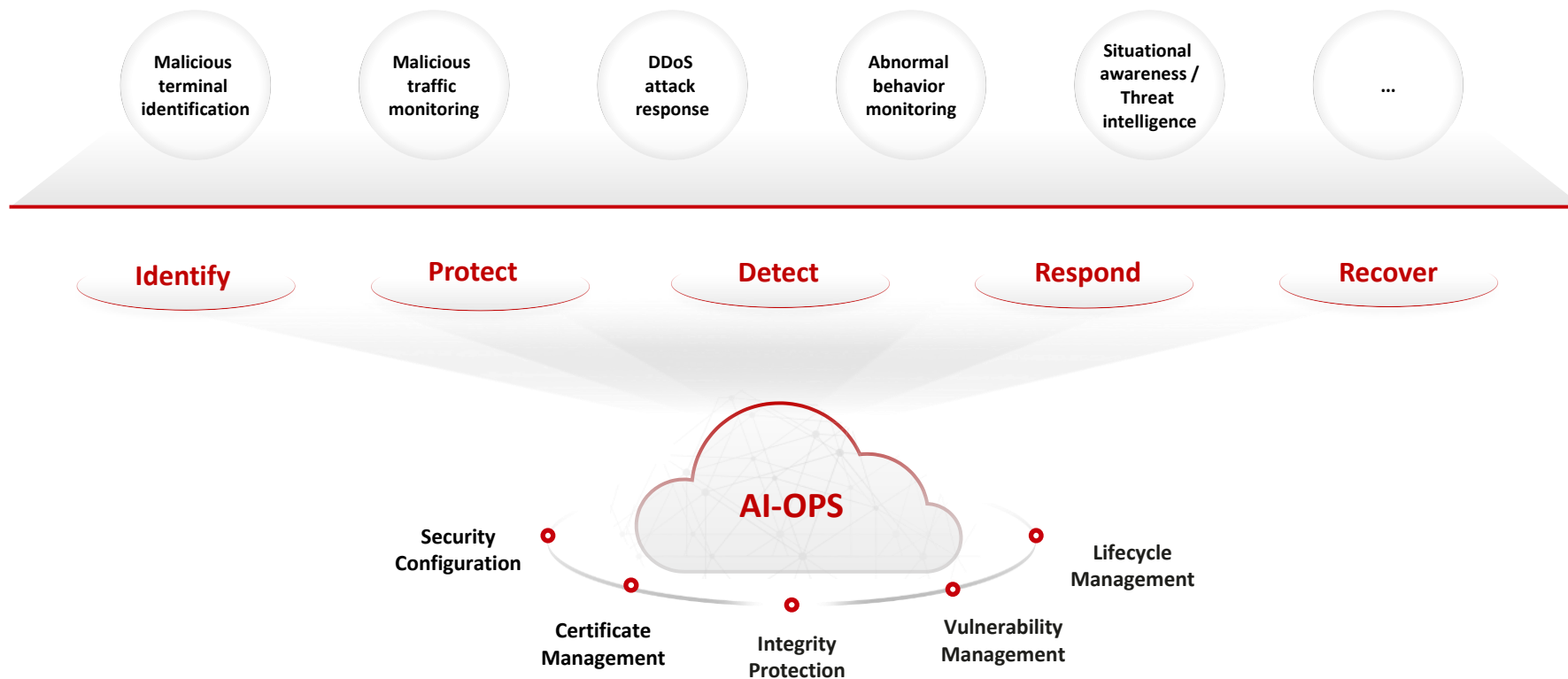
Case 1: Security Development and Test Assistant



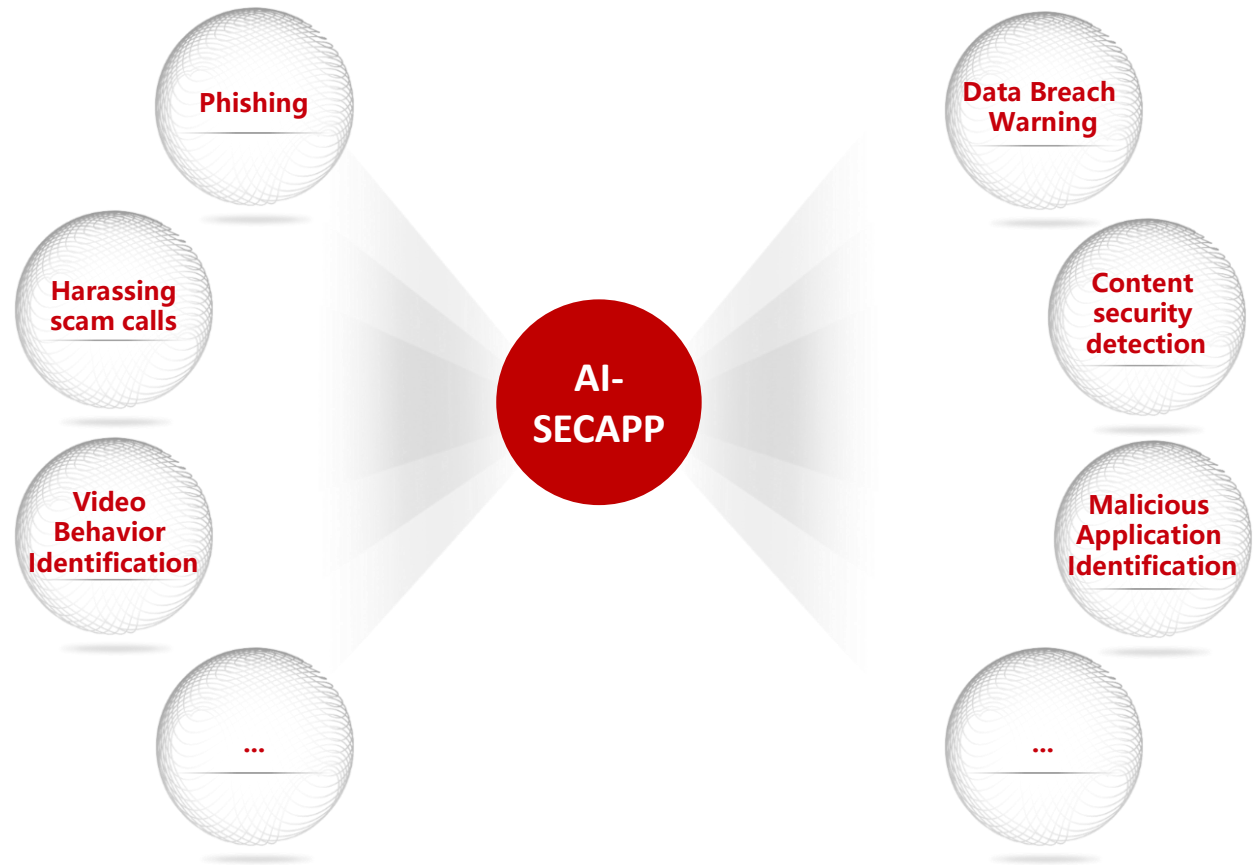
AI assisted software development

- Enabled by Pangu R&D Model, supports mainstream IDEs and programming languages
- **Automatic generation** of code/test cases/test scripts, **efficiency increased by 20%+**
- **Intelligent Q&A & Collaboration**, one-stop application deployment

AI-based Network Deployment and O&M | AI-OPS Helps Enterprises Deploy and Operate Resilient Networks

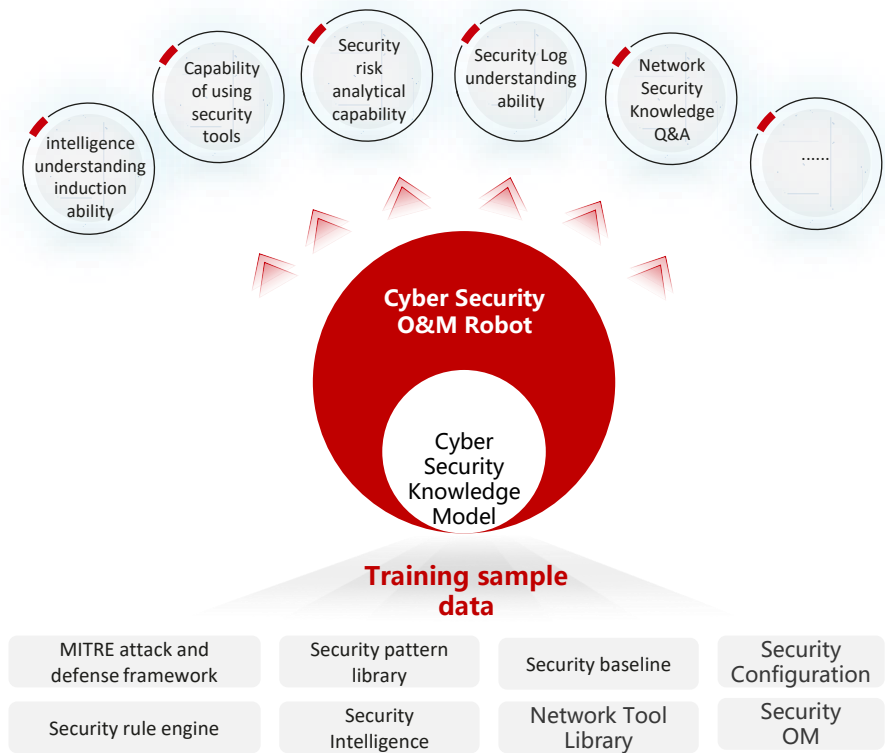


AI application security | AI Identifies Malicious Content and Security Traps, Helping Users Identify Phishing Emails and Internet Fraud

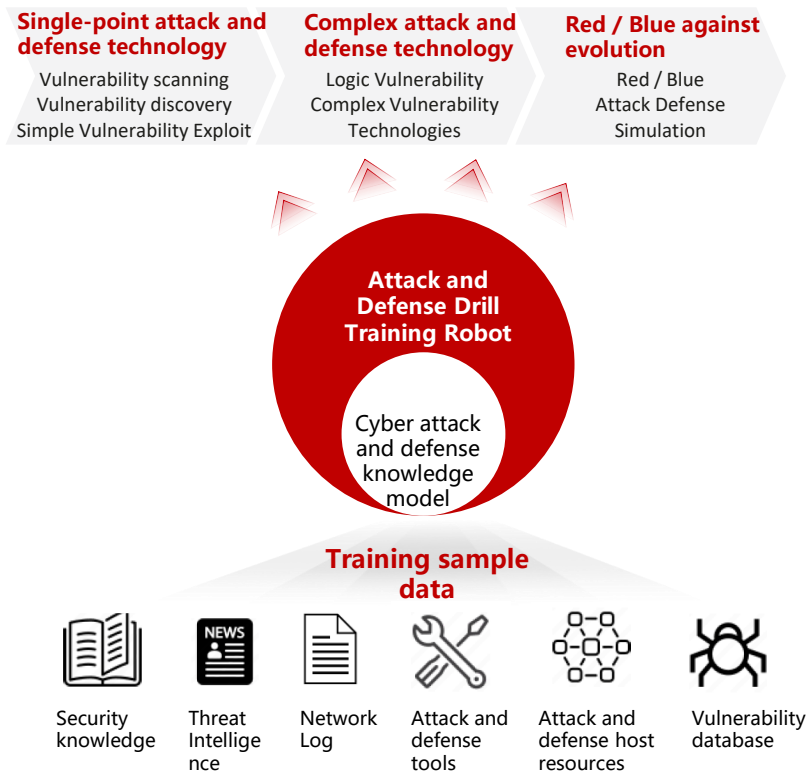


AI for Security Case Study

Case 2: Network Security O&M Robot



Case 3: Attack-defense Drill Training Robot

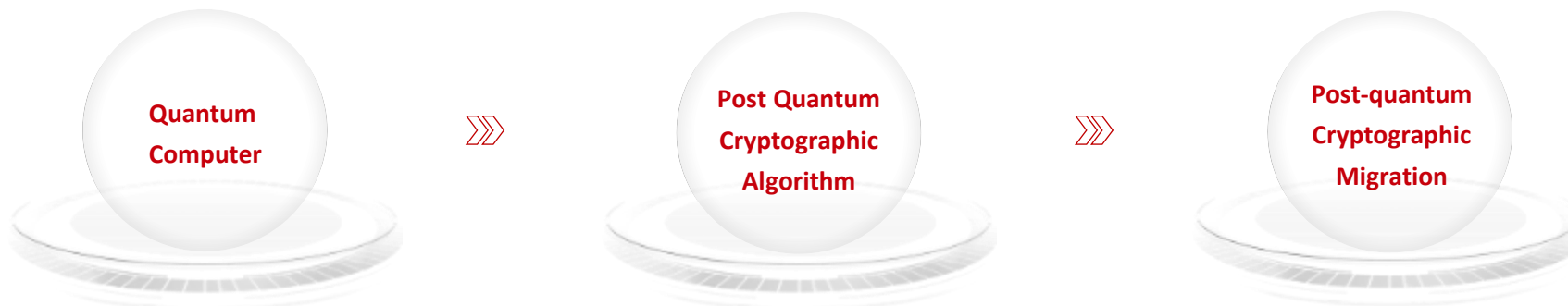


AI for Capability Improvement | AI Experts and Human Experts Improve Each Other's Capabilities



AI experts and human experts learn from each other and improve each other. Human experts train better domain expert models, and AI experts help human knowledge learning and capability improvement.

Post-quantum Cryptographic Algorithm & Migration | Building a Trust Foundation for the Digital World in The Post-quantum Era



Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and
organization for a fully connected,
intelligent world.

**Copyright©2018 Huawei Technologies Co., Ltd.
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



MWOC24

Moderator: Sam Barker

Juniper Research

Mikko Karikytö

Ericsson

Dr Galina Pildush

Palo Alto Networks

Nagendra Bykampadi

Rakuten Symphony

MWOC24