Bitdefender

SECURITY AT THE SPEED OF DEVOPS

Bitdefender® Endpoint Security Tools for Pivotal® Cloud Foundry

SPEED OR SECURITY?

Pivotal® Cloud Foundry (PCF) lets you rapidly create and automatically deploy cloud-native applications on the infrastructure of your choice, improving operational efficiency and accelerating time-to-value. But how do you protect those applications against cyberattacks? How do you fulfill your part of the shared responsibility model, in which the cloud provider secures everything "from concrete to hypervisor" and the customer protects the workloads that run in that cloud? How do you ensure your organization complies with PCI DSS, HIPAA, Gramm-Leach-Bliley Act (GLBA), GDPR, and other regulations stipulating endpoint security as a safeguard? Assuming you secure virtual machine (VM) instances that host your applications, you may be doing one of the following:

- Adding open-source antivirus (AV) to your BOSH deployments. This approach preserves the efficiency and agility of PCF (even though additional scripting may be needed to enable automatic updating required by regulatory standards), but it provides limited protection and complicates auditability. Open-source AV lacks many of the cutting-edge security technologies of modern commercial solutions and does not readily provide the centralized visibility and reporting capabilities required to prove compliance

- Bolting on commercial endpoint security after deployment. This approach presents two problems. First, it does not fit with the immutable infrastructure paradigm where no changes are allowed once a VM goes into production (i.e., security must be provisioned at the time of VM orchestration). Second, even though you may be getting enterprise-grade security, you do sacrifice PCF's all-in-one automation for a two-step process that may involve manual deployment of the endpoint agent into thousands of VMs. Consequently, the time and cost of application delivery increase.

THE BETTER WAY

The Bitdefender® Endpoint Security Tools (BEST) Tile for PCF is the first enterprise-grade solution that helps you prevent breaches and ensure compliance while maintaining the speed and efficiency of infrastructure provisioning and application delivery.

With the BEST Tile for PCF, you can automatically incorporate Bitdefender's award-winning endpoint security into BOSH-built VM instances when they are created. With VMs born secured, you can achieve the following:

- Maximize the operational efficiency and agility benefits of PCF by eliminating the time and effort required to manually deploy the agent and apply security policies after the fact

- Protect datacenter and cloud VMs from advanced cyberattacks with layered next-generation security from Bitdefender, a Gartner Representative Vendor of Cloud-Workload Protection Platforms, a Forrester® Wave Leader in Endpoint Security Suites and the winner of the AV Comparatives® Outstanding Security Product Award

- Streamline compliance with regulatory standards calling for an antimalware solution by always creating VMs with security built-in.

Bitdefender machine learning models use 40,000 static and dynamic features.

They are continuously trained on trillions of samples from hundreds of millions of endpoints globally.

This ensures Bitdefender effectiveness in malware detection and minimizes false positives.

B

HOW IT WORKS

You can deploy Bitdefender Endpoint Security Tools (BEST) for PCF by following the BOSH-orchestrated process summarized in the diagram below. BEST works in tandem with the unified GravityZone Management Console, which provides BEST with licenses, security policies, updates, and upgrades while ingesting security events it reports. The GravityZone Console is deployed separately from BEST - either on premises by the customer or in the cloud by Bitdefender.

BITDEFENDER ENDPOINT SECURITY TOOLS (BEST)
FOR PIVOTAL CLOUD FOUNDRY
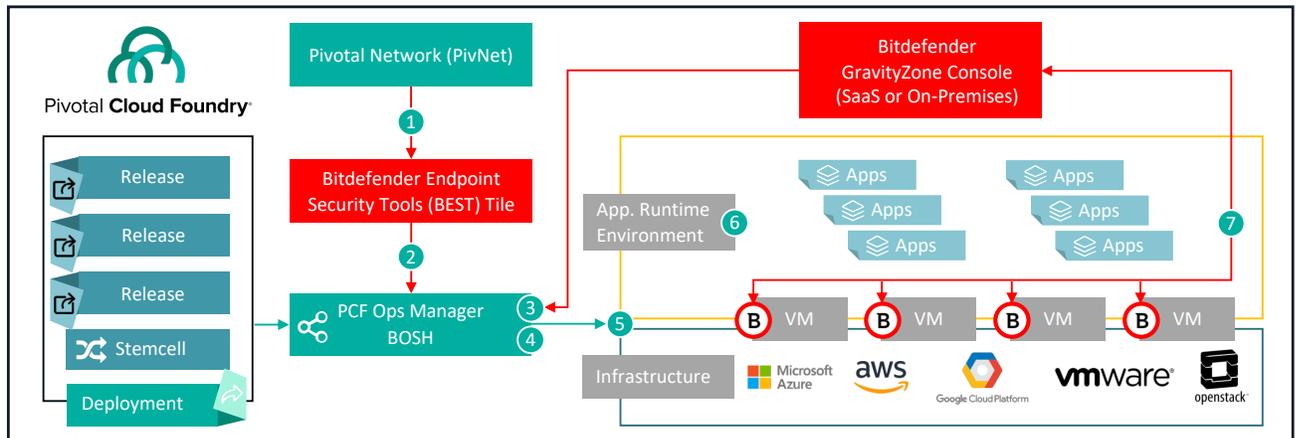
1 PCF Operator downloads BEST Tile from Pivotal Network (PivNet)

2 Operator imports BEST Tile into PCF Ops Manager's Installation Dashboard

3 Operator configures BEST by specifying URLs for OS-appropriate (Windows or Linux) BEST packages created in GravityZone Console

4 Operator specifies installation targets by Stemcell OS, deployment, job/release name, etc., and applies configuration changes

5 Operator adds BEST package to BOSH deployment manifest

6 *bosh –d <name> deploy manifest.yml* installs BEST into new or active deployment

7 BEST receives security policies from and reports security events to GravityZone. The runtime environment is now protected

SOLUTION FEATURES: BITDEFENDER FOR PIVOTAL CLOUD FOUNDRY

Management

Deployment Automation

Ensures BOSH automatically deploys BEST at the time of VM instantiation

Single-Console Administration

Allows single-pane-of-glass security management, ubiquitous visibility and consistent policy enforcement across heterogeneous datacenter and cloud infrastructure

Infrastructure-Management Tool Integration

Enables automatic application of security policies at scale, and security license recovery from decommissioned VMs in VMware® vSphere, AWS® EC2 and Microsoft® Azure environments

SIEM Connectivity

Allows automatic submission of security events for analysis to Splunk and other SIEM platforms (via Syslog)

B

Security

Layered next-generation endpoint security delivering, among others, the following advanced capabilities*:

Application Control

Provides both whitelisting ("default deny") and blacklisting capabilities to restrict the range of applications allowed to run in a VM.

Integrated Patch Management Add-On

Automatically discovers and characterizes vulnerabilities and the widest range of patches for OSs, applications and golden images.

Dynamic Machine Learning (Local and Cloud-Based)

Leverages proprietary models trained in URL filtering and file analysis on 500 million endpoint-sensors and trillions of samples to maximize efficacy and minimize false positives.

HyperDetect Tunable Machine Learning

Allows administrators to adjust aggressiveness of threat-detection to suit the context and risk profile of their organization and detect high-probability, high-impact attacks while minimizing false positives on lower-risk threats.

Sandbox Analyzer

Automatically submits suspicious files from VMs to a network sandbox based in the cloud or on premises for detonation and behavioral analysis.

Process Inspector

Continuously monitors and scores running processes and system events and tags suspicious activities to provide proactive, dynamic detection and remediation of unknown threats.

Anti-Exploit

Detects exploitation methods and protects the memory space of browsers, document viewers, media players and office applications.

* - Some of these features may not be available for Linux. Please consult your Bitdefender representative or inquire online at https://www. bitdefender.com/business/inquire.

WHY BITDEFENDER?

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries.

Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions.

Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

ENGAGE US

Get the BEST Tile for PCF: https://network.pivotal.io/products/bitdefender-endpoint

Call: (US) 800-388-8062

Request trial: bitdefender.com/business/free-trials/2596

Learn more: bitdefender.com/sve

Bitdefender®

w w w . b i t d e f e n d e r . c o m