McAfee
Together is power.

# Securing Critical Infrastructure and the Industrial Internet of Things

**The growing threat of cyberattacks to industrial targets is a major global concern and customers are demanding effective cybersecurity to assist and protect assets and people.**

## Critical Infrastructure Landscape

**70%**
of critical infrastructure organizations suffered breaches in the last year.[1]

**76%**
increase in Worldwide SCADA attacks from 2013 to 2014.[2]

**Standards**
and regulations are now government mandated (i.e. NERC CIP).[3]

## Real-World Breach

Worm enters nuclear program's system via USB stick.

Worm exploits multiple zero-day vulnerabilities of Windows Distributed Control Systems (DCS).

Worm hides from automated detection systems.

Once vendor-specific DCS is found the worm morphs and begins attack.

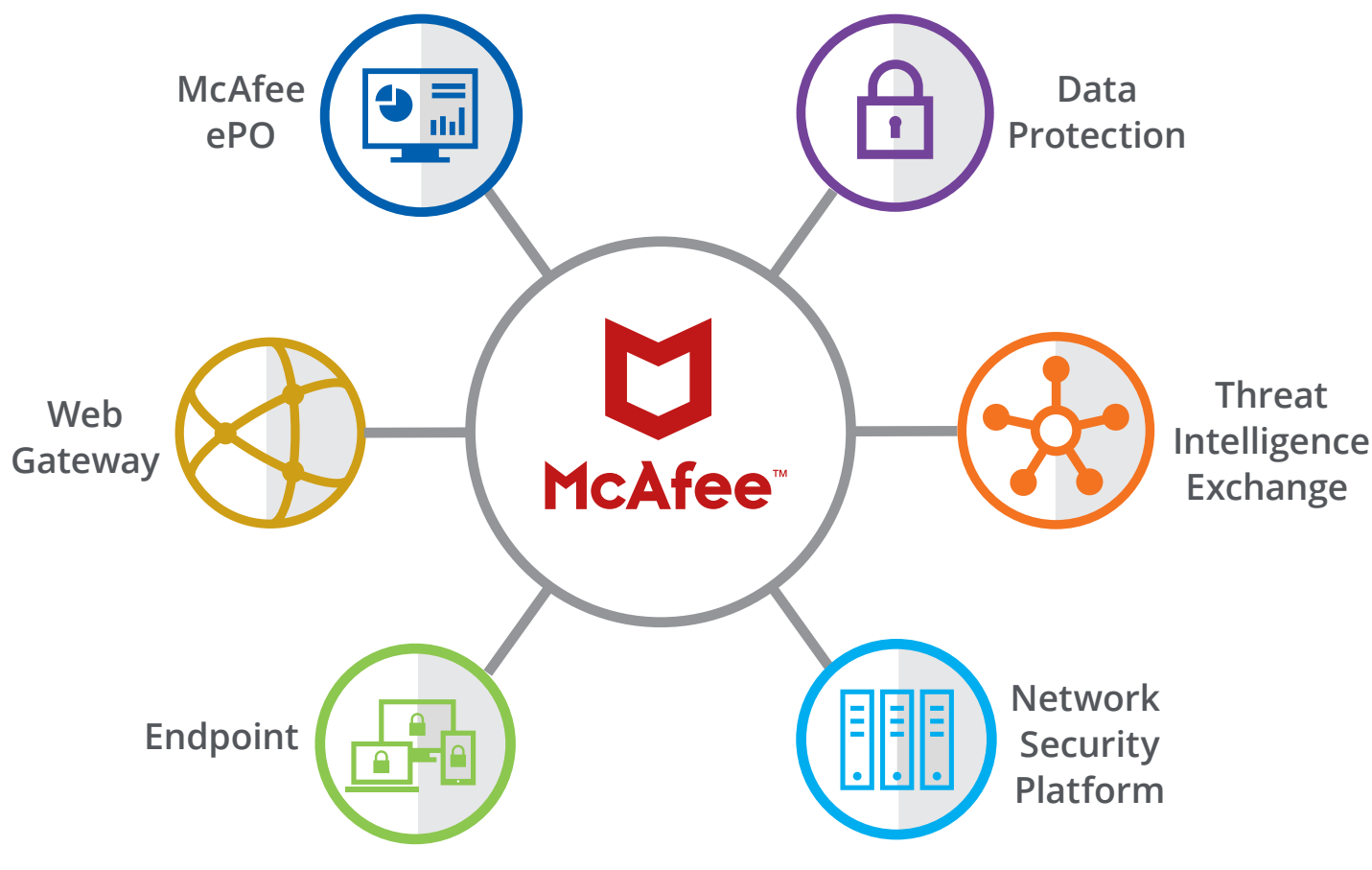
Worm targets system's logic controllers and spies on operations.

Worm gains control of centrifuges and provides false feedback to mask corruption in progress.

Worm destroys systems and damages machinery, causing over 6 countries to be affected.

## Security by Design

Protect industrial control systems, smart grids, sensors, monitors, robotic systems, communication, and network systems.




**Protect**
your system and data from exploits.

**Detect**
exploits of your systems and data.

**Correct**
damage to systems and lost or stolen data.

Learn more: www.mcafee.com/embedded

McAfee
Together is power.

1. Infosecurity Magazine, 2014, http://www.infosecurity-magazine.com/news/70-of-critical-infrastructure/
2. Dell Security Annual Threat Report, 2015, https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks/112241
3. North American Electric Reliability Corporation, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx