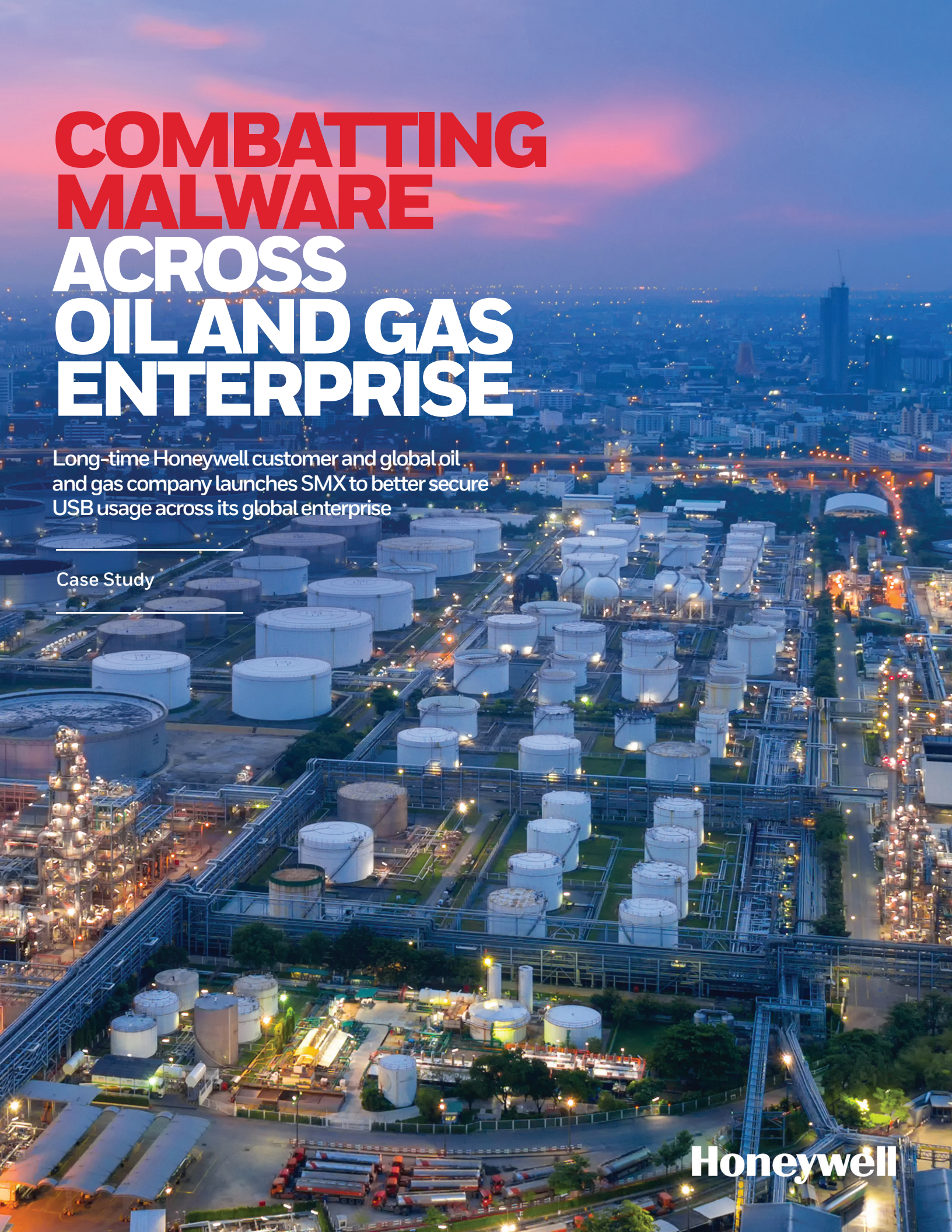

COMBATTING MALWARE ACROSS OIL AND GAS ENTERPRISE

Long-time Honeywell customer and global oil and gas company launches SMX to better secure USB usage across its global enterprise

Case Study

Honeywell

CONSISTENTLY, THE TOP THREAT VECTOR

Look no further than the 2021 ransomware attack on the Colonial Pipeline for proof that cybercriminals have the energy industry in their crosshairs. No wonder most oil and gas companies are placing unprecedented emphasis on protecting operational technology (OT) systems that are so critical.

USBs are one of the top threat vectors in the industrial space. Nevertheless, they remain the principal vehicle for updating and maintaining process control network configurations.

USBs are ubiquitous, low cost and nearly impossible to control with a corporate policy alone. To efficiently manage secure removable media and USB port usage, technology is advised as the primary tool.

The oil and gas industry needs a solution that enables the secure transfer of files using removable media without disrupting operations. One of Honeywell's long-time customers came to this realization.

MINIMIZE RISK AND ISOLATE MALWARE

The global oil and gas company trusted Honeywell cybersecurity engineers to help secure the use of USBs across multiple sites, globally.

The customer's overall goal was to deploy a solution that improves the security for anyone entering their facilities using USBs.

The rugged SMX solution also needed to have an outbound internet connection that was not connected to the company's industrial control network. Secondly, the customer required the solution to be deployed using centralized software distribution capabilities at an enterprise level.

SINGLE SOLUTION ENABLES BETTER THREAT PROTECTION

Honeywell cybersecurity engineers proposed and trialed Honeywell's Secure Media Exchange (SMX) solution.

This unique solution leverages multiple detection techniques to provide optimal threat protection for USB applications.

The Honeywell team tested the company's own operational technology network. SMX outperformed the customer's previous solution, and successfully detected and isolated a simulated malware infection. After determining SMX met all its requirements and offered a file transfer capability, the company stakeholders agreed to install SMX across multiple industrial sites.

The oil and gas enterprise was impressed with the ease of installation and the SMX's user-friendly customer interface, which made it simple for them to integrate the solution into their existing cybersecurity program.

SMX provided the oil and gas customer the capability to scan removable media, help identify advanced hardware-based threats and help prevent unchecked devices from using USB ports while keeping ports active for authorized devices.

When a user at one of the oil and gas company's site checks out, the device is checked again for anomalies and logging information is recorded for forensics purposes. During these security checks, SMX uses a powerful combination of intelligence feeds and multiple types of industrial threat detection techniques via Honeywell's Cybersecurity Global Analysis, Research and Defense (GARD) threat research team. GARD also uses proactive threat research, mining, hunting, and other techniques to help protect against current and emerging USB-born threats and detect targeted OT threats early.

The intuitive customer interface, transfer capability and threat detection capabilities of SMX convinced the oil and gas customer to deploy SMX units across the enterprise.

THE FUTURE IS WHAT WE MAKE IT

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.ai

Case Study | Rev 1 | 05/2022

Honeywell