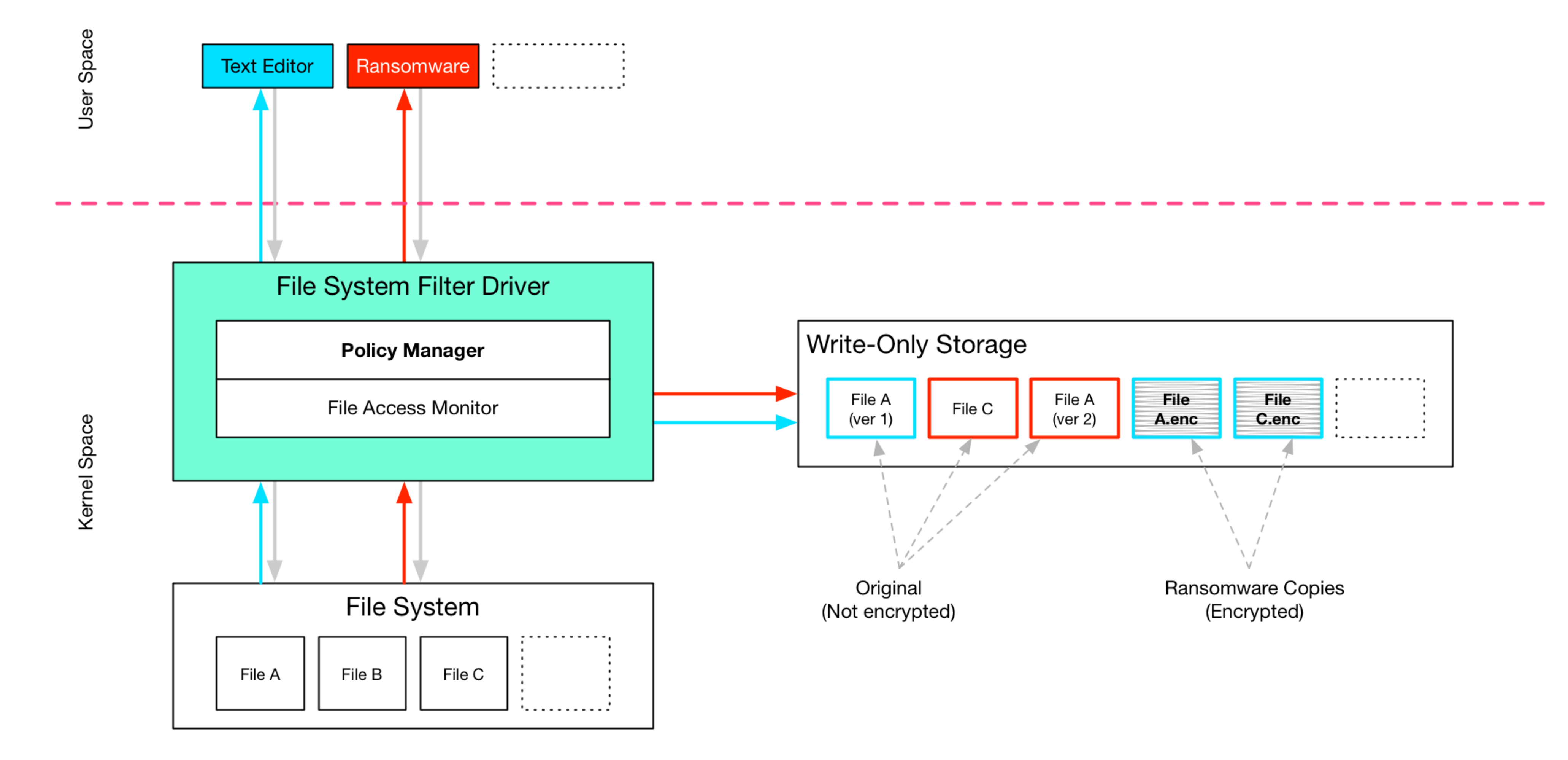
# An Approach to Ransomware Effects Mitigation

Dr. Marco M. Carvalho, Adrian Granados, Anthony Alves

School of Computing, Florida Institute of Technology

We propose a lightweight and seamless approach to mitigate the effects of ransomware in end-user systems. Our solution provides a risk-based mechanism to automatically backup the data associated with write system call operations performed by the kernel on user files, using an automatic, on-the-fly, write-only backup initiated when user behavior elevates risk level.



Backup File System Minifilter Flow

## Risk-Based Backup Mechanism

- Automatically initiated when risk level is above certain threshold
- Windows File System Filter Driver
- Transparent and secure
- User & document files only
- Data saved to a secure, write-only, circular buffer storage

## Risk Level Assessment

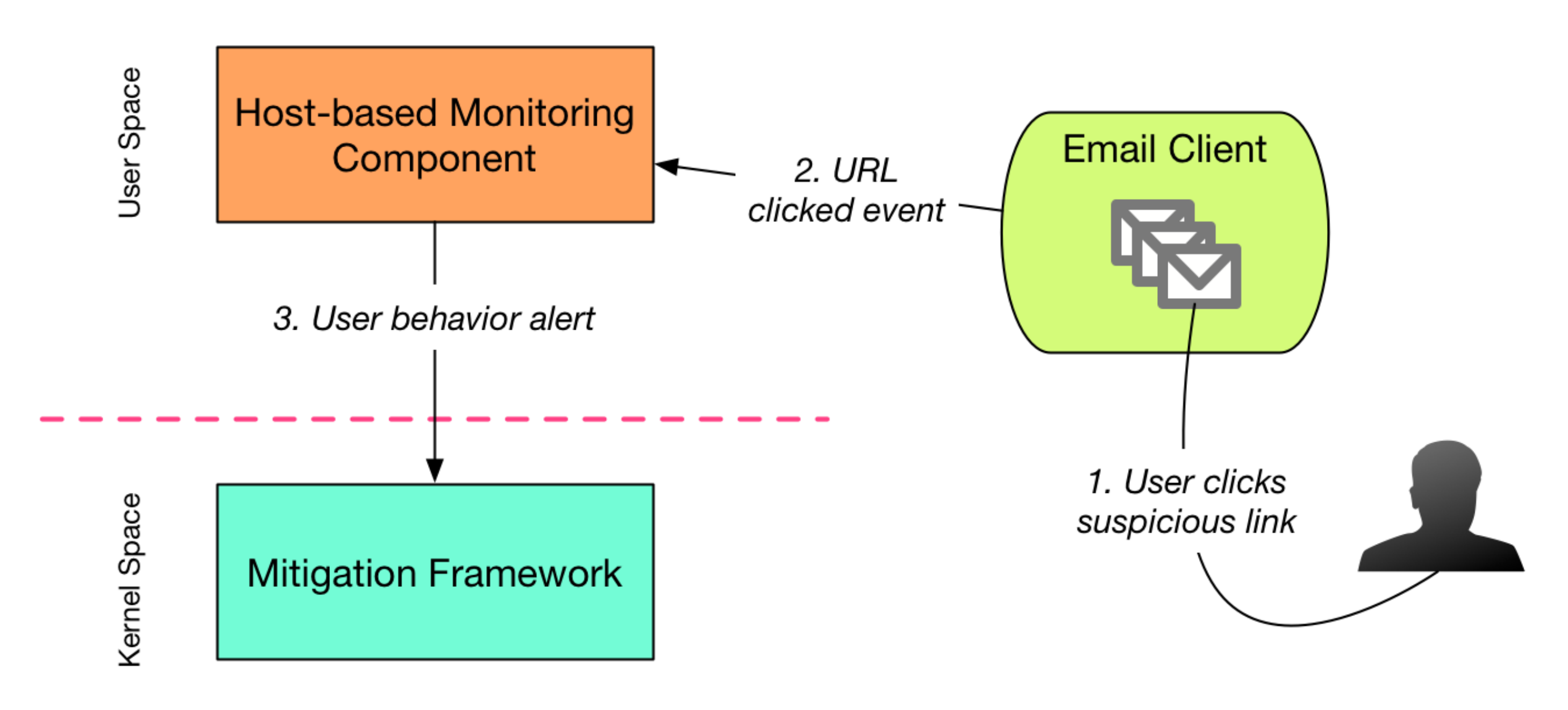
- Most attacks target users via phishing or compromised social accounts
- Even the most careful and informed user can become a victim of ransomware
- User behavior and system activity is monitored to determine risk level of infection by ransomware
- Host and network-based behavior monitoring

### *Host-based monitoring*

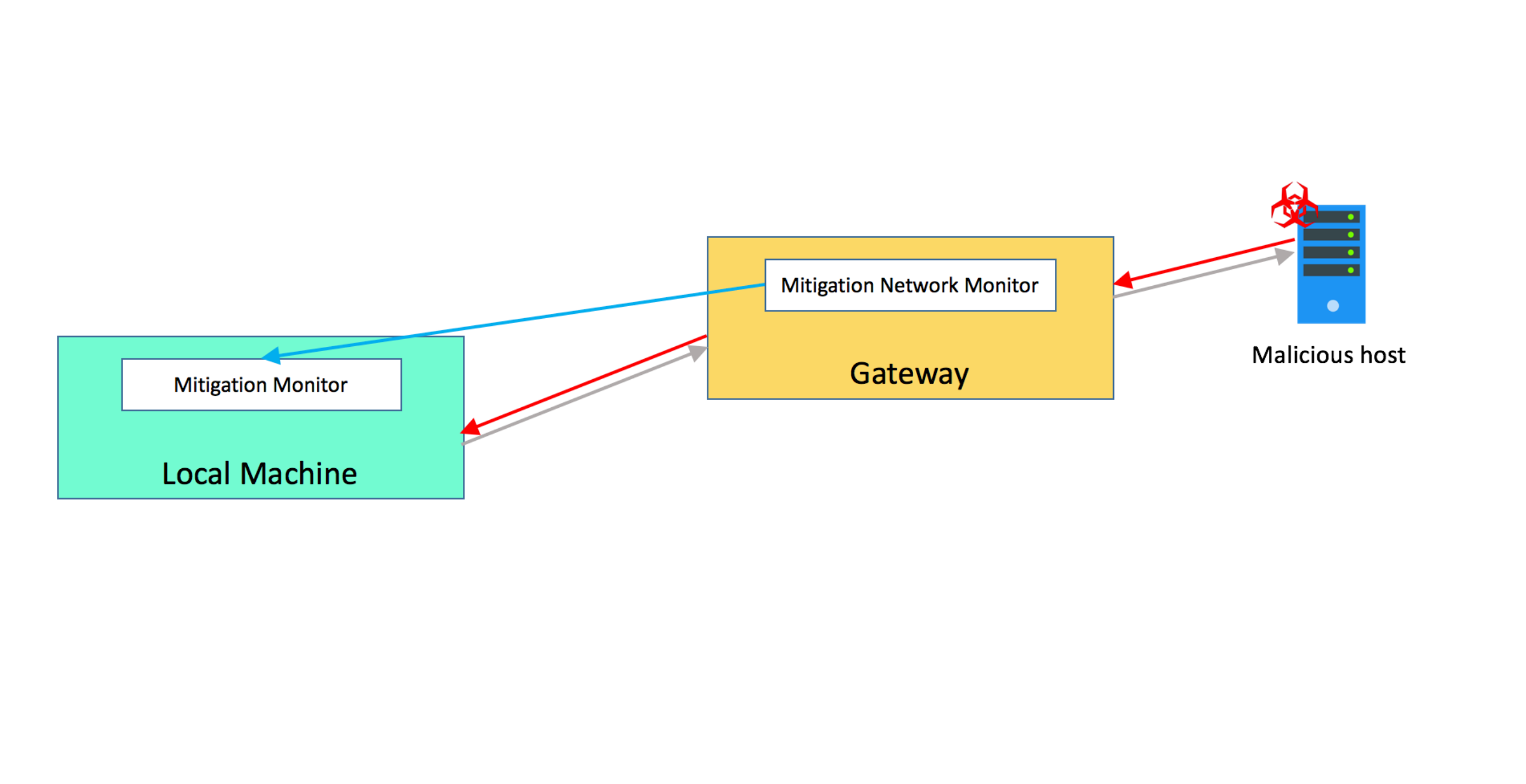
- User activity tracking agent
- Initial rule based approach
- System-wide monitoring capabilities
- Learns user behavior and constructs behavior models

### *Network-based monitoring*

- Enterprise gateway anti-spam & email scanning/filtering
- Suspicious URL database
- Send backup triggers to a list of connected hosts



Host-based Monitoring Model Flow



Network-based Monitoring Model Flow

SCORE
SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING

C3E

Computational Cybersecurity in Compromised Environments
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia