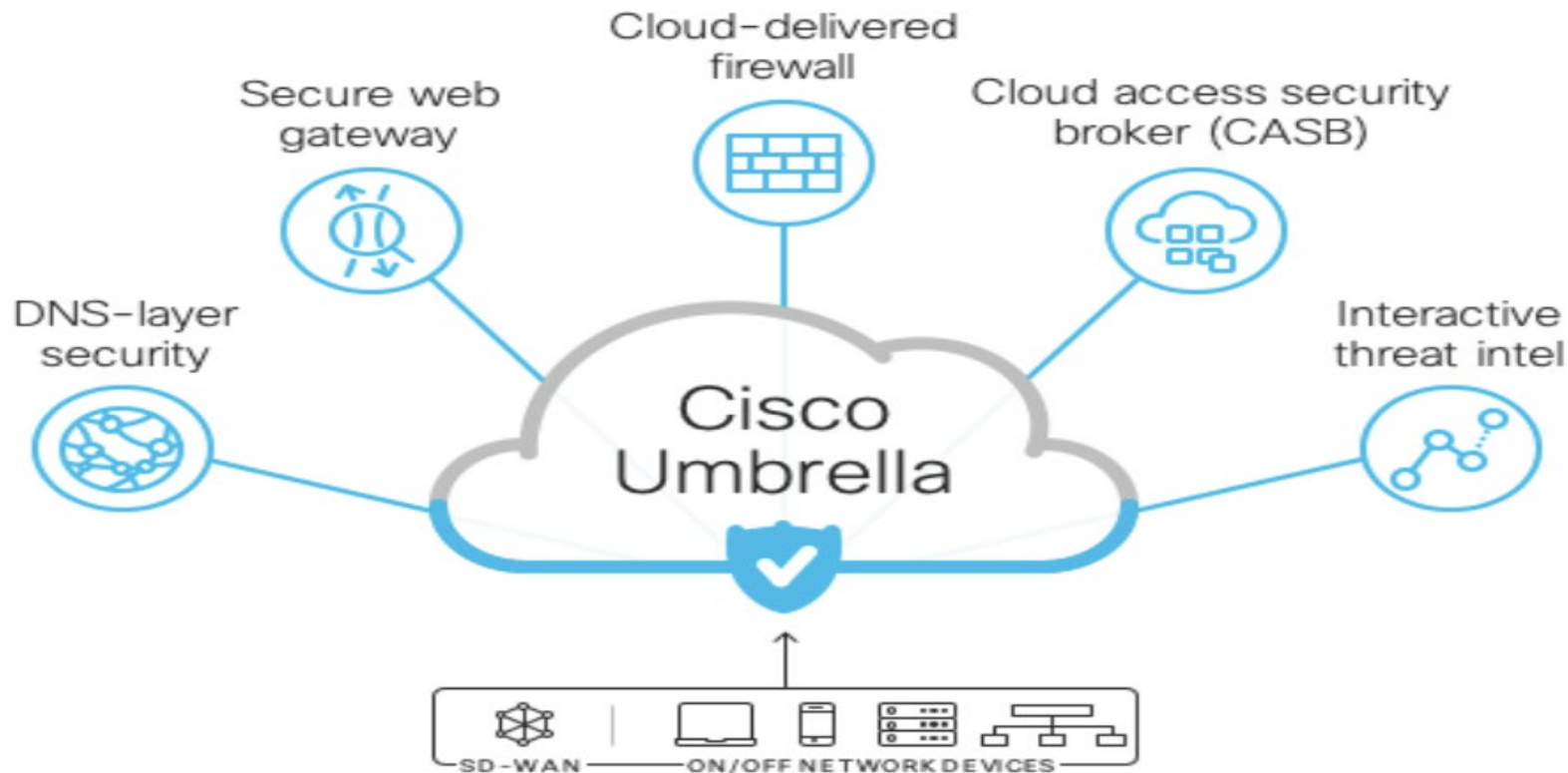# CYBERSECURITY POSTURE

April 23, 2024

Background

- Cybersecurity is a critical aspect of our operations in the city, especially in today's digital landscape where threats are constantly evolving.

- This briefing aims to provide an overview of our cybersecurity posture, including implemented solutions, ongoing initiatives, and future plans to ensure the security and integrity of our systems and data.

Current Cybersecurity Solutions
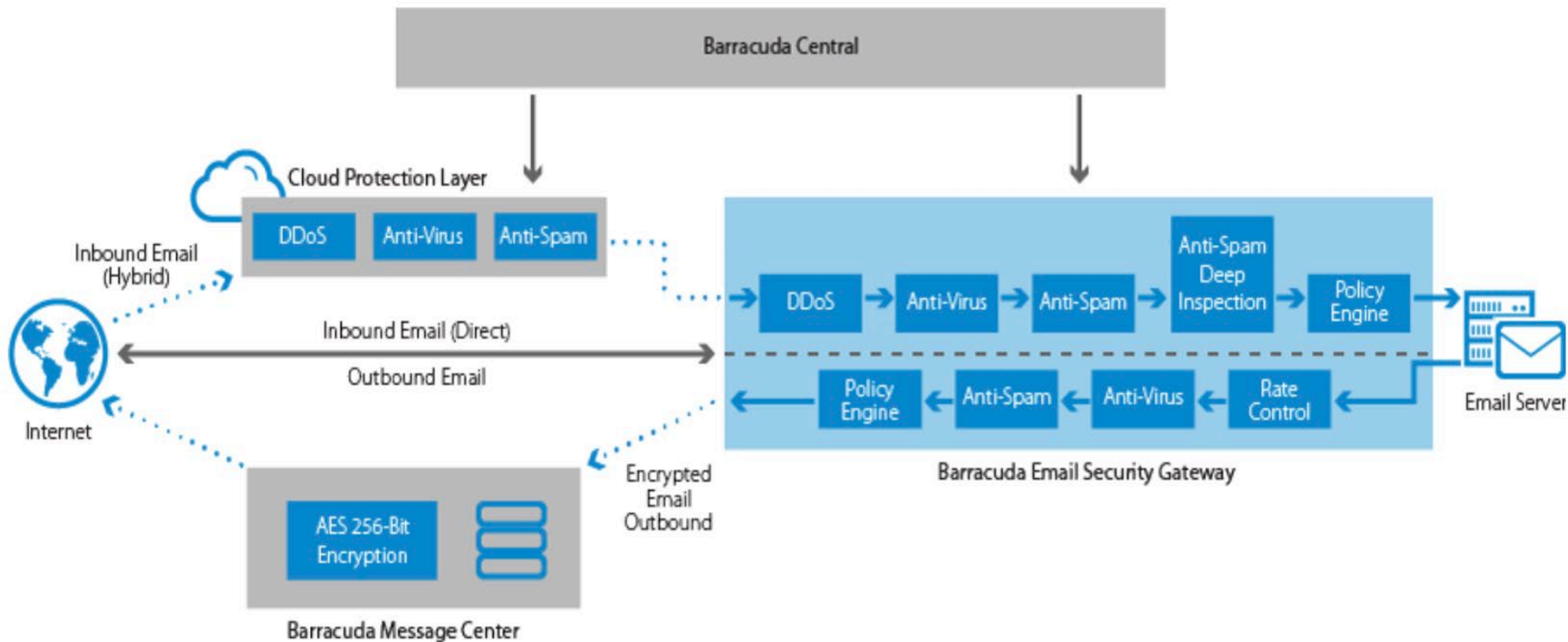
Current Cybersecurity Solutions

Cohesity – Architected for Managing Risk

PREDICTABLE RECOVERY

Compliance
FIPS-140-2| Cohasset | Common Criteria| PCI-DSS, etc.
1

Defend Backup Data
Secure by Design | SpanFS
Immutability | Encryption Inflight & at rest| WORM | Air-Gap
2

Respond
Instant Mass Restore | Global Actionable Search | Deep Visibility
5

Integrated Cybersecurity

Restrict Access
Multi Factor Auth. | Granular RBAC | No Service Backdoor | Whitelisting | Secure App Ecosystem
3

Detect
Ransomware Detection | Vulnerability Scanning | AD Granular Comparison | Auditing
4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Current Cybersecurity Solutions

Current Cybersecurity Solutions

Ongoing Initiatives

- Legacy Application Replacement:
  - Scheduled replacement of legacy applications such as Navaline and PDRMS system to modernize our infrastructure and mitigate potential security vulnerabilities associated with outdated systems
- Cybersecurity and Incident Handling Plan:
  - Developed a comprehensive plan to effectively respond to cybersecurity incidents, ensuring timely detection, containment, eradication, and recovery
- Annual Cybersecurity Training:
  - Conducting annual cybersecurity training sessions for all employees to enhance awareness and ensure compliance

Future Plans

- Regular Security Assessments and Audits:
  - Instituting periodic security assessments and audits to identify vulnerabilities, assess risks, and validate the effectiveness of our cybersecurity measures (completed Network Assessment Apr 2024)

- Collaboration with External Partners:
  - Strengthening partnerships with external cybersecurity experts and agencies to stay abreast of emerging threats and leverage their expertise in enhancing our cybersecurity posture