Honeywell

THE POWER OF CONNECTED

Connected Plant

# PLACING A VALUE ON INDUSTRIAL CYBER SECURITY

Honeywell Open VEP – Executing projects faster and at lower cost while protecting your company's knowledge in the digital world

Authored by **Chad McGraw**, Honeywell Process Solutions

White Paper

## Abstract

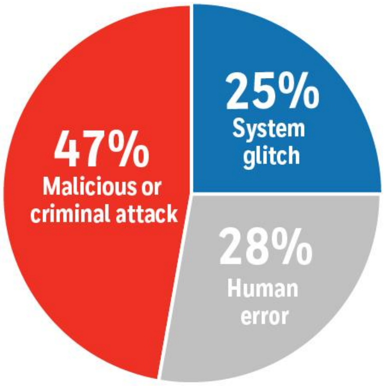
Honeywell's Open Virtual Engineering Platform (Open VEP) service provides a secure, centrally hosted cloud environment to implement an off-process engineering and validation system. With Open VEP, testing and project execution can be done from anywhere in the world, on an automation system at any configuration and release. This whitepaper explains how it also ensures the absolute security of your intellectual property.

# Contents

## Introduction

Companies are spending more than ever to protect their customer relationships and intellectual property. Although most studies don't consider the value of intellectual property, there are many studies available which help us understand how common data breaches are beyond the big events which hit our evening news every month. The 2017 Cost of Data Breach Study by Ponemon Institute (using research sponsored by IBM Security and derived from interviews with 419 companies who reported a data breach in 2016 and agreed to share details) showed an average cost of $3.6 million per breach. The cause of these breaches was nearly evenly split between internal (Human error / System glitch) and external (Malicious / Criminal Attacks) causes.

*"The 2017 Cost of Data Breach Study by Ponemon Institute showed an average cost of $3.6 million per breach"*



**Distribution of the benchmark sample by the root cause of the data breach`**

It is a testament to the creativity of those performing malicious and criminal attacks that it is still taking over 6 months to even recognize a data breach has taken place. As a statistical mean, there were just as many instances which took longer (up to 18 months) as shorter. Once identified, it took another 2 months (mean time) to stop further losses (ranging up to another 6 months).

The top factors to reduce the cost of a data breach include an identified incident response team, extensive use of encryption, employee training, Business Continuity Management (BCM) involvement, participation in threat sharing, and use of security analytics. Find more at www.ponemon.org .

## Honeywell Industrial Cyber Security

Nobody wants to be part of a data breach incident. Honeywell is the leading provider of industrial cyber security solutions that protect the availability, safety and reliability of industrial facilities and help securely deploy IIoT technologies. Businesses all over the world partner with Honeywell to address cyber security holistically and improve their cyber security posture with advanced technology, backed by continuous innovation and investment.

Honeywell's Industrial Cyber Security group has been working with our customers to protect their intellectual property for over a decade. On August 1, 2017, Honeywell announced it had completed its acquisition of Nextnine Ltd., a leading provider of industrial cyber security solutions. Honeywell and other industrial controls providers have been using their solutions for years to protect customer assets. This move further strengthens Honeywell's ability to provide complete multi-vendor, multi-site secure remote access, monitoring and support to protect industrial control systems and critical infrastructure against a growing threat of cyber-attacks. More information available at www.nextnine.com

Together, the new organization provides enhanced Managed Security Services (MSS) for Industrial Cyber Security with improved asset inventory management, security compliance and policy management, continuous monitoring and alerting, and integration with Honeywell's Risk Manager and Advanced Threat Intelligence Exchange (ATIX). In short, Honeywell knows Cyber Security and we build it into our solutions from the ground up.

## Honeywell Virtual Engineering Platform (VEP)

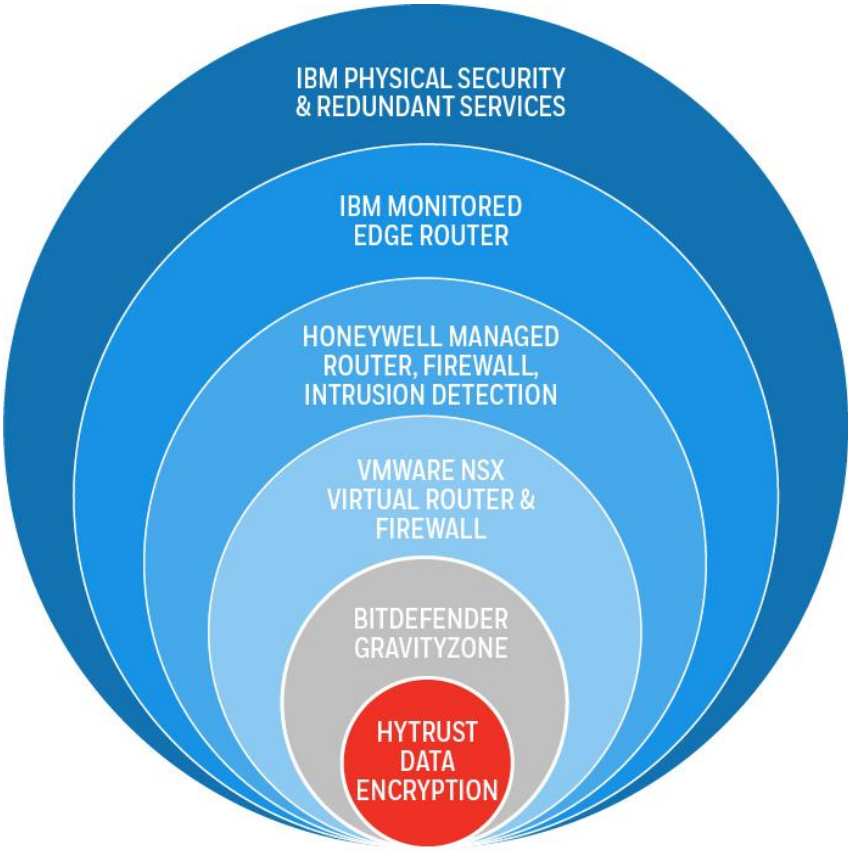
Honeywell has been deploying customer projects from an internally hosted platform since 2012. This VEP has been an internal tool which provided our engineering teams ready access to virtualized servers for their projects. Project managers simply request necessary number of Virtual Machines (VMs) and they are made available for use within hours. Projects frequently include 10-15 VMs but larger projects may use several hundred VMs. Over 500 projects have been completely developed and tested in this virtual environment with customers invited onto the system for witness testing prior to deployments. As customers became more familiar with our secret to fast project deployment, they started asking for their own permanent access.

Administrative access to Honeywell infrastructure may not be provided to Non-Honeywell parties. To allow access to a VEP environment to our customers the platform had to be replicated in a secure public location.

## Open Virtual Engineering Platform

The better solution was to design a new space off the Honeywell network. This “Open” Virtual Engineering Platform (Open VEP) would feature all we had learned in our first five years of internal use but add customer friendly features like additional layers of third party security, direct and faster internet connectivity through 10+ carriers, and more robust utilities and physical security typically available only in a dedicated data center run by a professional team and backed by a company who needs to protect their brand as much as you do. That’s just the outer security layers. Honeywell adds our own completely independent security features inside of this protected environment including a Honeywell managed firewall protecting all user systems, Bitdefender GravityZone endpoint security for VMWare, and an additional VMWare NSX soft firewall between each customer system, and finally full HyTrust encryption of data of each system with customer managed encryption key.

This multi-layer approach is referred to as “Defense-in-Depth” within the IT security industry and has been proven to be highly effective in stopping unauthorized access. It provides a variety of challenges to the would-be thief while providing time and traffic for the intrusion detection systems to identify and track back to the source. If they are successful in getting all the way to the internally protected data, they find Strong AES 256-bit encrypted data with no way to read it.

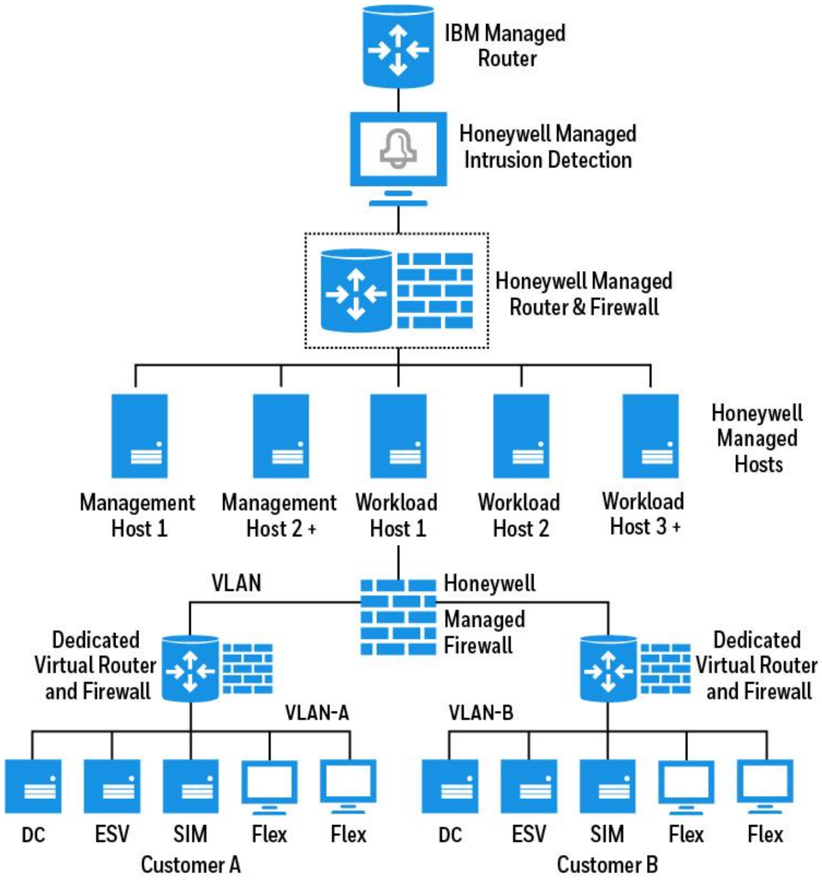

IBM PHYSICAL SECURITY & REDUNDANT SERVICES
IBM MONITORED EDGE ROUTER
HONEYWELL MANAGED ROUTER, FIREWALL, INTRUSION DETECTION
VMWARE NSX VIRTUAL ROUTER & FIREWALL
BITDEFENDER GRAVITYZONE
HYTRUST DATA ENCRYPTION

**Defense in Depth**

The soft firewall protecting the customer’s system and data encryption not only provide protection from external threats but protects intellectual property within each system from neighboring systems within the protected environment or even the administrator through compartmentalization with customer managed encryption key (FIPS 140-2 compliant Level 1 encryption key management). This assures nobody has access to the data without the knowledge and permission of the end user customer. HyTrust Cloud Security Policy Framework is a common and robust solution to a wide range of security and compliance challenges from insider threats and data breaches to an ever-expanding security regulatory landscape.

## Open VEP Secure Design Overview

Open VEP is built on the IBM Cloud platform with Honeywell dedicated firewall, networking, and servers utilizing Honeywell IP addresses. All accounts with access to the hardware are managed by Honeywell and no access is shared with other IBM tenants. The simplified diagram provides an overview of the architecture.



## Physical Security and Compliance Standards

IBM Cloud prioritizes the physical security of all data center facilities by incorporating strict security requirements in its standardized approach to building facilities around the world.

IBM Cloud's security management is aligned with U.S. government standards based on the NIST 800-53 Rev 4 framework, a catalog of security and privacy controls defined for U.S. federal government information systems. IBM Cloud maintains SOC 2 Type II reporting compliance for every data center. SOC 2 reports are audits against controls covering security, availability and process integrity. IBM Cloud's data centers are also monitored around the clock for both network and on-site security. A copy of IBM Cloud's SOC 2 audit is available to Open VEP customers on demand.

## Network Security

Three physical layers of security have been deployed in the Open VEP architecture. At the top of the stack is an IBM monitored router. Second, there is an intrusion detection appliance monitoring all Open VEP traffic. Third is a router and firewall appliance. The second and third layers are managed and monitored by the Honeywell Industrial Cyber Security Solutions team.

In addition to the three infrastructure layers, each individual Open VEP tenant environment is protected with its own Virtual Router and firewall. The individual firewall allows firewall settings to match the needs of each Open VEP environment. This ensures each individual environment in Open VEP is logically segregated.

There are no communication paths from Virtual Machines in one Open VEP environment to another. Virtual Local Area Networks (VLANs) are used to isolate traffic at outer and inner network levels, all the way down to the VLAN which provides secure interaction between the multiple VMs which make up a specific customer's system (typically 5 or more VM's).

VMWare's vAPP Edge Gateway Virtual Router is used to provide user flexibility by allowing duplicate copies of VMs using the same IP address, similar to Network Address Translation (NAT) functionality. For instance, a larger system may be constructed for testing purposes using multiple instances of the same simulated C300 configuration.

## Controlled Network Access

Each Open VEP environment has limited access by default. While this can be modified to suit the needs of each environment; by default, only port 443 is enabled inbound and most external IP addresses are blocked outbound from the VMs. Real-world controllers and I/O may be added to a customer's system for testing purposes using Honeywell provided VPN firewall and gateway preconfigured to securely connect to your system within the Open VEP environment.

## Open VEP Host Configuration Compliance

Each Open VEP host is managed by HyTrust Cloud Control. HyTrust ensures that each host is configured to the recommended guidelines. Each host is scanned daily and a compliance history is maintained.

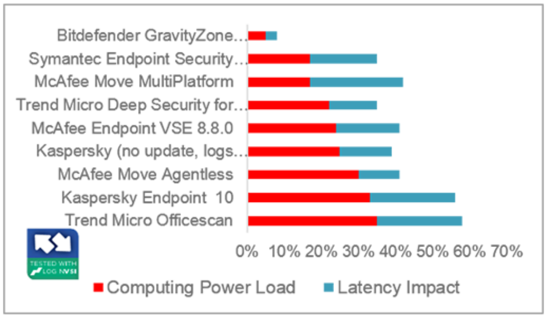
The HyTrust CloudControl policy engine ensures that no single administrator may perform critical or disruptive actions as defined by our policies such as to delete key virtual machines.

HyTrust Root Password Vaulting keeps hosts secure through a Root Password checkout process with a password valid for hours not months. Each password checkout is logged.

All hosts and management virtual machines are kept up to date via automated patching tools. Patch reports are reviewed on a periodic basis.

## Open VEP Malware Detection

Open VEP utilizes BitDefender GravityZone for VM anti-malware protection. GravityZone works directly at the hypervisor level and requires no agent at the OS level. Every Virtual Machine is automatically scanned for Malware. The host level architecture ensures that VM performance is not impacted with a peak Host CPU load of less than 2% and eliminates the possibility of AV Storms. The security gap that occurs during boot of an OS level protected machine is also eliminated. Virtual machines are protected from the instant that they are started. LoginVSI tests show Bitdefender's optimized security has the smallest impact on computing resources, while Bitdefender Endpoint Security has won the AV-Test Best Performance Award each of the last three years.



## Open VEP Virtual Machine Encryption

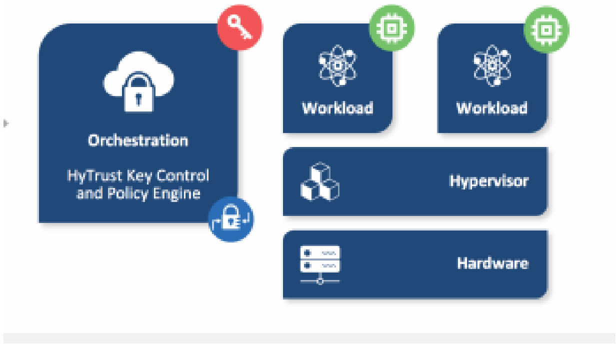
There are multiple layers of protection in Open VEP. Each measure increases the security of workloads hosted within the environment.

HyTrust DataControl has been deployed to ensure that in the unlikely event that the safeguards fail and a malicious user gets access to the system they will not be able to access any data contained within an Open VEP VM. HyTrust also protects against any bad actor with privileged access to Open VEP.

Each Open VEP Virtual machine is encrypted during the deployment process. This encryption is at the virtual disk level and is managed by a client installed at the individual OS level. Honeywell's customer controls the encryption key so not even Honeywell has access to the data installed on the system.

A portal account is provided for each set of virtual machines. Users may log into the HyTrust Orchestration server to manage and monitor the encryption status of all machines in their environment.

All access to the VM set is managed only by the customer.



## Conclusion

Honeywell's Industrial Cyber Security Solutions team, IT organization, and solution architecture specialists worked together to develop Open VEP to provide fast, convenient anywhere access to our best-in-class software while maintaining absolute security of your intellectual property. The solution provides high availability for 24/7/365 access for your people to develop Experion PKS interfaces and controls, provide simulation, validate, and train your people to perform their best. Open VEP is just another example of how Honeywell delivers high quality solutions to solve real problems while giving you the power to get there before your competition.

**For More Information**

To learn more about Open VEP, visit
www.honeywellprocess.com/OpenVEP
or contact your Honeywell Account Manager.

**Honeywell Process Solutions**

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

WP-18-02-ENG
April 2018

Honeywell