```
Administrator: C:\Windows\System32\cmd.exe

Platform    : UltraCUSE
Version     : 5.1.3.00250

C:\Program Files\UltraAS\UltraCUSE>
C:\Program Files\UltraAS\UltraCUSE>
```

Port of Seattle / Seattle-Tacoma International Airport (SEA) Cyber Attack

Matt Breed, Chief Information Officer

September 24, 2025

Rhysida Ransomware Group

A sophisticated threat actor group known for targeting critical infrastructure and government organizations. Named after a genus of centipede.

To gain unauthorized access to sensitive systems, they employ advanced techniques, including:

- Phishing
- Malware
- Exploit kits
- Recon

What Was Impacted

Unavailable Services at SEA & Maritime Facilities

Our Apologies

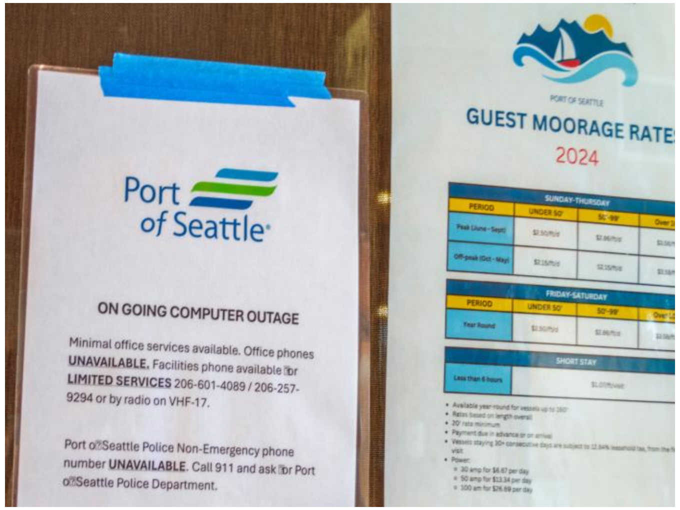
THIS KIOSK IS TEMPORARILY UNAVAILABLE

Please see your airline's ticket counter for further assistance.

DUE TO TECHNICAL ISSUES. THE MAIN OFFICE PHONE IS DOWN

NEED ASSISTANCE?

CALL (206) 617-4898



ON GOING COMPUTER OUTAGE

Minimal office services available. Office phones **UNAVAILABLE.** Facilities phone available or **LIMITED SERVICES** 206-601-4089 / 206-257-9294 or by radio on VHF-17.

Port o Seattle Police Non-Emergency phone number **UNAVAILABLE**. Call 911 and ask or Port o Seattle Police Department.

Traveler-facing systems:

- Wi-Fi
- Phones (non-cell)
- FIDS and BIDS
- Website and mobile app
- Ground transportation systems
- Checkpoint wait times
- Common-use ticket counters
- ...and more

Life Safety & Security

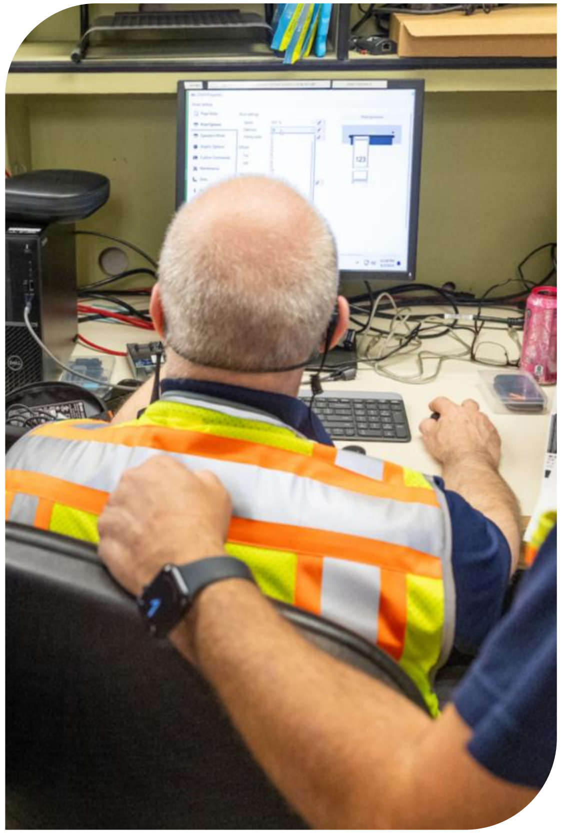
- Alarms
- Fire watch
- Some camera systems
- Door Fobs

What Was Impacted

Unavailable Internal Services

- Email
- Teams and One Drive
- Contracts database
- GIS and mapping software
- Printing
- Badging (new and renewing)
- Payroll applications
- Accounting applications (invoicing and payments)

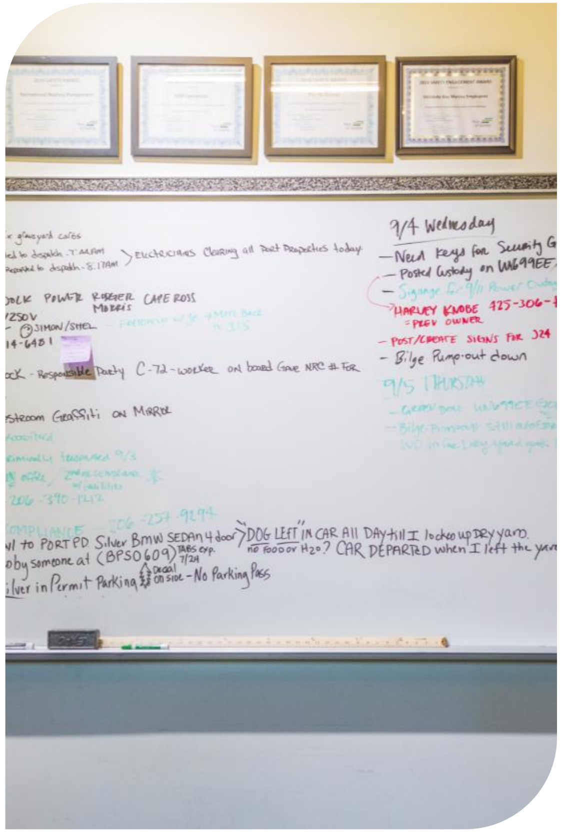
Collaborative and Cross Department Response



Detection, Investigation and Recovery

Continuity of Operations

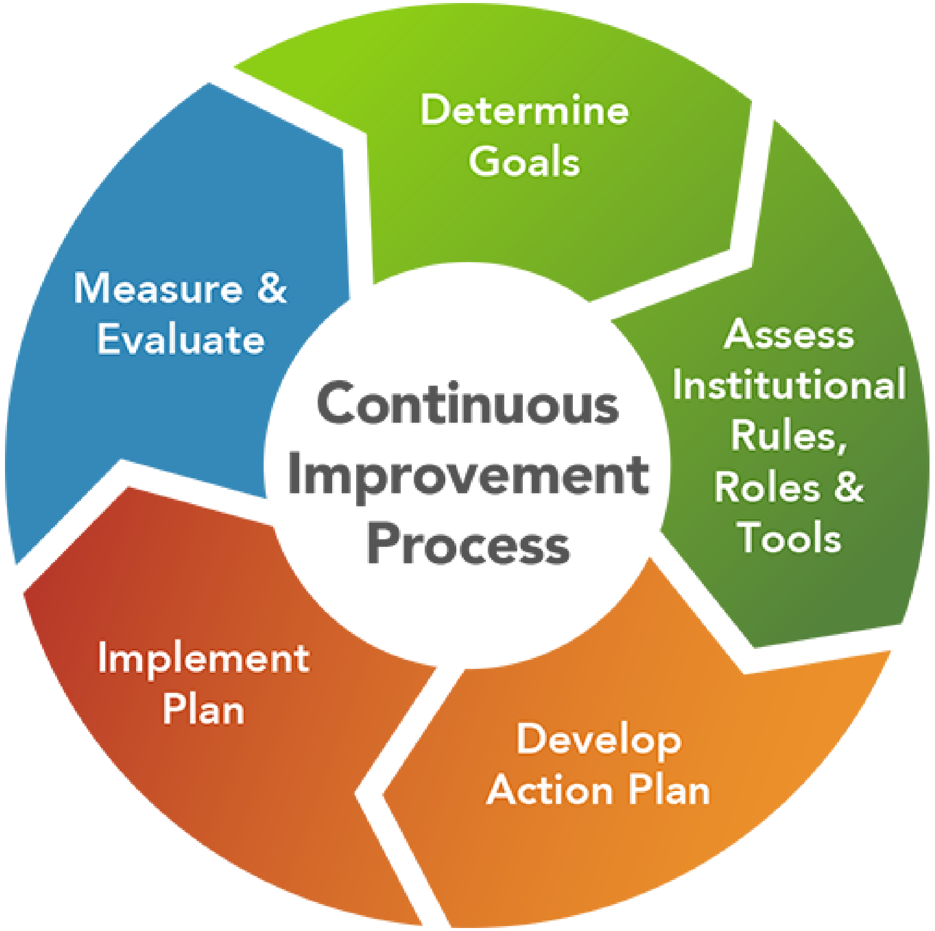
Enterprise Mitigation


graveyard cares
dispatch 7:AAAM
Responded to dispatch 8:17AM
Electricians Clearing all Port Properties today
9/4 Wednesday
— Need keys for Security
— Posted Custody on WA699EE
— Signage for 9/11 Power Outage
HARVEY KNOBE 425-306-
= PREV OWNER
— POST/CREATE SIGNS FOR J24
— Bilge Pump-out down
9/5 THURSDAY
POWER ROEGER MORRIS CAPE ROSS
1250V
SIMON/STEEL
14-6481
Responsible Party C-72-worker on board Gave NRC # For
Restroom Graffiti on MIRROR
206-390-1212
COMPLIANCE 206-257-9294
to PORT PD Silver BMW SEDAN 4 door (BPS0609) TABS exp. 7/24
by someone at
Silver in Permit Parking Decal on side - No Parking Pass
"DOG LEFT" IN CAR All Day till I locked up DRY yard.
no food or H2O? CAR DEPARTED when I left the yard

Policy Decisions

After Action

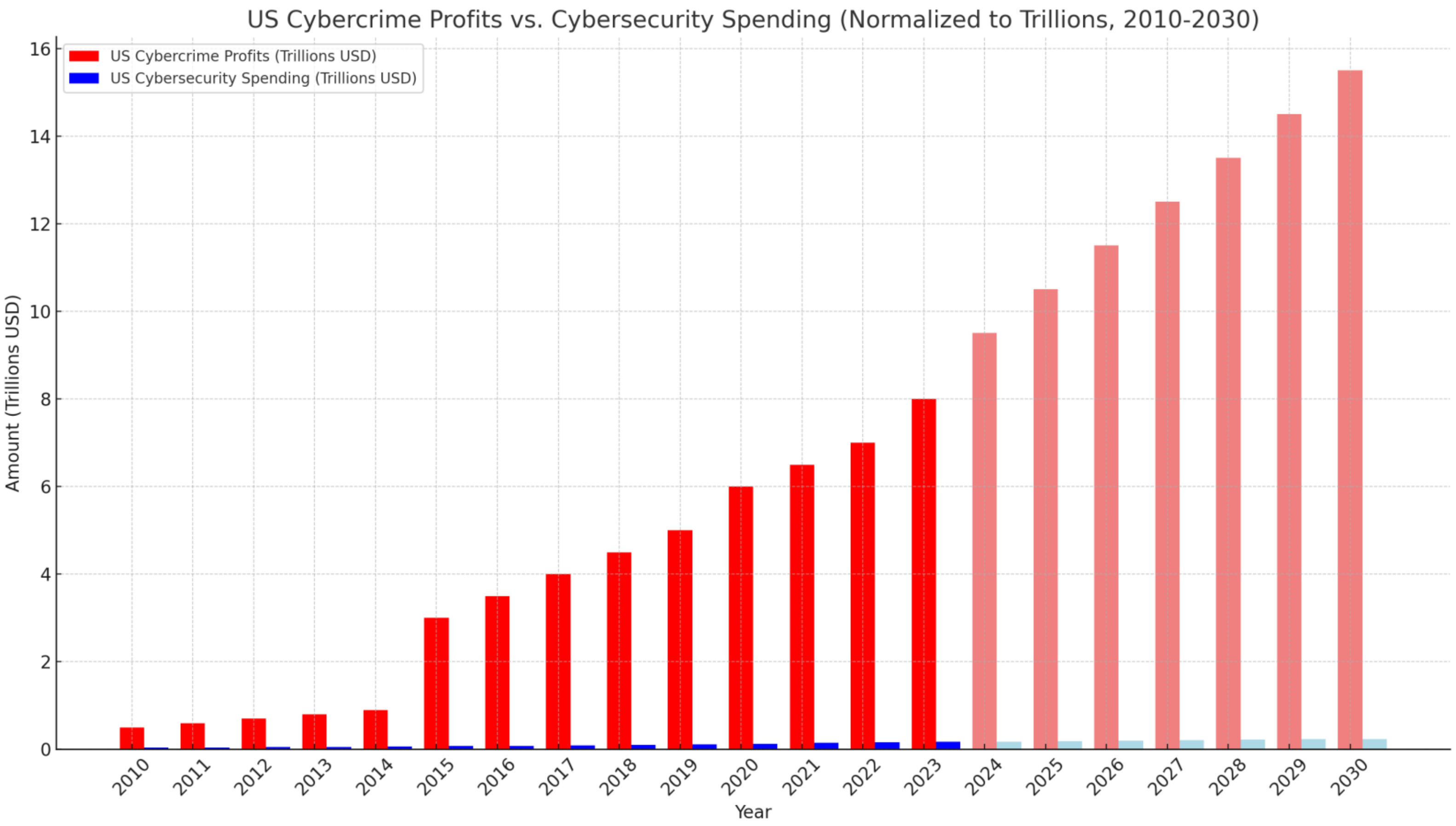
- Operational Analysis - What Worked / What Didn’t
- Solidify Technical Analysis
- Identify Ways to Improve
- Implement
- Share Results


Determine Goals
Assess Institutional Rules, Roles & Tools
Develop Action Plan
Implement Plan
Measure & Evaluate
Continuous Improvement Process

WHAT HAVE WE LEARNED?

Threat Actors (TAs) are Well-Organized and Well-Funded

- Run as a business
- Deploy multiple functional teams
- Organized by specialty
- Will flex teams based on situation



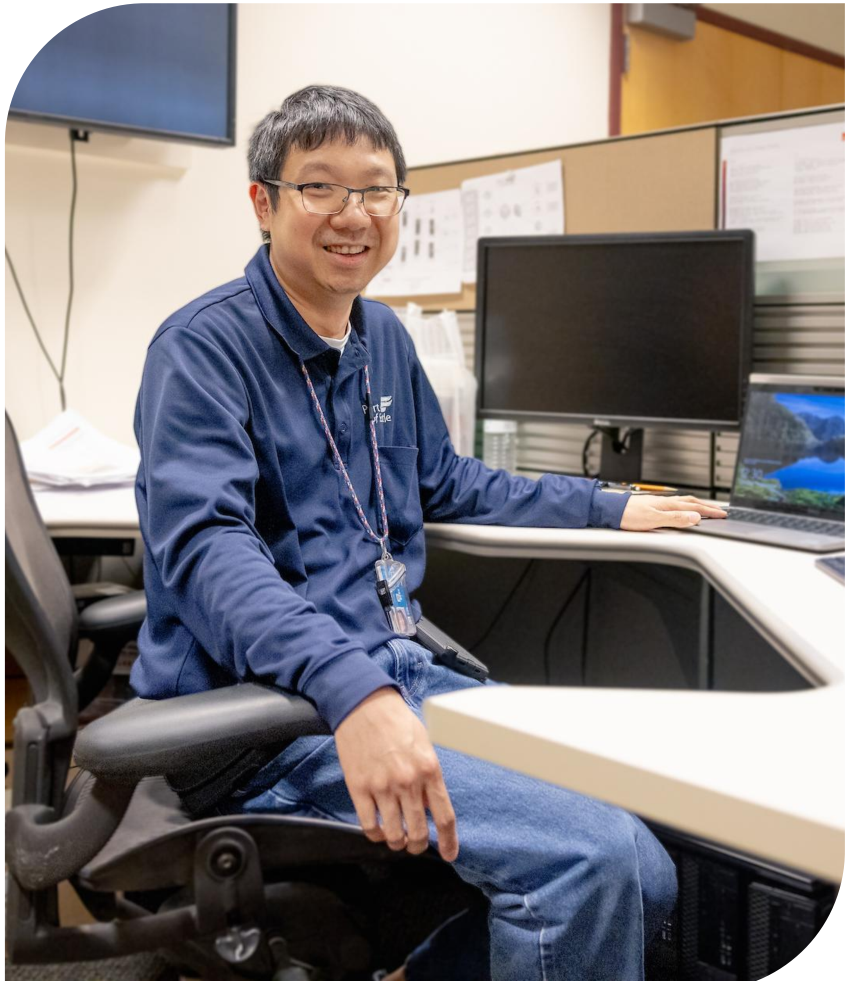
Tactics Evolve Quickly

- TAs understand business
- TAs build roadmap of systems and architecture
- TAs adapt as more information is acquired
- Execution is automated and rapid
- Clean up is automated and thorough
- Guidance from “experts” may be dated

TA = Threat Actor

Recovery Prioritization

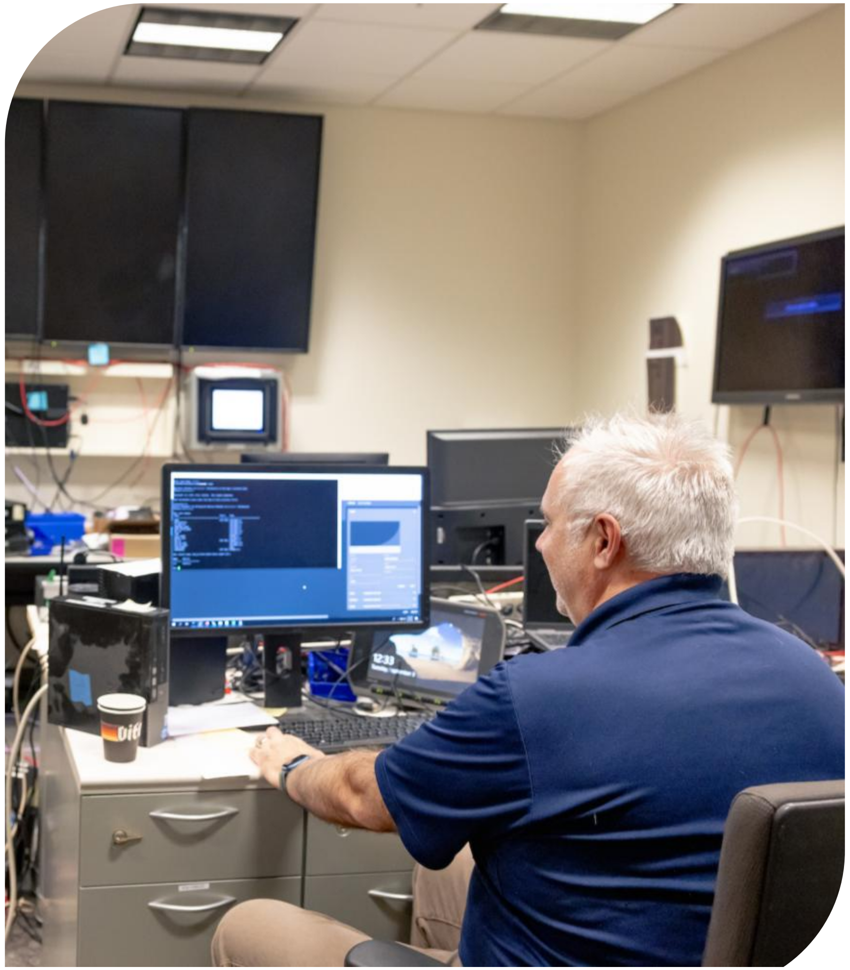
- Communication is key – one source-multiple views
- Defined system prioritizations need to be aligned with current organizational priorities
- Know your key vendors and leverage those relationships
- Leverage your existing staff



DO NOT WASTE A GOOD CYBERATTACK

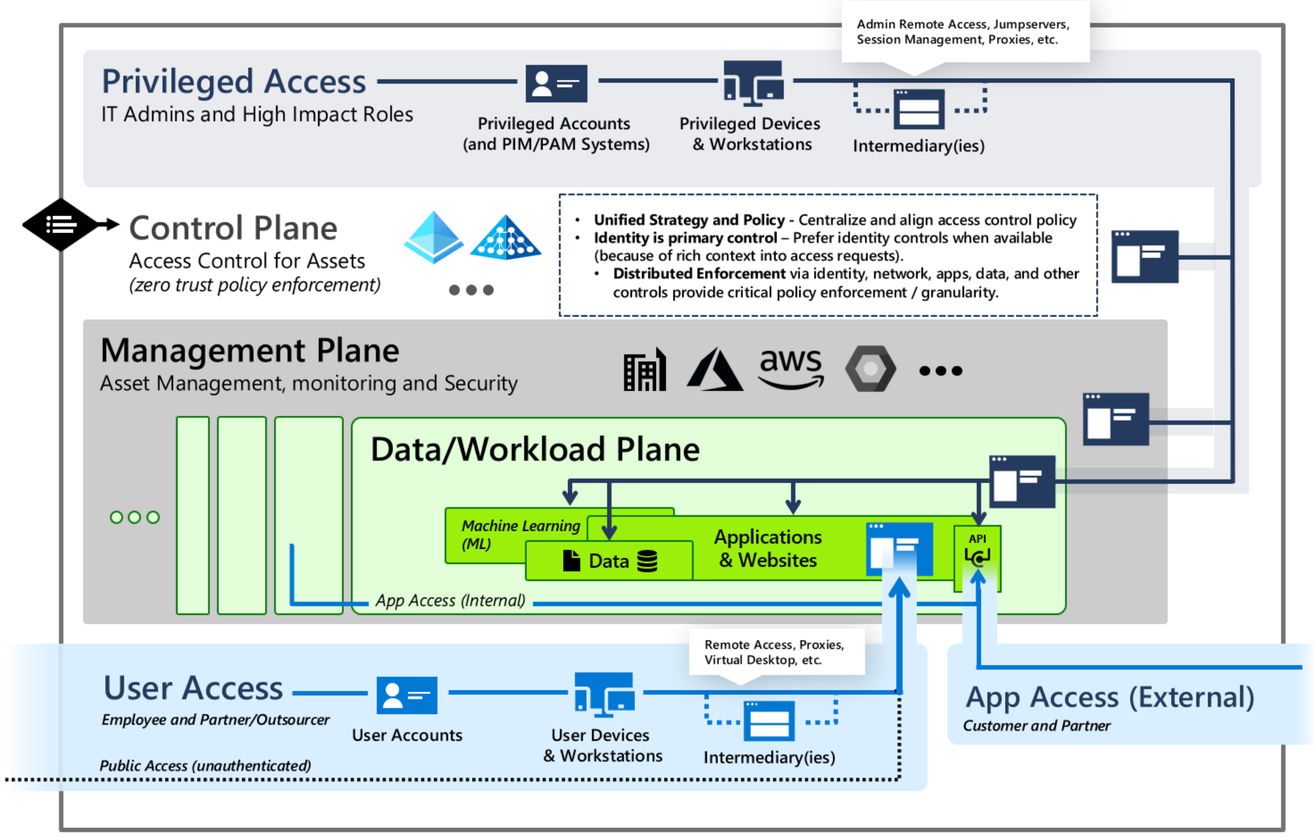
Projects Accelerated

- Windows Modernization (Servers and Workstations) – Accelerated
- Network Refresh
- Server Refresh
- Firewalls
- Endpoint Protection
- Various application upgrades and retirements



Updated Security Posture

- Aggressive Tiering
- Better Endpoint Security
- Better Endpoint Management
- 24x7 Security Operations Center / Managed Detection and Response (MDR)
- Enhanced perimeter security



Admin Remote Access, Jumpservers, Session Management, Proxies, etc.

Privileged Access

IT Admins and High Impact Roles

Privileged Accounts (and PIM/PAM Systems)

Privileged Devices & Workstations

Intermediary(ies)

Control Plane

Access Control for Assets

(zero trust policy enforcement)

- **Unified Strategy and Policy** - Centralize and align access control policy
- **Identity is primary control** – Prefer identity controls when available (because of rich context into access requests).
  - **Distributed Enforcement** via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.

Management Plane

Asset Management, monitoring and Security

Data/Workload Plane

Machine Learning (ML)

Data

Applications & Websites

API

App Access (Internal)

Remote Access, Proxies, Virtual Desktop, etc.

User Access

Employee and Partner/Outsourcer

User Accounts

User Devices & Workstations

Intermediary(ies)

Public Access (unauthenticated)

App Access (External)

Customer and Partner

Matt Breed

CIO Port of Seattle

breed.m@portseattle.org | +1.206.660.5233 c