FORESCOUT

Phoenix Contact's mGuard Integration with eyeInspect™

Prevent undesired access and detect operational problems and threats for the strongest industrial cyber resilience

Highlights

- Phoenix Contact's mGuard firewalls restrict access to critical networks and systems only to authorized users and services.
- Forescout's passive OT network monitoring and situational awareness platform, eyeInspect (formerly SilentDefense), detects and reports operational problems and cybersecurity threats.
- The integration leads to industrial control system (ICS) networks which are more secure and resilient and to a significant reduction of unplanned downtime and problem mitigation costs.

PHOENIX CONTACT

The Challenge

Industry 4.0 has introduced significant changes in the way industrial networks are designed and managed. Legacy systems and protocols have been substituted by commercial-off-the-shelf (COTS), interconnected devices and standard communication technologies. Despite the strong business advantages, this trend has led to manufacturing networks which are more complex and highly heterogeneous and, as a result, are operating with an **increased risk of flaws**.

These flaws pave the way for cyber and operational incidents, as endured by a German steel factory in 2014[1], several car manufacturers in 2017[2], and many plant floors every day. With hundreds of devices from different vendors in the network, it has become more difficult to maintain **visibility** and **control** over who is accessing which systems and information, to track network and process activity, and to identify the source of malfunctions. Nevertheless, uptime and productivity goals need to be met, and in order to do so, the network and its devices need to be protected from unauthorized access and increasing external and internal threats.

Phoenix Contact's mGuard

As one of the worldwide market leaders and innovators in electrical engineering, electronics and automation, Phoenix Contact operates, among other things, its own center of excellence for cybersecurity located in Berlin. Based on long-standing expertise in this environment, the company provides customized products and network solutions that implement special industrial requirements. The mGuard series is the core of their security product line and includes a product family of industrial routers and firewalls.

Deployment and Operation

The mGuard products offer comprehensive routing features, a stateful inspection firewall with special extensions for industrial applications, Deep Packet Inspection (DPI) modules and VPN (Virtual Private Network) functionality. The security appliances are fanless and are available as compact DIN rail device, PCI(e) card, desktop or 19" device to fit all industrial applications. mGuard products are ideally suited to distributed protection and secure remote maintenance of production cells or individual machines. The security appliances allow the Defense-in-Depth concept, based on the international standards ISA 99 and IEC 62443, to be implemented. Thanks to the decentralized security concept, production plants are reliably protected against sabotage and the associated malfunctions in the production process.

Forescout's eyeInspect

eyeInspect is the most advanced and mature network monitoring and situational awareness platform for industrial networks. It leverages full Deep Packet Inspection (DPI) capabilities and a library of over **2,100 ICS-specific threat indicators** (Industrial Threat Library™) to analyze industrial protocol communications and alert in real-time for any threat to operational continuity. These threats include network connectivity problems, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials, advanced cyber attacks, and exploit attempts.

Deployment and Operation

eyeInspect is a fully passive solution, and therefore does not introduce any latency or have any impact on the monitored network and its devices. It is **deployed in a matter of hours** and provides immediate visibility into existing problems and threats. It leverages **patented anomaly detection technology** that enables users to automatically baseline network communications, minimizing configuration effort. eyeInspect's engines can be selectively enabled by the user to achieve full protection of the network and effective responses to existing and emerging threats.

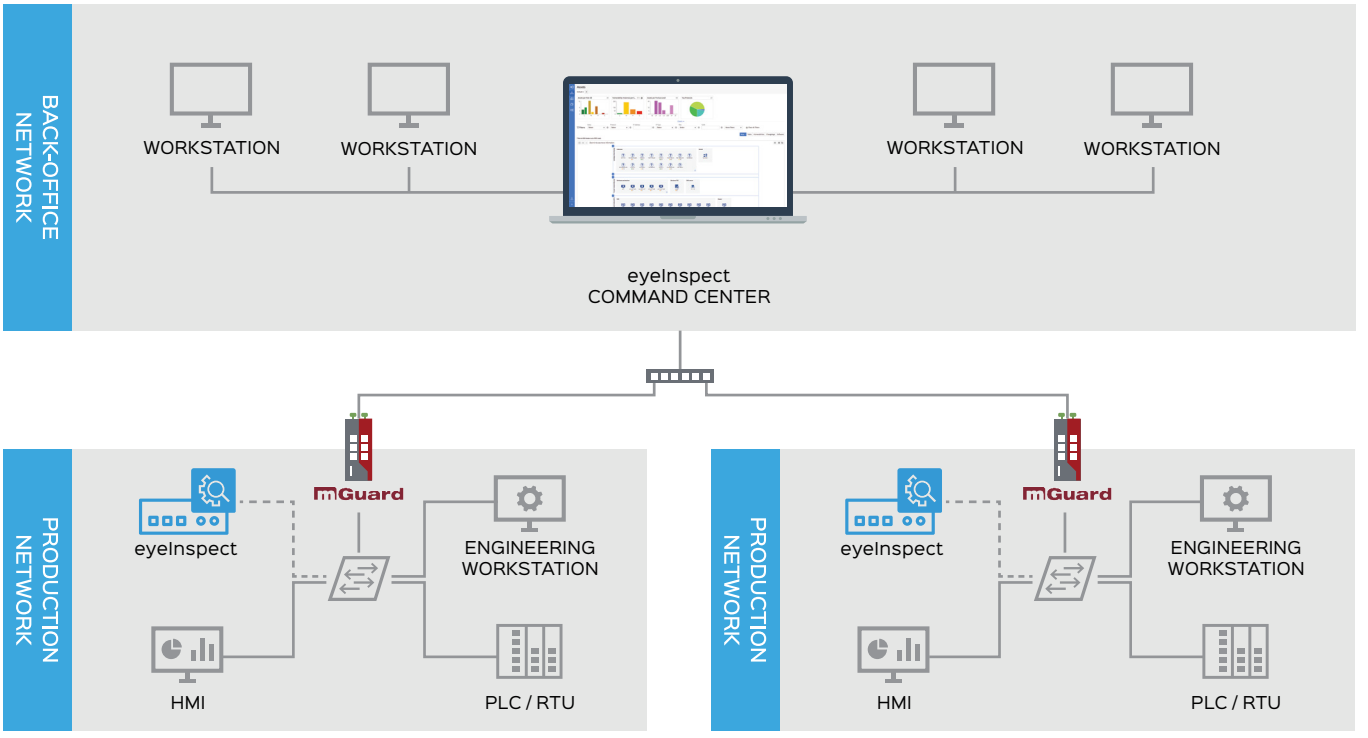
mGuard & eyeInspect

The integration of mGuard and eyeInspect makes industrial networks **more resilient** to cybersecurity threats and enables users to quickly identify and react to network malfunctions and misconfigurations. mGuard firewalls protect critical networks and devices from unauthorized access, blocking all incoming communications from illegitimate devices and preventing internal systems from connecting to undesired external servers. eyeInspect complements this protection with full visibility into advanced intrusion attempts and other potential causes of process disruption.

The self-configuring and advanced threat detection capabilities of eyeInspect bring additional benefits to the integration. eyeInspect's ability to automatically generate network baselines can be leveraged to speed up the initial mGuard configuration or to adjust firewall rules following process configuration changes. The integration can also block communications if new threats are detected and will temporarily prevent access to the network from a non-critical server that appears to be corrupted, for example.

Benefits of the Integration

- Full visibility of the OT network and its devices
- Protection of critical networks and devices from unauthorized access
- Minimized attack surface
- Faster firewall configuration setup and response to configuration changes
- Detection of networking, operational and security threats at their earliest stage
- Simplified root cause analysis of problems and incidents
- Dynamic response (blocking) to emerging threats and threat sources
- Reduction of problem resolution time and troubleshooting efforts and costs
- Maximized uptime and productivity
- Compliance with international standards and security best practices (e.g. IEC 62443 and the NIST Cybersecurity Framework)



[1] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[2] https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes/#1ab5c91c5e2b

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com