TrapX Security, Inc., 3031 Tisch Way, 110 Plaza West
San Jose, CA 95128

+1–855–249–4453
www.trapx.com

CUSTOMER CASE STUDY

HOW PROCTER & GAMBLE TRANSFORMED ITS CYBER RESILIENCE PROGRAM

A Fortune 500 company and manufacturing leader partners with TrapX Security to enhance IT and OT (Operational Technology) cybersecurity

THE MANUFACTURING CYBERSECURITY CHALLENGE

The manufacturing space relies on a wide range of embedded and proprietary operating systems to maintain smooth operations at high volumes. Many of those systems were not designed with built-in security measures or are managed by third-parties. Such devices offer hackers a tempting attack surface to launch malicious threats against operations. Comprehensive security measures for the entire life cycle of these manufacturing tools and control systems present a challenge.

Traditional IT cybersecurity techniques are not always applicable in the OT space. Common practices in the IT space, such as frequent system updates, are unrealistic and ineffective in operational environments. This is particularly true in large distributed networks. These attacks on processes could disrupt manufacturing and distribution chains resulting in large losses. Procter & Gamble identified a need to innovate in order to passively protect the deployment and operation of deception practices.

TRAPX DECEPTIONGRID LED TO EFFECTIVE, EFFICIENT THREAT DETECTION AND PREVENTION

> *"With TrapX, our 12-hour days turned into 10-hour days because we were able to more efficiently monitor the network."*
>
> -Bill Fryberger
> Director of Enterprise Security Operations at Procter & Gamble

TrapX Security is a leader in deception-based cybersecurity technology. Automated solutions detect, analyze, and thwart threats in tandem with other forms of cyber-defense. The DeceptionGrid deploys turn-key traps disguised as authentic company assets. When disturbed, decoys instantly pinpoint malicious threats and provide actionable intelligence. This real-time breach protection is a proven solution for commercial and governmental organizations worldwide within top industries.

Using TrapX's DeceptionGrid, hundreds of traps were deployed throughout Procter & Gamble manufacturing sites. Centralized management of the deception platform made it easy to operate on a global scale. Decoys included simulated sites, workstations, servers, and devices. These deception artifacts stayed silent when undisturbed. The security team regularly rotated locations to gain visibility to different types of threats within both IT and OT environments, and TrapX produced actionable results through the identification and discovery of threats. TrapX DeceptionGrid provided visibility ranging from insider threats and malware to more advanced attackers.

Adjustability remained key as the TrapX platform recognized threats and misconfigurations. Compatibility with Windows, Linux, SCADA and network devices makes it a viable solution for the entire scope of operations. TrapX's nature allowed it to work without disrupting existing systems or draining resources. This underlying passivity is key to its short- and long-term success.

A CYBERSECURITY SOLUTION THAT LISTENS WITHOUT SPEAKING

> ***"Fidelity is probably the highest of the solutions we have seen; if you get an interaction then you know it's an event you are going to investigate. TrapX is the only tool Procter & Gamble found able to work in the manufacturing environment… it is really easy to deploy."***
>
> -Bill Fryberger
> Director of Enterprise Security Operations at Procter & Gamble

Procter & Gamble evaluated many options based on quality standards, the impact to existing technology and cost. Evaluating the TrapX DeceptionGrid, the company found the tool to be truly unobtrusive in even the most sensitive of environments. The approach of emulating devices in order to gain visibility into any malicious activity is by far the most effective in both IT and OT environments.

"Fidelity is probably the highest of the solutions we have seen; if you get an interaction then you know it's an event you are going to investigate," Fryberger said. "TrapX is the only tool Procter & Gamble found able to work in the manufacturing environment… it is really easy to deploy."

High accuracy and minimal false positives allowed a small team to monitor a large network. Specialists focused on real-time alerts and threats as reported by the TrapX DeceptionGrid. Additionally, implementation of traps, or emulated devices, lent insight into misconfigurations impacting efficiency. The capacity to detect, deceive, and adjust with precision made life easier for security, IT, and plant operations alike.

CHALLENGES IN THE MANUFACTURING ENVIRONMENT

- Legacy Operating Systems and embedded windows systems
- Critical devices lack security software and complex network topology
- Vendor support via VPN allows backdoor access to company assets

IMPACT OF CYBERATTACKS ON THE BUSINESS MODEL

- Critical processes fail or perform in an unexpected manner
- Manufacturing line downtime halts production
- Exposure of sensitive business logic and patented technology
- Damage to brand reputation

KEY BENEFITS OF TRAPX'S DECEPTIONGRID

- A low-cost deception-based security solution reduces reliance on more disruptive threat detection measures.
- Innovative cybersecurity techniques define, locate, and defend against the latest and most sophisticated attacks.
- Compatibility and ability to integrate itself with existing Procter & Gamble operations and defense systems.
- Improved detection minimizes Procter & Gamble financial loss due to the destruction or theft of vital corporate assets.
- An advanced real-time analysis enables the cybersecurity operation center to take immediate action against threats.
- Passivity in the manufacturing environment alleviates plant operations reluctance to adopt new technology.