IBM Security

Security Trends & Direction

Fearless in the face of uncertainty

Michel Bobillier
Program Director
Worldwide Security Solutions

March 2019

IBM

AGENDA

1. Some Facts
2. The Dark Side at Work
3. Now… and Then

Where we are now

- Largest enterprise cybersecurity provider
- Leader in 12 security market segments
- 8,000+ security employees
- 20+ security acquisitions
- 70B+ security events monitored per day

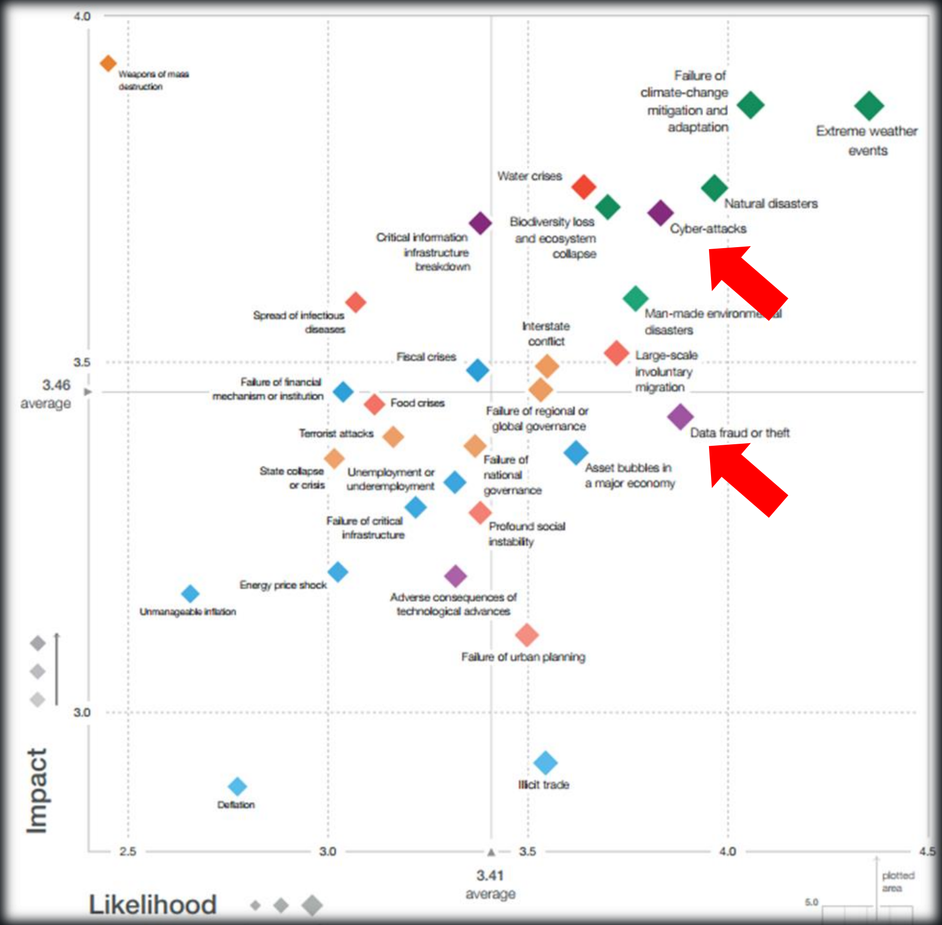
Are we safe ?

- 2018 Nov. : 500M Marriott client records stolen incl. phone, mail, passport #, credit card #
- 2018 Sept. : 380K British Airway client records stolen including credit card (with CCV)
- 2018 Aug. : 2M T-Mobile client records incl. personal data and passwords
- 2018 July : 1.5M Singapore Health System medical records compromised in attack
- 2018 March : 9.4M Cathay Pacific client records incl. passeport # and credit cart #
- 2018 March: 1.1B Aadhar (Indian Gvt portal) users data breach incl ID card # and bank accounts

- 2017: 145M Equifax full user accounts
- 2017 : elections influenced by foreigners' hack
- 2017 : 50M Facebook accounts

- 2016: 3B Yahoo user accounts (sale to Verizon cut by $350m in 2017)

World Economic Forum (WEF) Global Risk Landscape 2019



Cybersecurity is a universal challenge

What's at stake...

20.8 billion
things we need
to secure

5 billion
personal data
records stolen

$6 trillion
lost to cybercrime
over the next 2 years

What we face...

Compliance updates

GDPR fines can cost
billions
for large global
companies

Skills shortage

By 2022, CISOs will face
1.8 million
unfulfilled
cybersecurity jobs

Too many tools

Organizations are using
too many
tools from too
many vendors

AGENDA

1. Some Facts ?
2. The Dark Side at Work
3. Now… and Then

The Dark Side at work – Standard Bank ATM cash withdrawal

- What
  - 1.8 billion yen ($13M) ATM withdrawal

- How
  - Counterfeit credit cards from Standard Bank (South Africa)
  - 100 people, 14’000 transactions at 1’400 Seven Eleven ATMs
  - Under 3 hours on a Sunday morning in Japan.

- Probable Standard Bank system in South Africa hacked prior to actual attack
- Loss fully absorbed by the bank

The Dark Side at work – Bangladesh Central Bank

- What
  - Feb. 2016: fraudulent SWIFT transfers for $951M
    - $20M to Sri Lanka (recovered)
    - $81M to Philippines ($18M recovered)
    - $850M blocked due to typo in client name (f$_o$undation)

- How
  - Compromised bank network
  - Silent observation of transfer procedure
  - Access to bank transfer SWIFT credentials
  - Acted a Friday when bank was closed

- Bank unsure about hack even after facts
- 2013: similar unresolved $250K hack at Sonali Bank
- Bank’s governor resigned, executives fired

The Dark Side at work? -- Research on Chrysler Jeep

- Objective
  - Unaltered car
  - Remote attack with no physical interaction

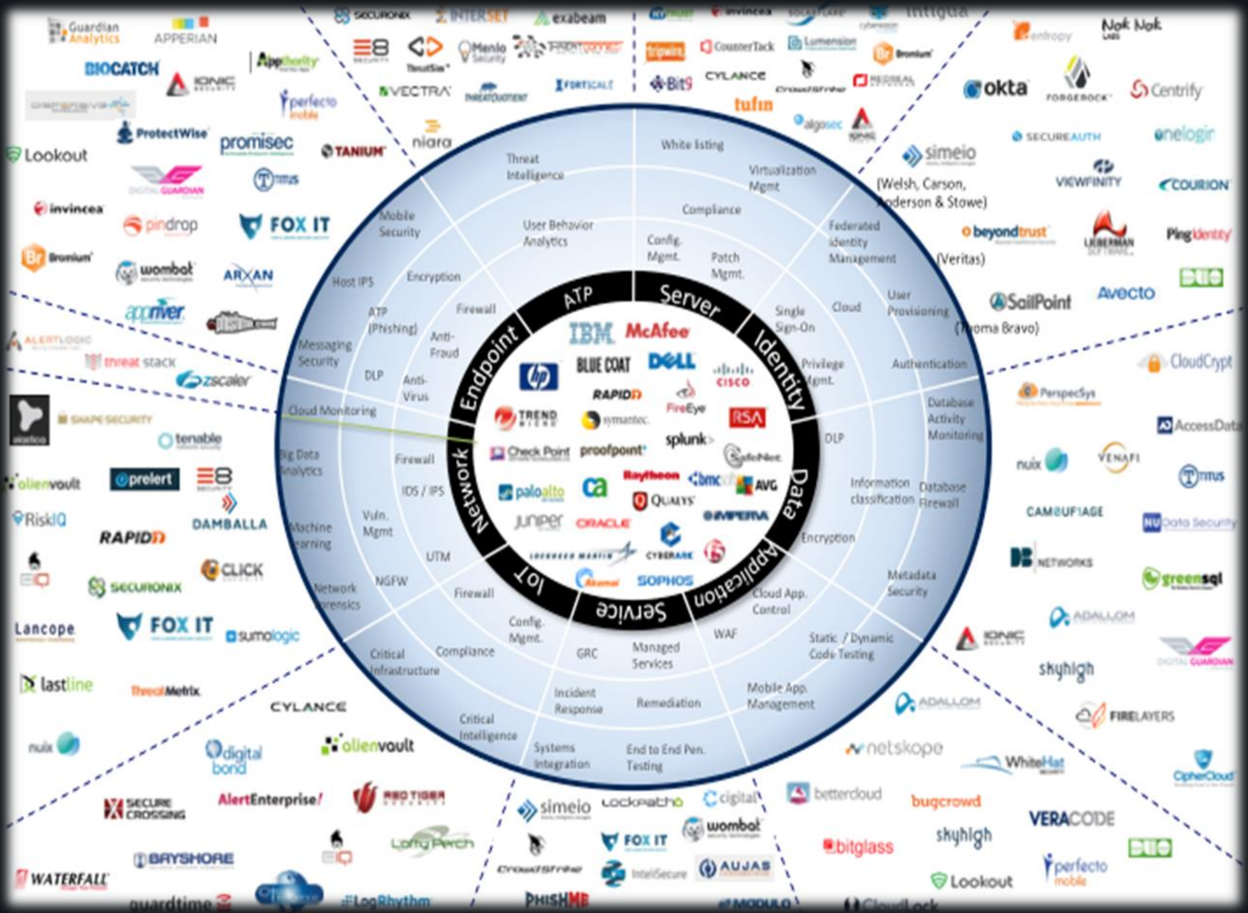
- Results
  - Entered via wireless system
  - Control steering, disable brakes

- 1.4 million vehicles recall
- Cost to design securely vs recall ?
- Wide attack surface
  - Bluetooth, Wifi, radio, remote key system, tire pressure monitoring system, …

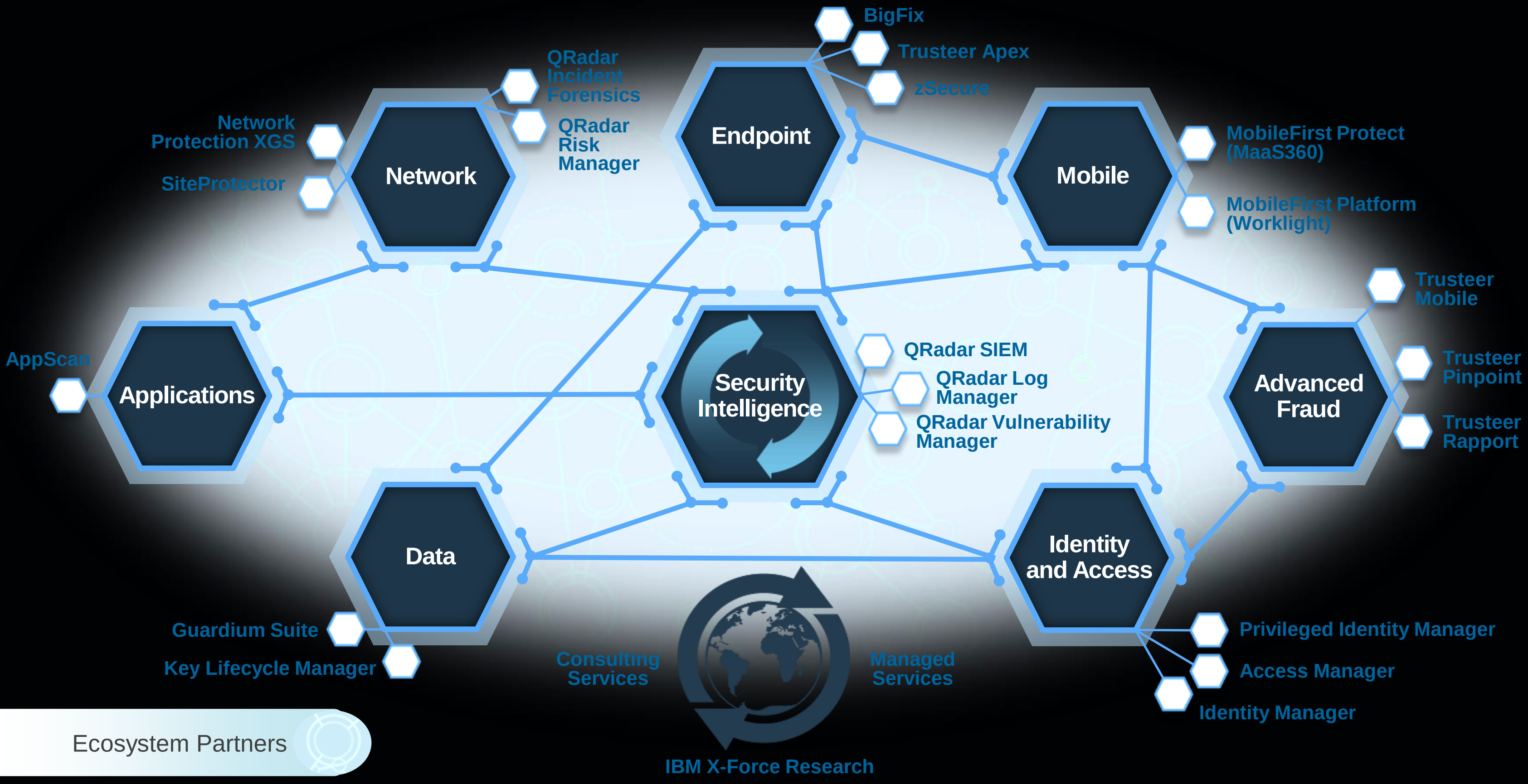
AGENDA

1. Some Facts ?
2. The Dark Side at Work
3. Now… and Then

We act in a noisy, fragmented market of 1’200+ companies

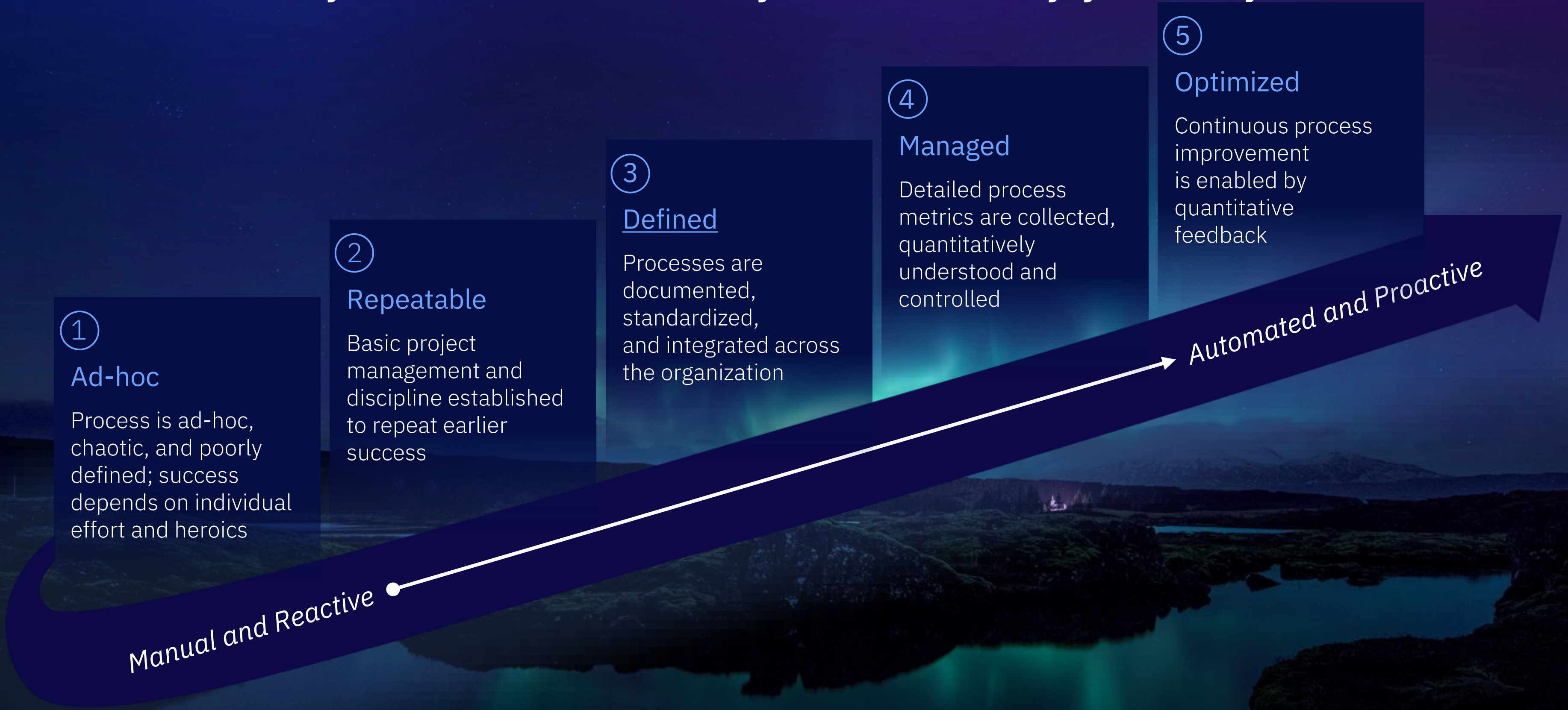


Think about Security as an Immune System



Ecosystem Partners

Define where you want to be in your security journey



1 Ad-hoc

Process is ad-hoc, chaotic, and poorly defined; success depends on individual effort and heroics

2 Repeatable

Basic project management and discipline established to repeat earlier success

3 Defined

Processes are documented, standardized, and integrated across the organization

4 Managed

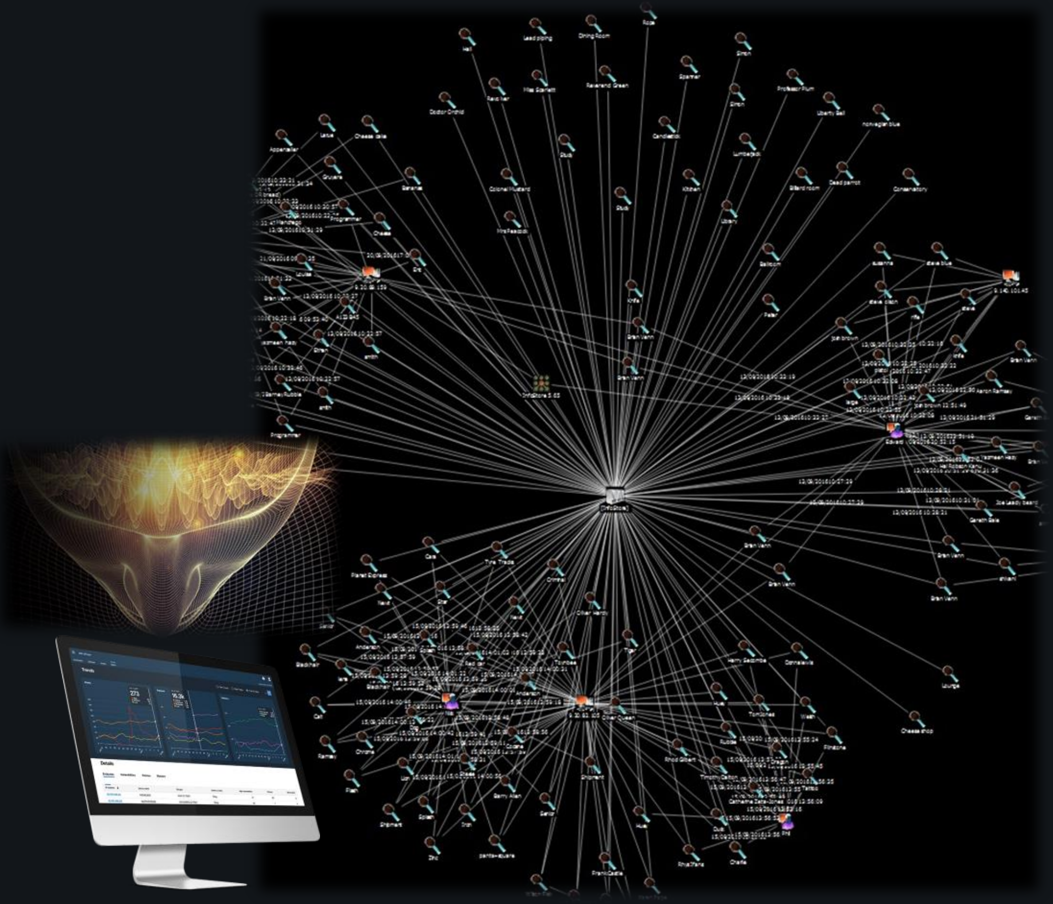
Detailed process metrics are collected, quantitatively understood and controlled

5 Optimized

Continuous process improvement is enabled by quantitative feedback

Speed up your Security Operation Center (SOC) with AI

Security Fusion Center
Cyber Security Command Center
Situational Awareness



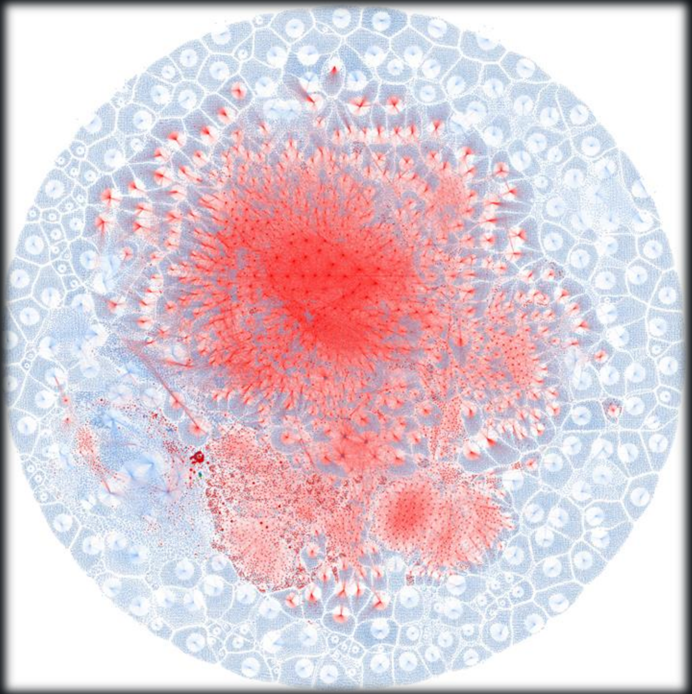
The corpus of Watson for Cyber Security in action

Continually growing and adapting through the absorption of new security knowledge

Performs cognitive exploration of suspicious activities and behaviors identifying root cause and additional indicators

Creates and finds paths and linkages easily missed by humans

Learns, adapts and doesn’t forget



- **70B security events/day**
- **1M+ IP addresses**
- **270M+ end points**
- **800TB+ of threat intel.**
- **10B elements (+4M/ hour)**
- **1.25M docs (+15K/ day)**

Happy to help to your next steps

Save

X-Force IRIS’s number
1-888-241-9812

Schedule

a consultation with
our security experts

Sign-up

for IBM X-Force Exchange
exchange.xforce.ibmcloud.com

Visit

the X-Force Cyber Range
bit.ly/X-ForceCommand

BACKUP

What we’re hearing from customers

From thousands of engagements across the world, we’ve heard some common security concerns.

Help me...

Modernize security frameworks and controls

Respond to the global security skills shortage

Address increasing cyber attack vectors including IoT

Secure the journey to cloud and digital transformation

Maintain data privacy and regulatory compliance

IBM Security can help transform your security program

Strategy and Risk

Unify business leaders with security risk management

Threat Management

Identify and respond to threats with speed and confidence

Digital Trust

Govern and protect your business, data, users and assets

IBM Security can help transform your security program

Strategy and Risk

Get Ahead of Risk and Compliance

- Strategy and Planning
- Risk Assessments
- Advisory Services

Build Leadership and Culture

- X-Force Cyber Range
- X-Force Comes to You
- X-Force Cyber Tactical Operations Center

Threat Management

Detect and Stop Advanced Threats

- Security Operations Consulting
- X-Force Threat Mgmt. Services
- X-Force Red
- QRadar
- X-Force Detect

Orchestrate Incident Response

- Resilient
- X-Force IRIS

Master Threat Hunting

- i2 Intelligence Analysis
- QRadar Advisor with Watson

Digital Trust

Protect Critical Assets

- SDLC Consulting
- Data Protection Services
- AppScan
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

Govern Users and Identities

- Identity Mgmt. Services
- Identity Governance
- Cloud Identity
- Access Manager
- Secret Server

Deliver Digital Identity Trust

- Trusteer
- Cloud Identity

Secure Hybrid Cloud

- Infrastructure and Endpoint Services
- Hybrid Cloud Security Services
- QRadar Cloud Analytics
- Cloud Identity
- Guardium for Cloud

Unify Endpoint Management

- Endpoint Mgmt. Services
- MaaS360
- BigFix

We realize every client is on a security journey

What clients tell us they need

Guidance & Wisdom

Tools & Resources

Clarity & Action

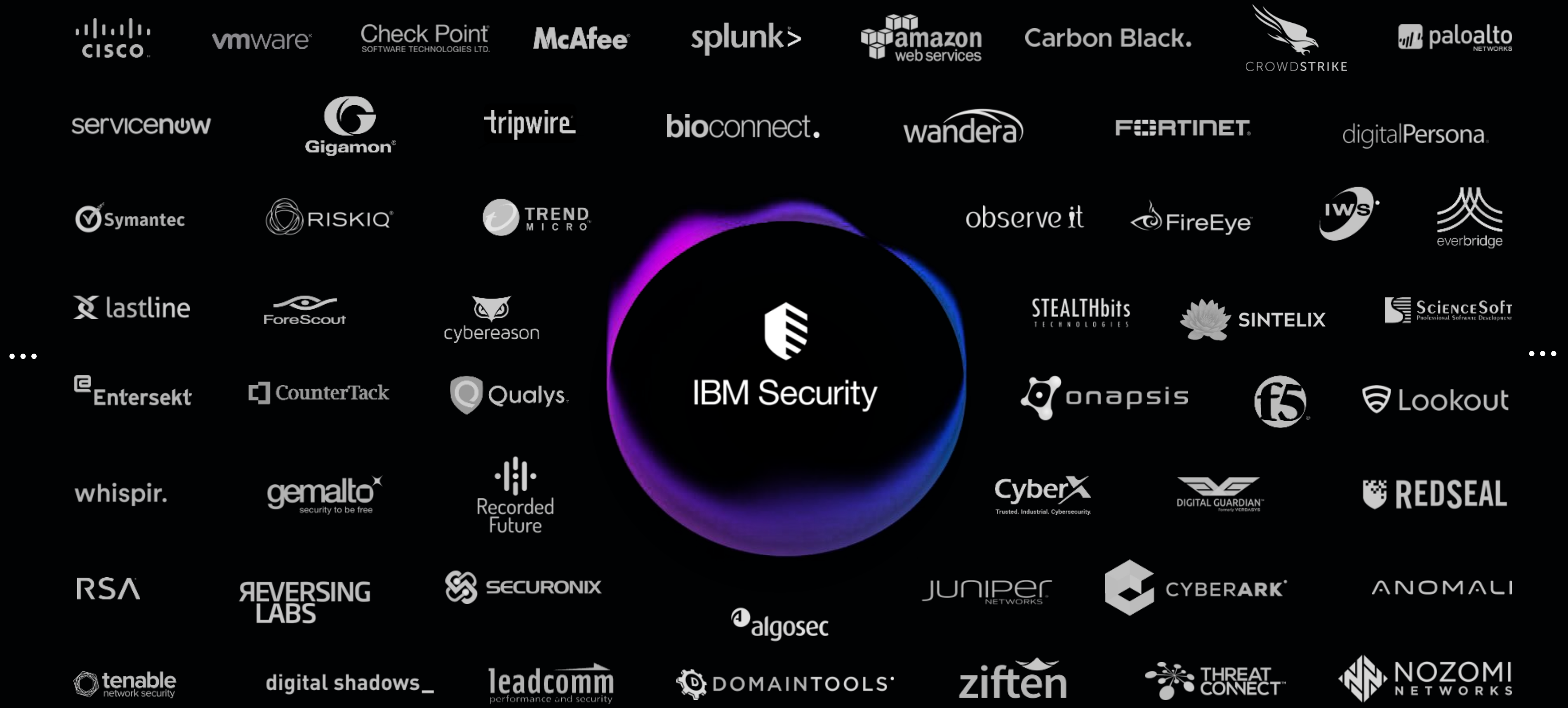
IBM Security uniquely delivers

Global visibility and industry expertise

Integrated products and services

Leading analytics, AI and orchestration

Supported by hundreds of open integrations


cisco
vmware
Check Point SOFTWARE TECHNOLOGIES LTD.
McAfee
splunk>
amazon web services
Carbon Black.
CROWDSTRIKE
paloalto NETWORKS
servicenow
Gigamon
tripwire
bioconnect.
wandera
FORTINET
digitalPersona
Symantec
RISKIQ
TREND MICRO
observe it
FireEye
IWS
everbridge
lastline
ForeScout
cybereason
IBM Security
STEALTHbits TECHNOLOGIES
SINTELIX
ScienceSoft Professional Software Development
...
...
Entersekt
CounterTack
Qualys.
onapsis
f5
Lookout
whispir.
gemalto security to be free
Recorded Future
CyberX Trusted. Industrial. Cybersecurity.
DIGITAL GUARDIAN formerly VERDASYS
REDSEAL
RSA
REVERSING LABS
SECURONIX
algosec
JUNIPER NETWORKS
CYBERARK
ANOMALI
tenable network security
digital shadows_
leadcomm performance and security
DOMAINTOOLS
ziften
THREAT CONNECT
NOZOMI NETWORKS