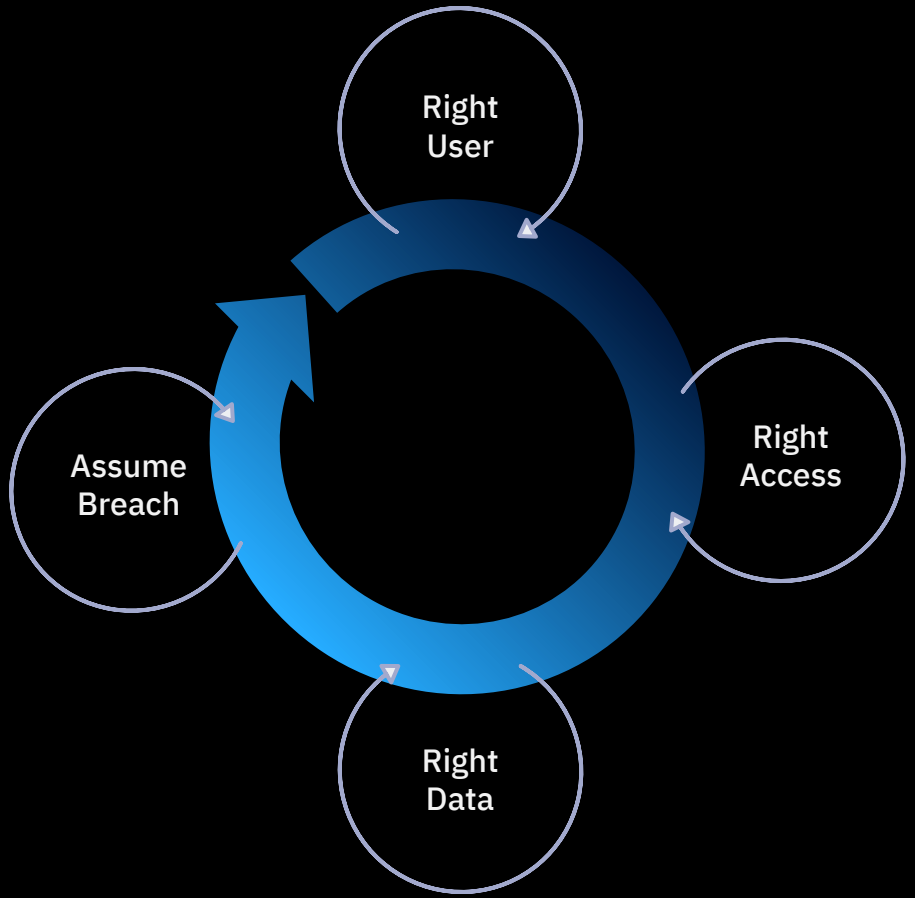
Adopting Zero Trust
A Deeper Dive

Alden Hutchison
Partner, IBM Security
ahutchison@us.ibm.com

LinkedIn Profile

Zero Trust concept



These are the top use cases our clients are focused on

Reduce the risk of business disruption and ransomware

Insulate business from ransomware
Enforce least privilege access
Discover risky user behavior

Protect the hybrid cloud

Manage and control all accesses
Monitor cloud activity and configurations
Secure cloud native workload

Preserve customer privacy

Simplify and secure user onboarding
Manage user preferences and consent
Enforce privacy regulation controls

Secure the hybrid workforce

Secure BYO and unmanaged devices
Eliminate VPNs
Provide passwordless experiences

Reduce the risk of insider threat

Enforce least privilege access
Discover risky user behavior
Embed threat intelligence

Cyberattacks are a top cause of business disruption, with ransomware leading the way

$1.59M

portion of data breach costs attributable to lost business (38%), including business disruption, system downtime, lost customers and reputation losses.[1]

23%

of all security attacks in 2020 were the result of ransomware, up 15% from 2019.[2]

20%

Share of breaches initially caused by compromised credentials, the most common initial attack vector.[1]

Double Extortion:

Occurs about 60 percent of the time attackers couple ransomware with stealing data

Ransomware pays:

We estimate Revil alone earned $120m, trending to a billion-dollar business

Shift to Ransomware-as-a-Service:

Affiliate or franchise operations, enables multiple infection vectors using the same ransomware

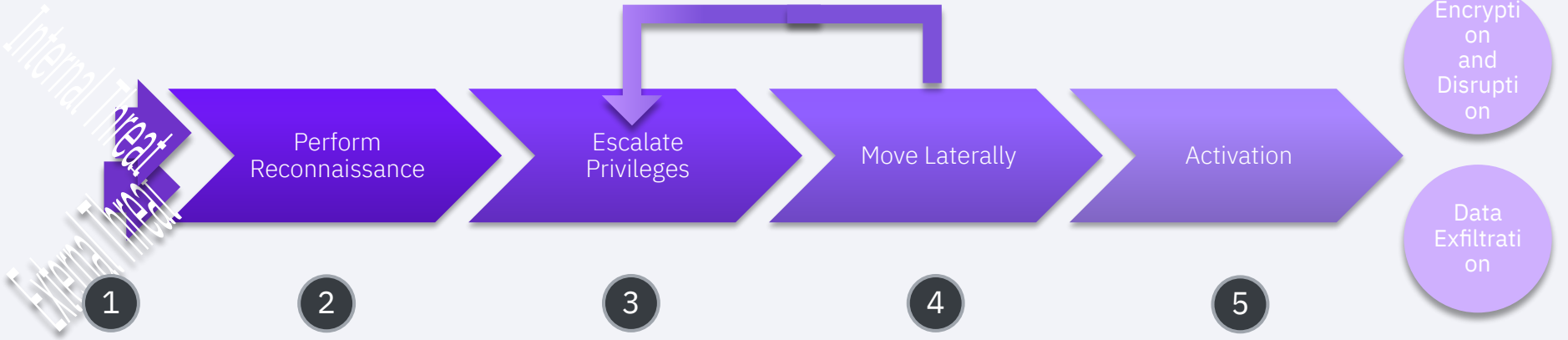
Incidents are taking longer to remediate:

Trending to 400+ hours in 2021

Ransomware is an organized cybercrime activity that is on the rise and continuing to evolve

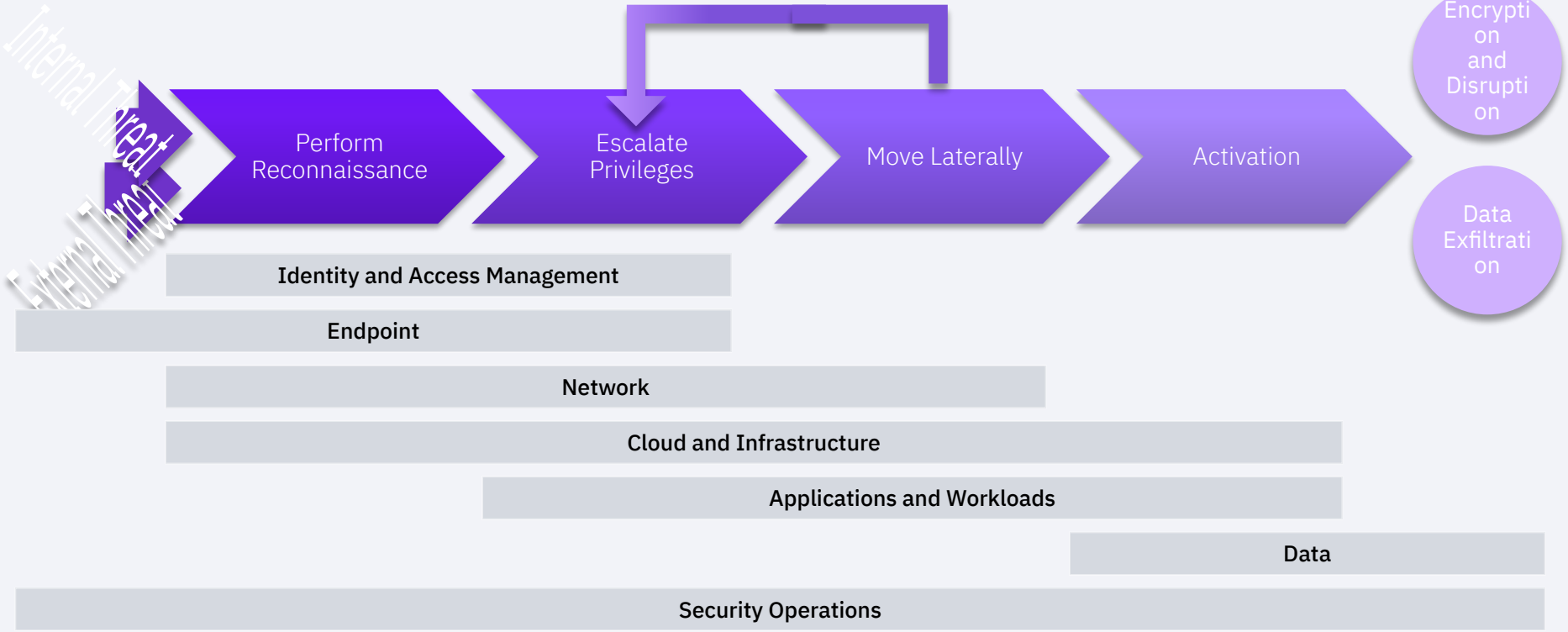
[1] IBM Security Cost of a Data Breach Report 2021
[2] IBM Security X-Force Threat Intelligence Index 2021

Understanding the attack chain is critical for preparation, protection, and prevention

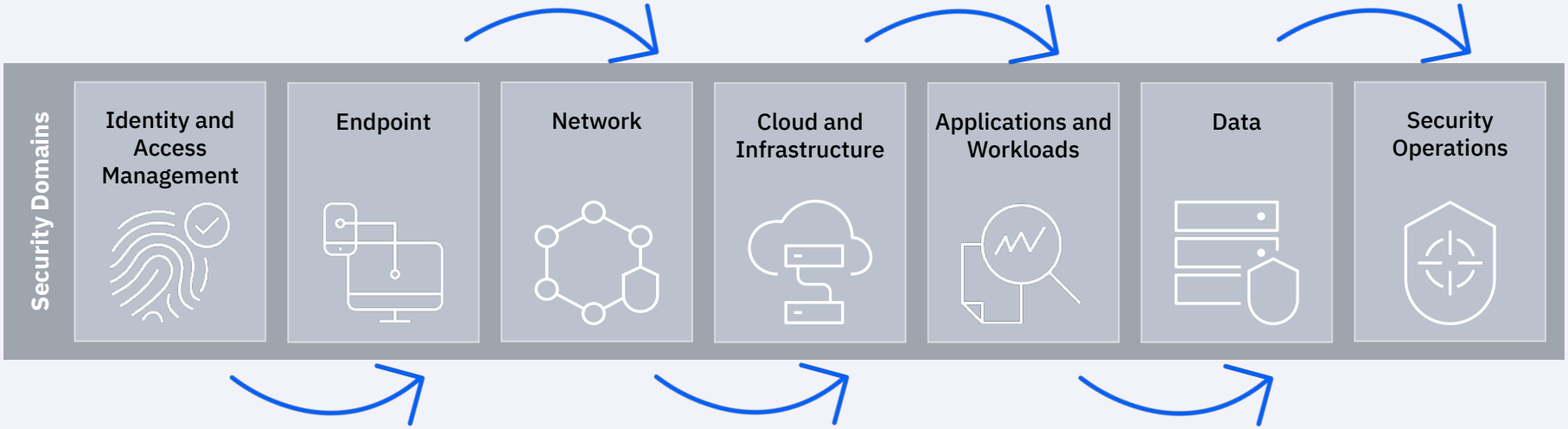


Ransomware attacks are highly sophisticated and can go undetected for weeks or months

There are many individual controls that can be applied to enable protection and improve detection…



...However, no single tool can holistically solve the challenge of business disruption.



It demands open integration across security and IT domains.

Assessing your Maturity

1 Ad-hoc

Rudimentary security controls exist in some places

- Remote workforce connectivity isn't organized in a structured way.
- VPN without additional measures or peer-to-peer RDP connectivity.

2 Repeatable

Basic security controls are in place but in siloes

- VPN used for most of the remote connectivity
- 2FA authentication for power users
- Internet traffic still backhauled to data center for inspection

3 Defined

Zones exist that require different levels of authentication for user to access

- Adaptive access for on-premise web applications but not for all end-user applications
- End-user device posture fed into adaptive access
- ZTNA being evaluated

4 Managed

Security controls to make trusted decisions. Trust level defines the required authentication method

- ZTNA used for connectivity to most of enterprise applications
- Adaptive access used for full context to make access decisions
- Enterprise applications in micro segments
- SOAR capabilities reactive
- SASE provides network security from the Cloud

5 Optimized

Architecture with central policy engine enables integrated decisions across planes and security domains to grant or deny access

- All SASE capabilities core building blocks for network security throughout organization
- Integration with IAM and XDR platforms automated bi-directional
- Security alerts affect sessions
- AI & ML capabilities improve security and end-user experience.

Foundational — **Zero Trust**

A roadmap for no matter where you are

1, 2
Getting started (Prepare)
Where do I begin?

Identifying high-value assets and enabling recovery.

Solutions may include:
- **Discover**, classify, record high-value assets and enable MFA for access
- Use a **risk-based approach** to strengthening security posture
- **Define a cyber resiliency** (backup / recovery) plan
- **Segment,** limit, continuously assess need for access
- **Rehearse** incident response through adversarial simulation exercises, pen testing, etc.
- **Educate** personnel on cyber security and incident response
- Implement Vulnerability Scanning & Patch Management

3, 4
Intermediate (Protect)
How do I advance?

Early detection and accelerated response.

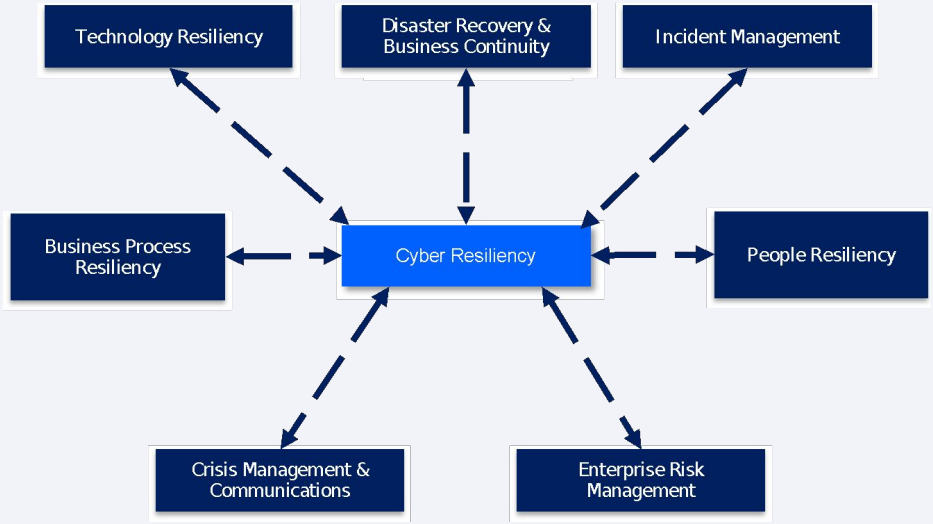
Solutions may include:
- Enable **enterprise-level visibility** by monitoring high value assets for suspicious access activity
- Deploy a threat intelligence driven full-fledged **EDR** solution across endpoint and server systems
- Enable **AI-based detection and response** (rule/ML, IoC/IoB)
- Enforce **least privilege access** and mandatory PAM access control for high value assets
- Enforce minimum patch levels & security standards on devices accessing the network

5
Advanced (Prevent)
How do I excel?

Reducing the attack surface.

Solutions may include:
- Reduce attack surface with **micro-segmentation**, rule optimization, and enforcement
- Ensure **risk-centric protection** with capabilities like adaptive authentication
- Achieve continuous detection and automated response with **extended detection and response (XDR)**
- Enable **automated response** and recovery capabilities
- Infuse lessons learned into **DevSecOps** to improve config and threat management
- **Continuous testing of our security controls through automation**

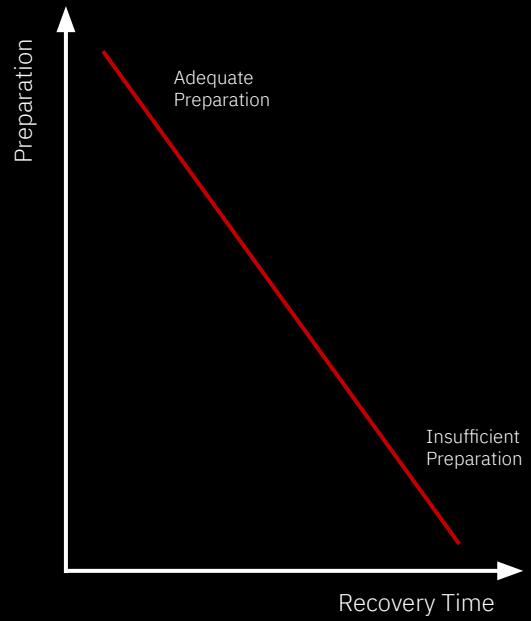
Ransomware is one specific use case that drives a demand for overall cyber resiliency



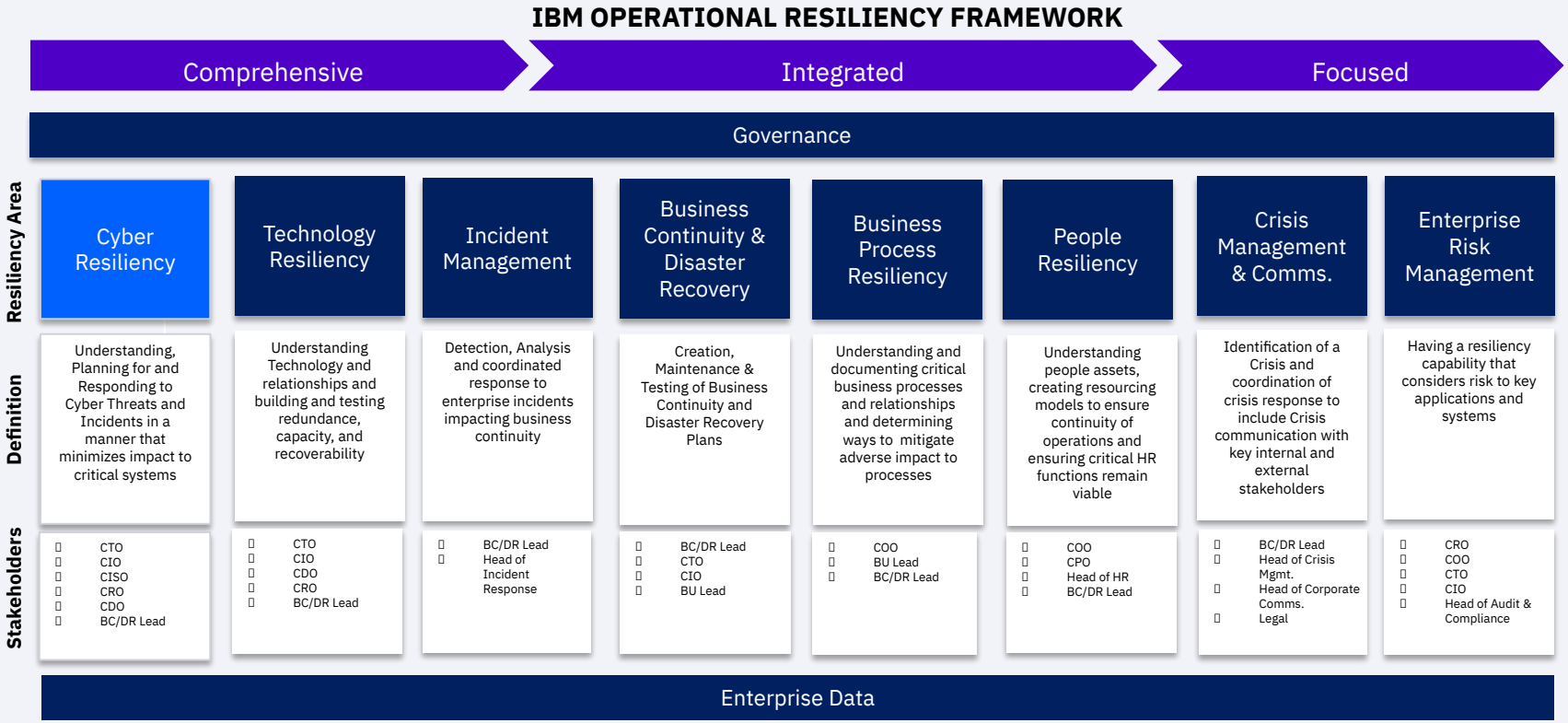
NIST 800-160v2 outlines specific Goals and objectives that need to be met in order to achieve Cyber Resiliency

Recovery time is proportional to preparation.

- Network Segmentation
- Identity & Access Management
- Data Security
- Disaster Recovery
- Threat and Vulnerability Management
- Incident Response

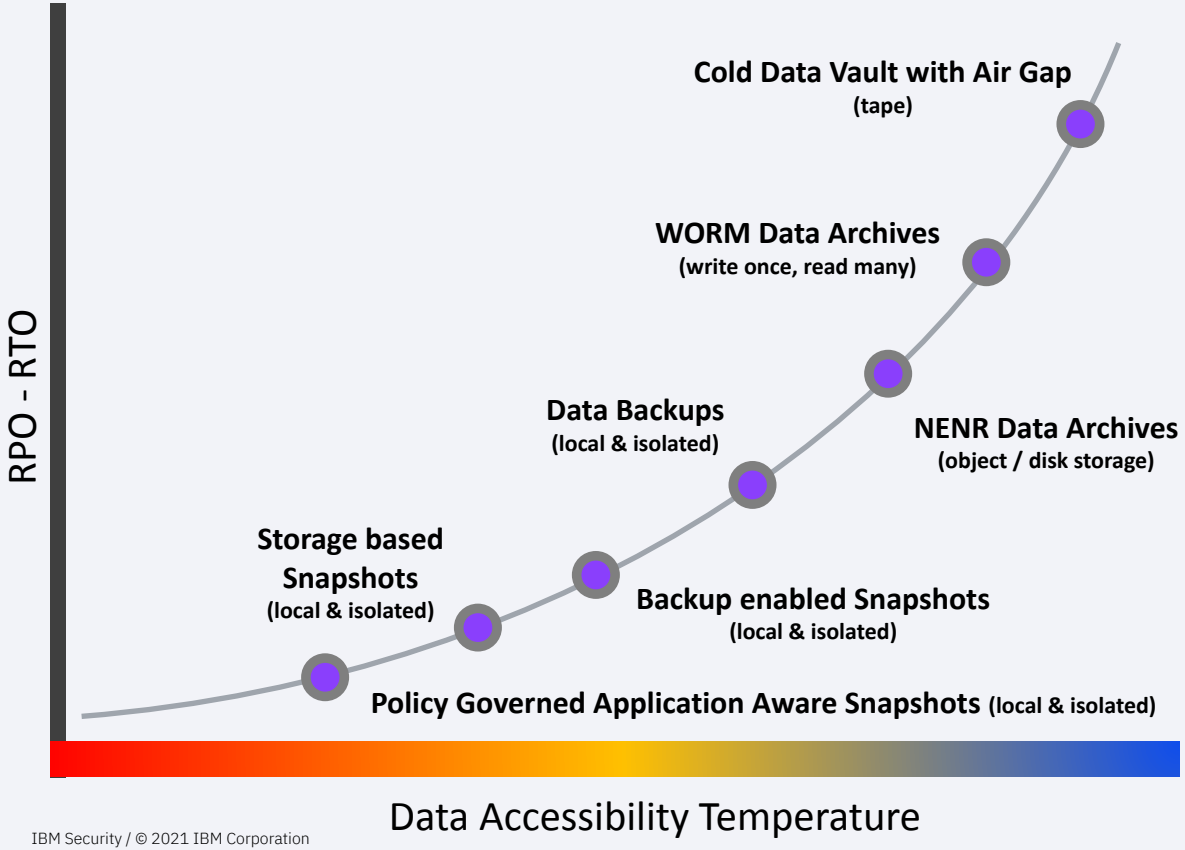


Cyber Resiliency strategy and controls must be in place, across the enterprise, to mitigate the impact of a breach



Source: If applicable, describe source origin

Having the right data resiliency is critical to meeting recovery objectives



Copy Separation:

Create a structure of data separation across multiple layers and services including

- Copy Services
- Backup Services
- Separation of security controls

Immutability & Access Isolation:

Create a structure of data isolation multiple layers and services including

- Air Gap
- Non-erasable / Non-rewritable Storage
- Cold Storage / Object Storage
- Data Vaults
- Isolated Infrastructure

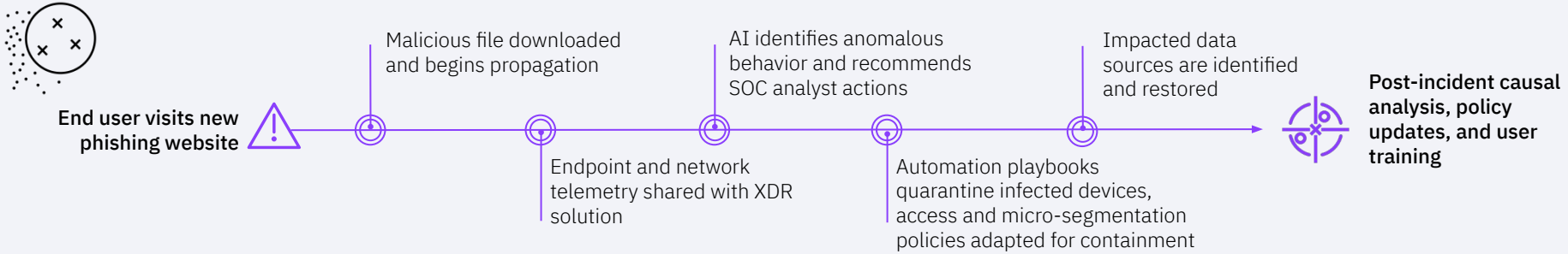
Cyber Resilience:

Requires short- and long-term retention capability

- High snapshot frequency & fastest restore for short-term recovery
- RPO policy governed snapshot frequency for long-term retention and fast recovery

Exercise our new capability

Detecting, responding, and recovering from ransomware



Challenges

- No good baseline for what “normal” activity looks like to aid in detection
- Containing an attack after initial identification is manual and disruptive
- Incident response plans are not well understood or rehearsed in order to be launched and carried out by the teams responsible
- Restoring data from backups is time-consuming, manual, and error prone

Solutions

INSIGHTS
- Endpoint protection solutions to ensure updated operating systems and applications and ability to quarantine infected endpoints and systems
- Vulnerability management to patch systems

ENFORCEMENT
- Micro-segmentation to restrict lateral movement
- Adaptive access to block malicious access

DETECTION & RESPONSE
- Data resilience solutions to automate the restoration of critical data resources
- Extended detection and response (EDR, NDR, SIEM, SOAR, and UEBA) to detect anomalous behavior via integrated telemetry and automate response
- Threat intelligence to quickly identify known attacks

Benefits

- Faster identification and containment limits business impact
- Adaptive access control policies allow for more targeted response
- Immutable backups are hidden and protected for business continuity
- Enables recovery in hours rather than weeks

Capabilities are only one part of the equation – you need a battle-tested incident response plan

- Simulate an attack
- Test your processes
- Test your team
- Improve your responses

IBM is helping our clients address ransomware and working across the industry to build best practices

200
Ransomware-specific incident responses in 2020-21

150
Ransomware related threat reports

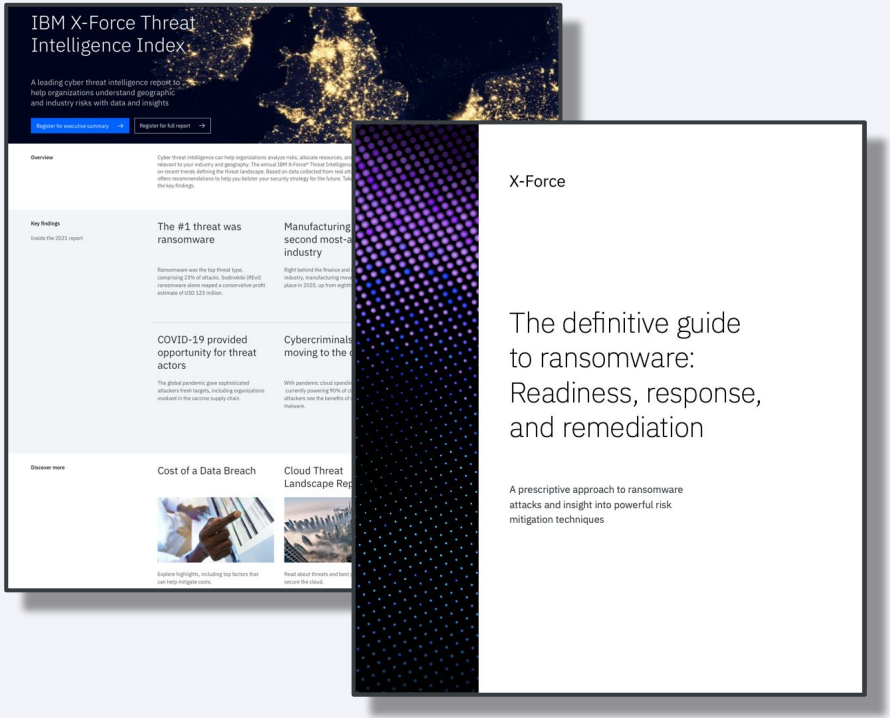
107
APT hives analysis

50B
Categorized URLs

10M
Spam analysis per day

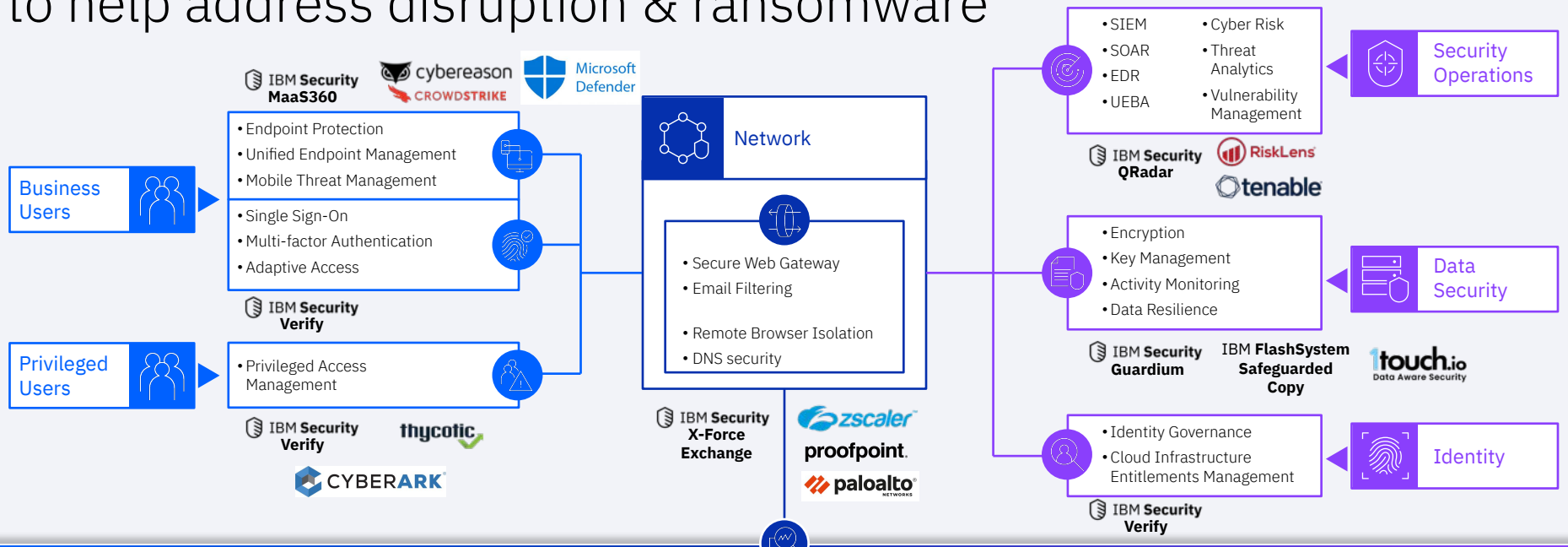
250B
Security events analyzed per day

1B
Malware indicators



OPEN CYBERSECURITY ALLIANCE
NIST
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
THE WHITE HOUSE WASHINGTON

IBM has leading technology, services, and a partner ecosystem* to help address disruption & ransomware



IBM Security

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

** Not an exhaustive list of IBM partners*

Questions?

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity


IBM