Technical Brief by Doug Tallinger
Controller Platform Strategy, Global Delivery Group/Workplace Controller Development
Xerox Corporation

Make Threat Response Instantaneous with Xerox, McAfee and Cisco

Protecting multifunction printers and your network with comprehensive security.

xerox™

Time is a critical factor in cybersecurity.

While other networked print devices use a fractured, manual approach to cybersecurity, Xerox® multifunction printers (MFPs) employ an orchestrated response that neutralizes threats at their source the moment they occur.

By augmenting our embedded security technologies with the market-leading McAfee® DXL and Cisco® pxGrid platforms, Xerox® MFPs allow you to:

- Gain insight into access and threats
- Automatically manage and enforce enterprise security policies
- Eliminate delays and address threats in real time
- Break up silos and cut down on security blind spots

xerox™

Introducing a more sophisticated approach to cybersecurity.

How Our Orchestrated Response Works

- When the Xerox® MFP* detects a threat, McAfee® Embedded Control whitelisting technology stops the attack at its source.
- The MFP sends an alert of the attack to McAfee® ePolicy Orchestrator (ePO).
- McAfee® ePO communicates the event to Cisco® Identity Services Engine (ISE) over the DXL/pxGrid framework.
- Cisco® Authentication Service takes the affected device off the network until the extent of the attack can be completely evaluated.

Comprehensive network visibility of endpoints and threat response

* Xerox® ConnectKey® i-Series, WorkCentre® EC7836/7856 and AltaLink® Multifunction Printers

Use Case 1 – Automated Response to Threat

1 – MFP detects potential threat (e.g., unknown user, malicious act, polymorphic zero-day attack)

2 – MFP's whitelisting technology prevents attack and logs event

3 – MFP sends alert of event to McAfee® ePO

Normal Usage

- Known users
- Approved tasks

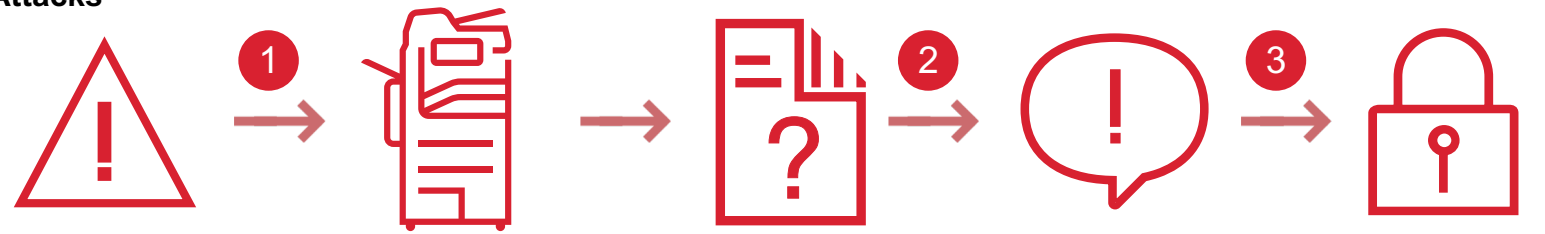
Xerox® Multifunction Printer (MFP)* with McAfee® Embedded Control

Known Files and Software

Policy Compliance
- Config attributes
- Software version
- Port settings

- Email
- Xerox® CentreWare® Web
- Xerox® Device Manager

Attacks



- Unknown users
- Malicious acts
- Polymorphic zero-day attacks

Xerox® Multifunction Printer (MFP)* with McAfee® Embedded Control

Unknown Files and Software Whitelisting technology allows only approved software to run

Alerts

McAfee™ ePolicy Orchestrator

* Xerox® ConnectKey® i-Series, WorkCentre® EC7836/7856 and AltaLink® Multifunction Printers

xerox™

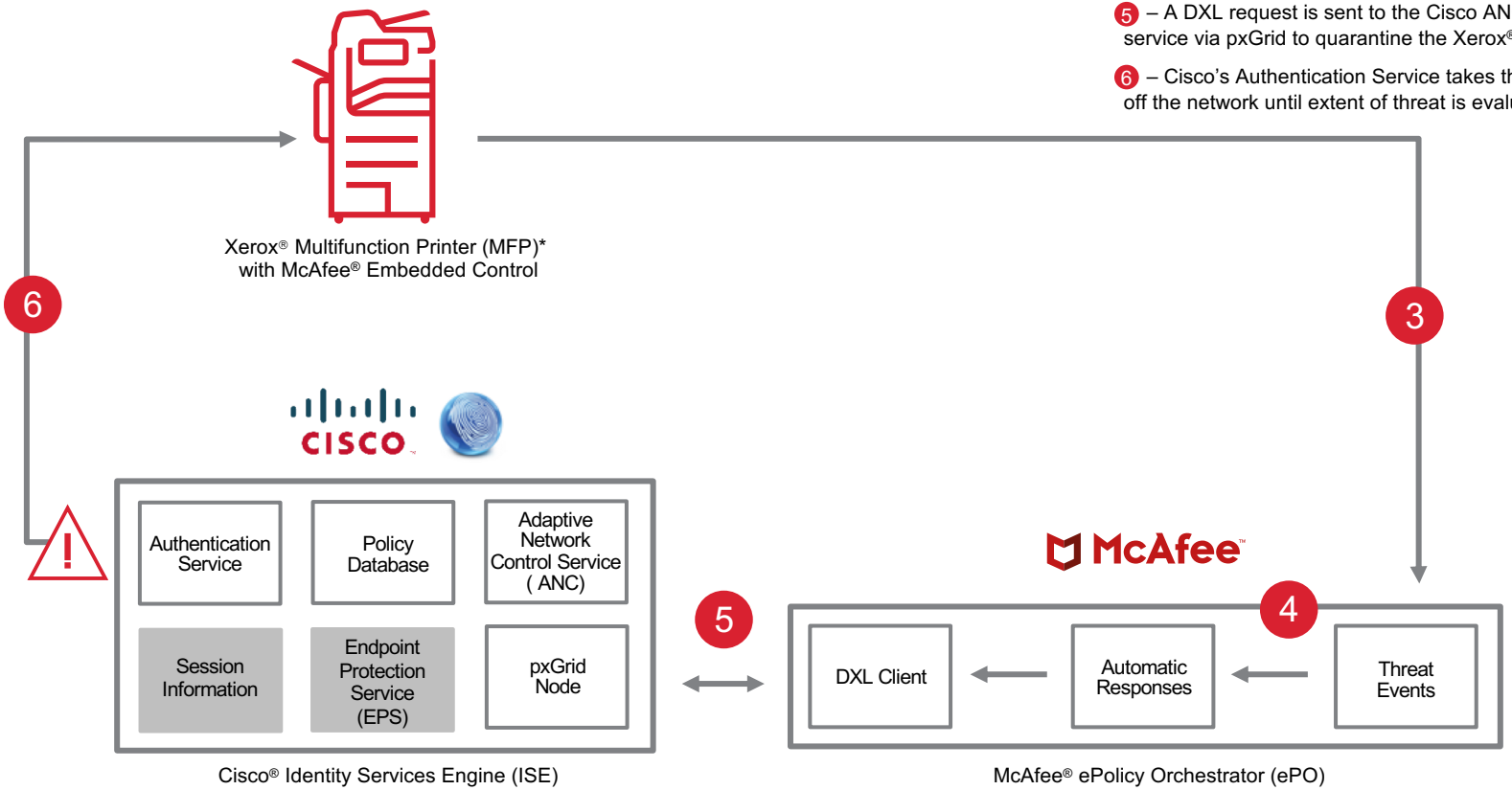
Use Case 1 – Automated Response to Threat (continued)

3 – MFP sends alert of event to McAfee® ePO

4 – ePO Automatic Response is triggered to DXL

5 – A DXL request is sent to the Cisco ANC service via pxGrid to quarantine the Xerox® MFP

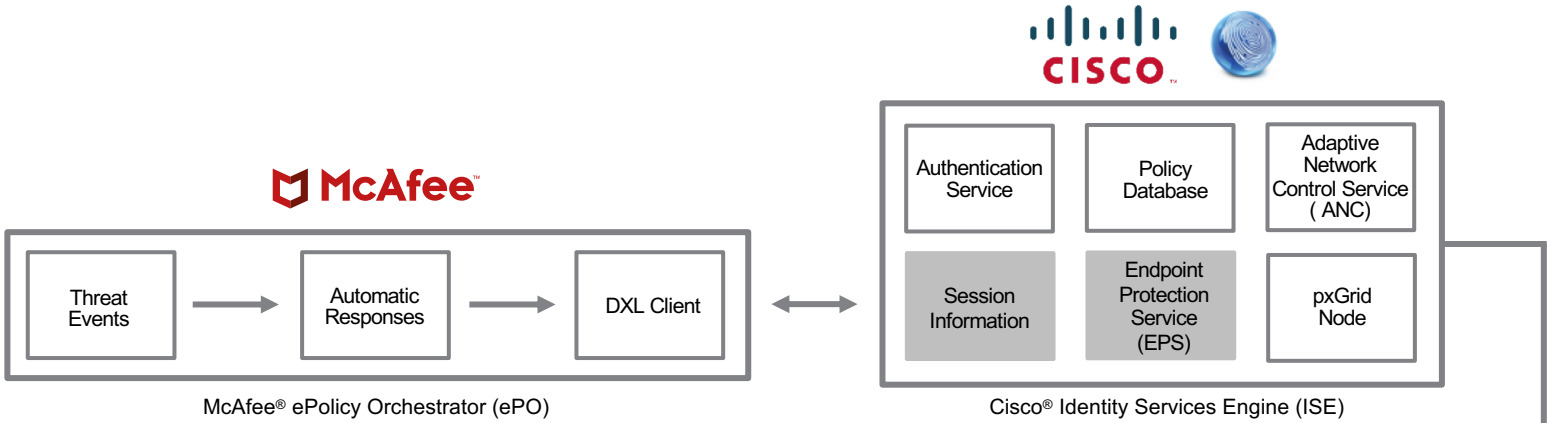
6 – Cisco's Authentication Service takes the MFP off the network until extent of threat is evaluated



* Xerox® ConnectKey® i-Series, WorkCentre® EC7836/7856 and AltaLink® Multifunction Printers

xerox™

Use Case 2 – Xerox® Devices Are Trusted Endpoints



- Cisco Policy Database recognizes that Xerox® printers are McAfee-protected.
- Xerox® printers are designated trusted endpoints.
- This allows security professionals to focus resources on less secure endpoints.

Xerox® Multifunction Printer (MFP)*
with McAfee® Embedded Control

* Xerox® ConnectKey® i-Series, WorkCentre® EC7836/7856 and AltaLink® Multifunction Printers

Behind-the-Scenes Enablers

- Xerox® MFP has McAfee® Agent & Embedded Control
- McAfee® DXL Brokers configured to bridge to Cisco® pxGrid
- Bidirectional communication between fabrics
    - Session notifications and ISE-related services
    - Adaptive Network Control (ANC) messages and related notifications
    - New Automatic Response within ePO that invokes ANC/EPS services (quarantine, etc.)
- pxGrid messages and services available to OpenDXL clients
- OpenDXL Cisco® pxGrid Python Client

Additional Resources

- Xerox® ConnectKey® State-of-the-Art Security: https://www.xerox.com/en-us/connectkey/printer-security
- Lock down printer security with McAfee: https://www.xerox.com/en-us/connectkey/insights/mcafee-security
- Xerox partnership with Cisco on security policy management and enforcement: https://www.xerox.com/en-us/connectkey/insights/cisco-ise-printers

xerox™

McAfee™ Together is power.

CISCO™

xerox™