STEALTH™

EXECUTIVE OVERVIEW

Advanced Technology for Today's Global Threats

A Fresh Approach to Security in the Chemical Industry

Keep Critical Infrastructure Secure

Modernizing Security for Chemical Enterprises

To remain competitive, deliver the best products to the market securely, and meet increased regulatory requirements, the chemical processing industry must modernize. Unfortunately, these goals are often at odds with one another. Innovation and competitiveness rely on new technology that integrates business processes (real-time analytics, enterprise resource planning, supply chain automation) with production.

But many of the supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and programmable logic controllers (PLCs) and their related human-machine interface (HMI) and machine-to-machine (M2M) software leaves a potential hole in the overall security fabric, with significant risk for cyber-attacks.

The UK Office of Cyber Security and the Information Assurance estimated cybercrime to cost the UK Chemical industry £1.3Bn in 2015[1]. Reuters reported in March 2014 that at least 48 chemical and defense plants were attacked with a virus called 'Nitro.' Sources report the virus originated in China, and the targets were vulnerable to data theft, such as formulas and processing techniques.[2]

Today's attacks get in, move around, and then start doing damage. So how can chemical companies protect their facilities against advanced persistent threats (APT) and other sophisticated cyber-attacks while also reducing costs and improving agility? Unisys brings expertise and insight to address the critical security needs unique to the chemical processing industry.

[1] Detica report in partnership with the office of cyber security and information assurance in the cabinet office

[2] Finkle, Jim. 'Nitro' Attacks: China-Based Hacker Targeted Chemical Firms. Reuters, March 26, 2014.

Key Features

Stealth vs. Traditional

Security With No Limits

A Fresh Approach to Security

There is a better way to approach security, but it requires a fresh approach using Micro-segmentation. It allows enterprises to quickly and easily divide their physical networks into hundreds or thousands of logical micro networks, or microsegments, with access restricted based on identities. This new approach can help chemical enterprises:

Secure industrial control systems. By logically separating the industrial control systems and limiting the access based on secure identity management, Micro-segmentation can dramatically reduce the threat vector of chemical processing companies.

Go invisible. Make servers, devices, and other endpoints dark and undetectable to hackers and unauthorized users inside and outside your enterprise.

Secure data centers. Based on user identity, it lets enterprises tighten access control by focusing on user identity rather than physical devices, so security moves with the user and is easier to manage.

Secure data-in-motion. Protect sensitive data from potential compromise through point-to-point encryption.

Scale, adapt, and stay in compliance. Upgrade legacy systems, easily meet emerging needs and compliance requirements with agile, software-based

Stop Cyber Assaults Before They Happen

With its radically different approach seen through micro-segmentation, Unisys Stealth™ addresses the most critical security concerns. Stealth is designed to make SCADA/ICS and PLC endpoints at chemical processing plants on the command and control network invisible to unauthorized users and to secure data-in-motion across any network. Stealth enables definition of access control policies through roles and identities, rather than IP addresses, thus securing the access to industrial systems further to provide advanced protection and reduce the likelihood of future incidents.

By creating highly-trusted communities of interest (COI), Stealth is designed to allow only authorized users to access automated devices, applications, and systems critical to the chemical processing facility. In addition to strengthening mission-critical protection, chemical companies can reduce infrastructure costs by safely modernizing their industrial controls and software with one unified security solution. And as business requirements or regulatory mandates change, Stealth can deliver the agility enterprises need without requiring costly upgrades or extensive reconfiguration.

Don’t Be A Target.

Why Stealth Now?

Unisys Stealth is the innovative, mission-critical security that chemical companies need to help secure their operations via the following:

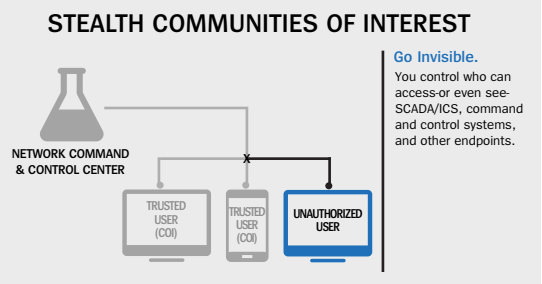
No operational disruption. Stealth works with existing firewall, intrusion detection, and other security systems with easy installation so you can upgrade your systems without compromising security.

Reduces risk. Make automated chemical processing controls such as ICS/SCADA endpoints and HMI systems invisible. Isolate critical systems from the rest of the enterprise. Tighten access control based on user identity. Protect data-in-motion over the industrial control network.

Facilitates compliance. Stealth can help achieve compliance with the Executive Order on Improving Critical Infrastructure Cybersecurity, and other regulatory requirements and recommendations. Stealth also helps reduce audit scope by segregating systems directly subject to compliance from the rest of the network.

Reduces costs. Protect the chemical processing enterprise system, including sensitive financial, production processes, formulas, and network data with one cost-effective solution.

Improves agility. Stealth allows for quick, easy changes to accommodate rapidly evolving business needs.



Stealth is What Innovative Security Looks Like

When it comes to critical infrastructure, there can be no compromise. Stealth can help move your organization from vulnerable to mission-critically secure. But don’t take our word for it. Read why Unisys Stealth’s advanced approach to security earned the Frost & Sullivan 2015 New Product Innovation Award for solving many of today’s most urgent security challenges faced by the world’s most important enterprises.

It’s time to try a fresh approach to your security, from a provider that’s already solved many of the problems you face today. To get more information or to schedule a discussion and demonstration, please contact us at stealth@unisys.com or click on https://unisyssecurity.com/unisys-stealth to get started.

STEALTH™

Printed in the United States of America 03/16 16-0102