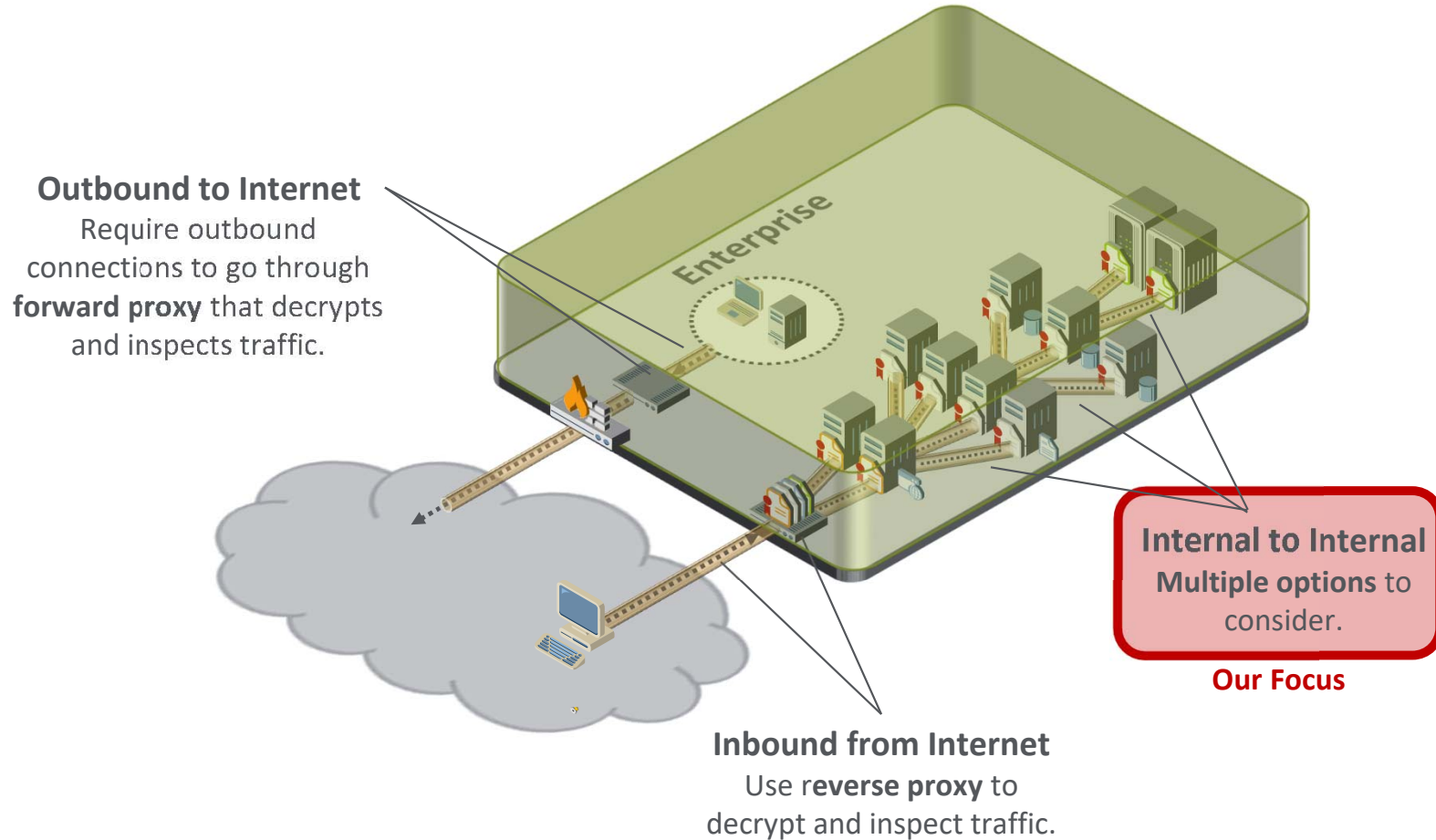


# Instructive Scenarios for Demonstration Projects

Paul Turner  
President, Epuio

# Epuio™ Area of Focus

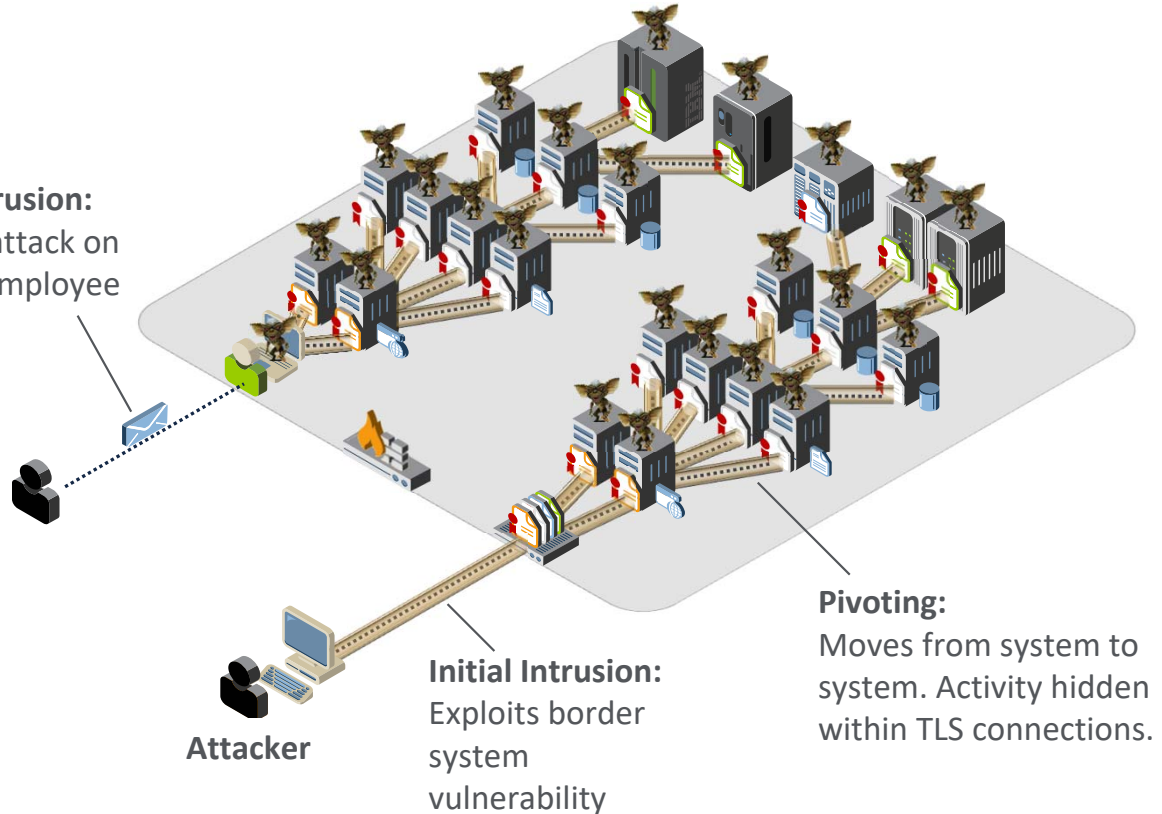


# Epuio™ Security: Pivoting

## Pivoting Requirements:

- Accurately monitor for and detect attempts to move between systems on the network
- Minimize operational impact of monitoring (e.g., added latency, CPU load, etc.)
- Visibility across all relevant connections
- Consistent data format for processing and analysis

**Initial Intrusion:**  
Phishing attack on internal employee



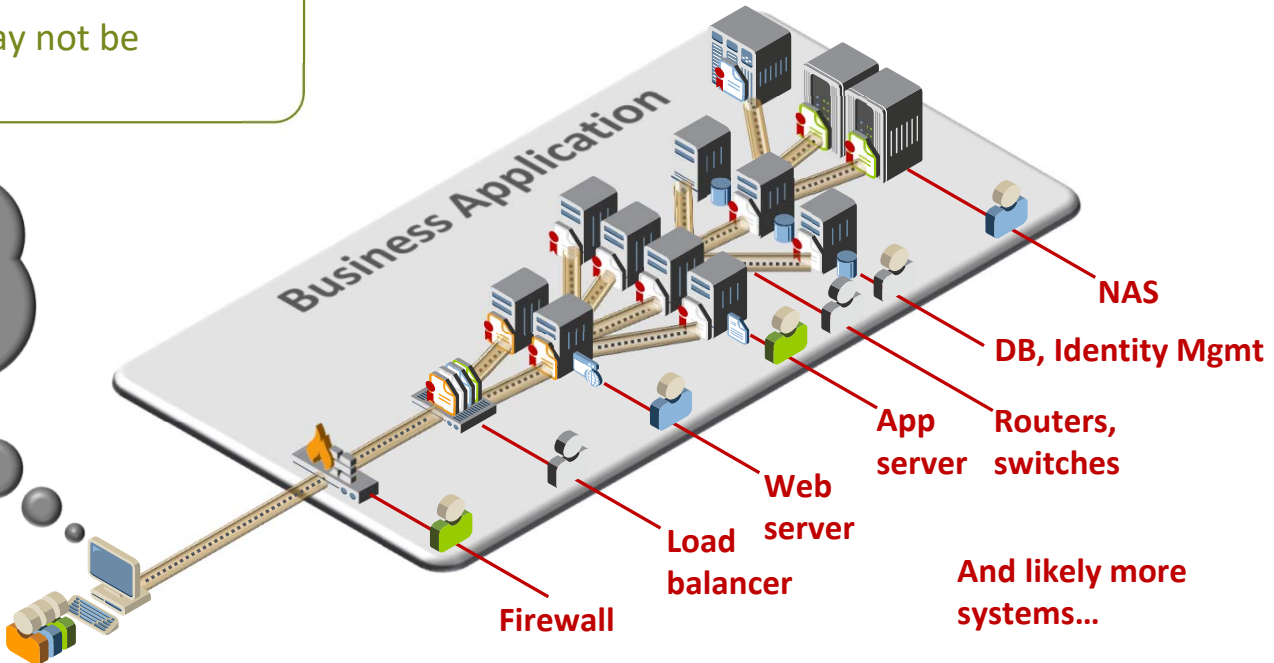
# Epuio™ Operations: Troubleshooting

## Troubleshooting Requirements:

- Ability to trace transactions through all tiers of application (including routers, firewalls, switches, etc.)
- Collect detailed information showing result of operations performed (may not be available in logs)
- Ability to view detailed historical data (may not be available in logs)

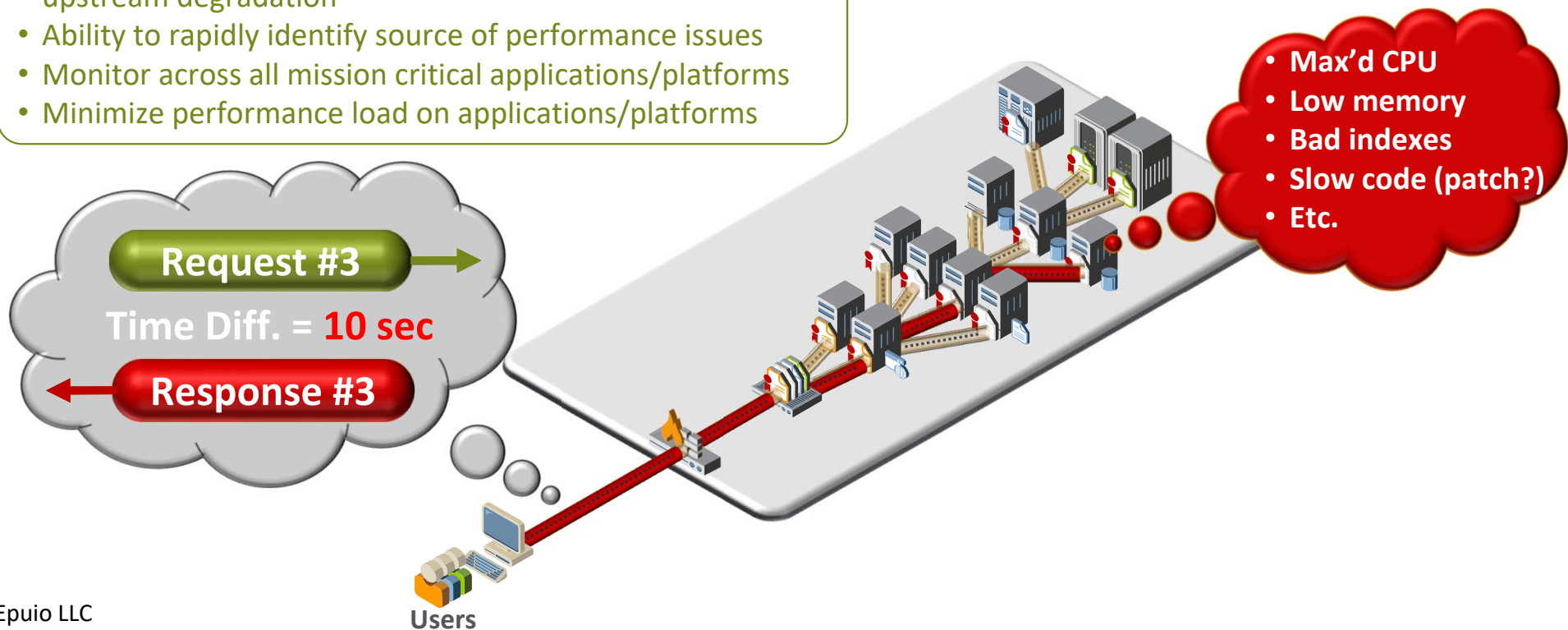
Sev 1 or 2 issues:

- Application down
- Intermittent failures
- Poor performance
- Etc.



## Performance Monitoring Requirements:

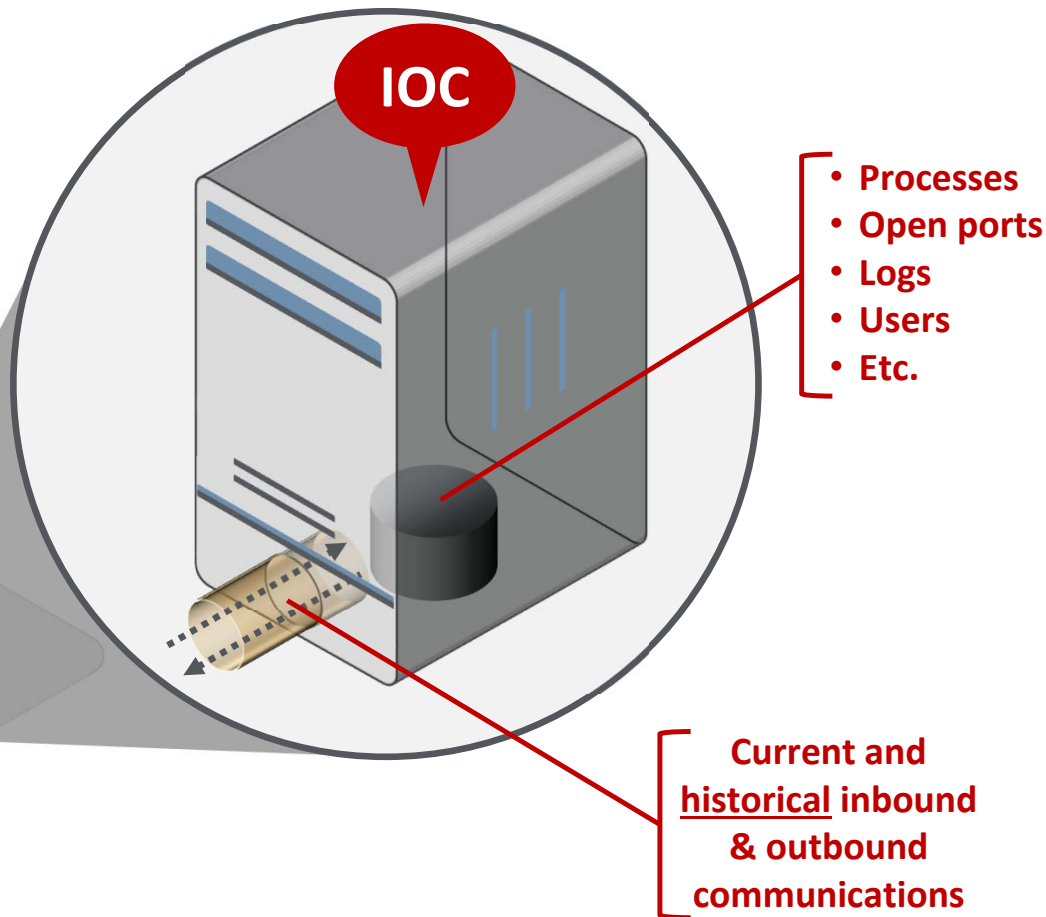
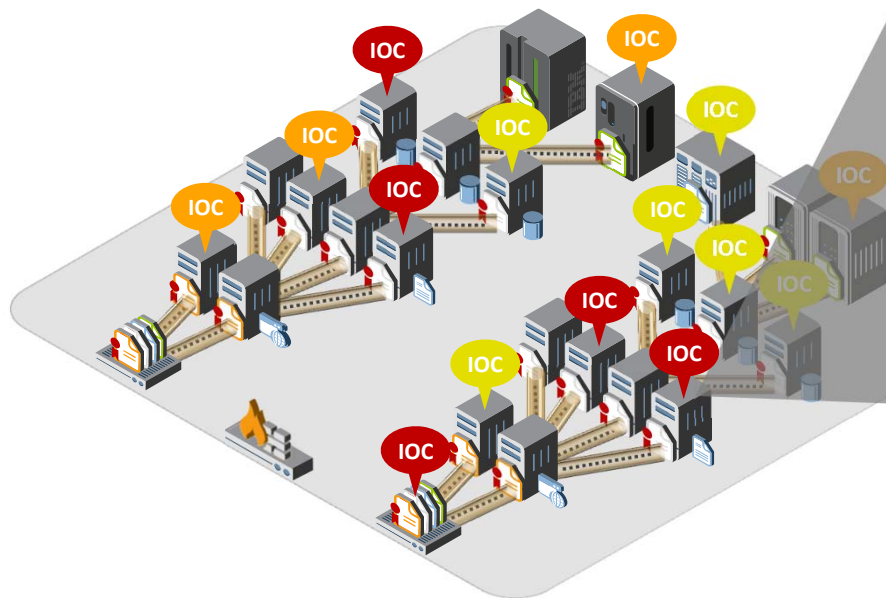
- Rapidly & accurately detect user performance issues
- Predict and resolve customer performance issues based on upstream degradation
- Ability to rapidly identify source of performance issues
- Monitor across all mission critical applications/platforms
- Minimize performance load on applications/platforms



# Security: Triage and Response to Indicators of Compromise (IOCs)

## Threat Triage Requirements:

- Rapidly get clear picture of system state
- Reduce triage time with an accurate, detailed picture of current and historical communications
- Minimize reliance on data sources that can be manipulated by attackers

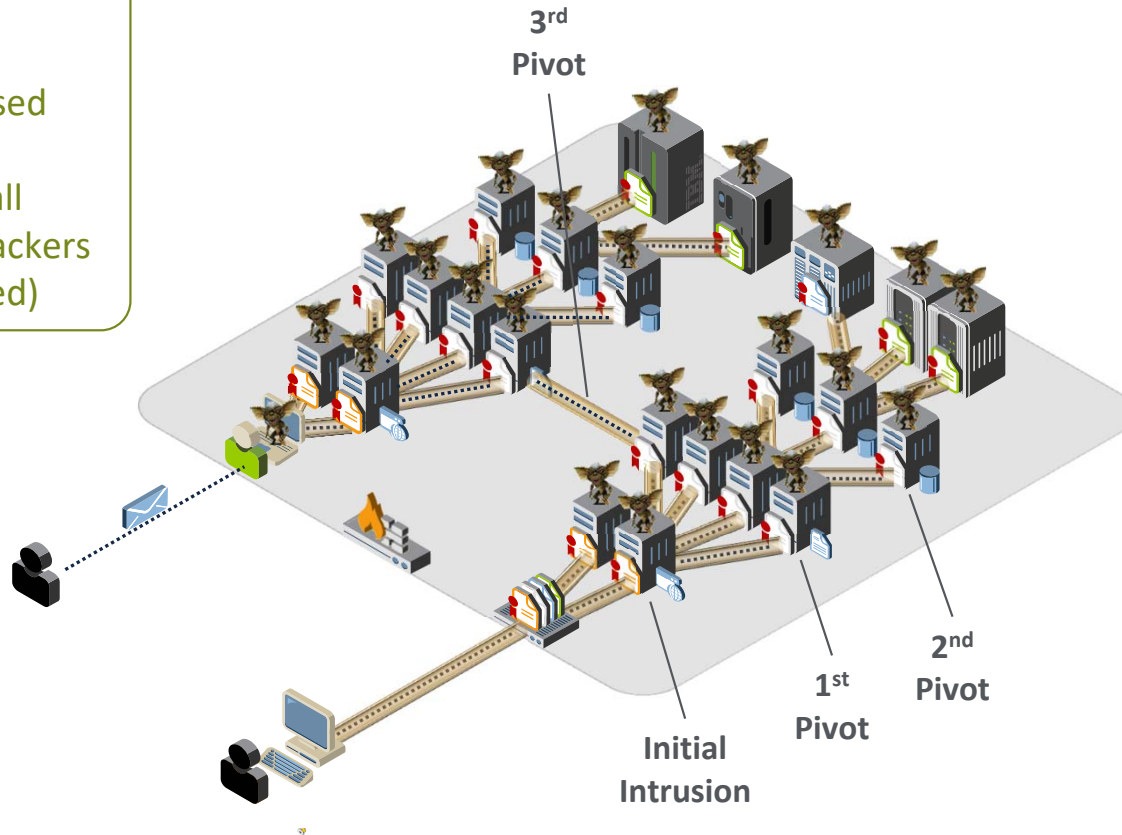




# Epuio™ Security: Forensics

## Forensics Requirements:

- Ability to trace path of attack across network of compromised systems
- Accurate information about all operations performed by attackers (even if logs were manipulated)





# Thank you!

Paul Turner  
President, Epuio  
[pturner@epuio.com](mailto:pturner@epuio.com)