Solution Brief

Sustainable Security Advantage with Cloud Workload Discovery

Discover, assess, and remediate cloud threats

Organizations have a diverse IT infrastructure to protect. On average, they leverage six clouds: three public clouds and three private clouds.[1] At the same time, they have complex IT environments that involve many users, an ever-changing number of endpoints, on-premises workloads, and an enormous amount of data flowing in and out of the organization. On top of this, IT security needs are also in constant flux.

CIO/CISOs, security operations, IT, and DevOps need to create a sustainable advantage against advanced attacks, zero-day malware, ransomware, and other threats. They also need to reduce the total cost of ownership associated with security and reduce the time to identify, prevent, and remediate threats. These goals require a strong cybersecurity defense. Cloud Workload Discovery provides organizations with a sustainable advantage while optimizing their security investment.

Cloud security is a shared responsibility. Cloud providers secure the infrastructure, and their customers need to secure workloads and configure platform security. Cloud Workload Discovery works with leading cloud platforms—including VMware, OpenStack, Amazon Web Services (AWS) and Microsoft Azure—for complete protection. It provides end-to-end visibility into all workloads and their underlying platforms. Insights into weak security controls, unsafe firewall and encryption settings, and indicators of compromise (IoCs) lead to faster detection, while the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console and DevOps tools enable faster remediation.

Using Cloud Workload Discovery, organizations can:

- Assess end-to-end security posture (workloads and platforms)
- Monitor and protect workloads across all private and public clouds
- Maintain regulatory compliance

intel Security

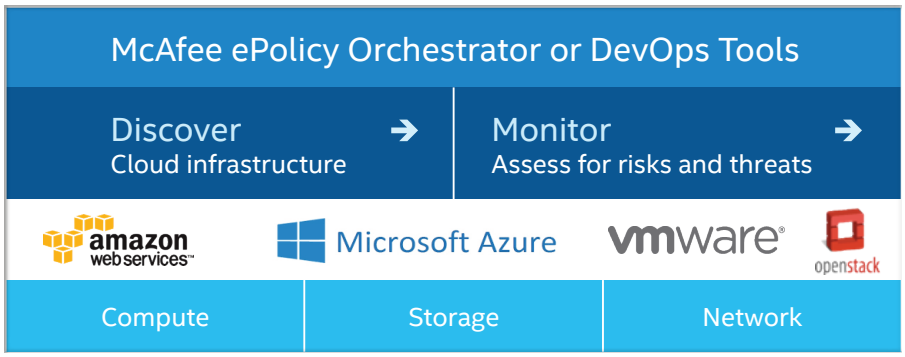

Figure 1. Derive a sustainable advantage with Cloud Workload Discovery.

Cloud Workload Discovery Enhances a Holistic Security Approach

Integrating Cloud Workload Discovery with other security solutions is crucial for building a strong defense in complex IT environments. Cloud Workload Discovery integrates with the McAfee ePO management console, empowering organizations to have effective controls across all their physical, virtual, and cloud environments. With this integration, security administrators can use a single management platform with streamlined workflows to address threat alerts and enforce policies, reducing the time to identify and remediate security issues.

Secure Posture Assessment and Compliance Across Multiple Clouds

Dynamic cloud environments are different from traditional on-premises environments. Deep real-time visibility into cloud workloads and their underlying platforms allows organizations to easily detect security gaps and threats and apply required solutions.

Cloud Workload Discovery allows administrators to have agentless security controls over multiple cloud infrastructures with thousands of cloud workloads. Organizations can leverage this powerful feature to discover and monitor threats, virtual networks, templates, and workloads.

Cloud Workload Discovery offers an innovative dashboard experience to maintain security compliance in the cloud. An end-to-end view of granular details such as DNS name, IP address, instance name, instance ID, and virtual network ID of workloads identify the exact location of threats for faster remediation.

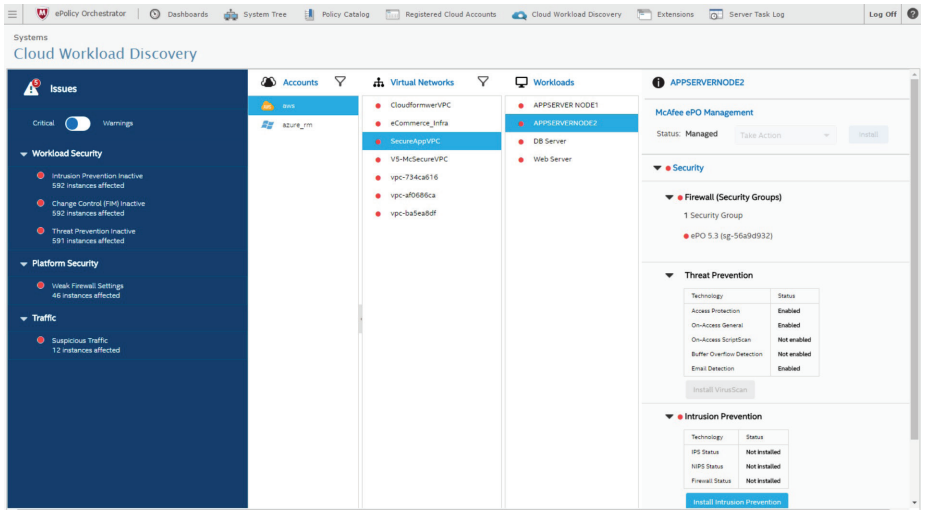

Figure 2. Cloud Workload Discovery provides an end-to-end view for multiple clouds.

Detect and Remediate Threats Faster

Detecting and correcting critical security issues as quickly as possible can reduce the impact of a breach. Cloud Workload Discovery leverages McAfee Global Threat Intelligence, a cloud-based service that provides reputation information on millions of IPs. Using this information, Cloud Workload Discovery highlights suspicious traffic and external IPs that are connected to cloud workloads. This allows administrators to quickly block suspicious traffic in a few clicks. Finer details regarding traffic—blocked, inbound, and outbound connections to a workload and blocked or allowed traffic (north-south and east-west)—give administrators granular control over their cloud infrastructure. Security alerts and identified threats are shared across all Intel Security solutions to build an intelligent security defense for an organization's entire IT environment.

Using Cloud Workload Discovery, IT teams can harden issues related to cloud firewall (security group) to reduce the time to resolve hundreds or thousands of cloud firewall related issues. With one management platform that includes multiple dashboards, IT professionals can edit or detach a large number of security group policies while addressing other security problems that involve numerous endpoints, users, and extensive data.

Sustainable Advantage in a Connected IT Security Architecture

The value of Cloud Workload Discovery is not just restricted to clouds. Its true value can be gauged in a complex IT architecture with thousands of users, endpoints, applications, and workloads and millions of bytes of data flowing across the network. When an organization adopts one or more clouds, having granular visibility of cloud workloads and threats and correlating security alerts across multiple layers of protection across the entire IT infrastructure is critical. Automated security intervention helps defend businesses from the most advanced attacks imaginable. Because Cloud Workload Discovery integrates security, enterprises obtain a sustainable advantage against threats and confidence to adopt multiple clouds.

Learn More

There are three Cloud Workload Discovery options to meet your cloud security requirements:

- Cloud Workload Discovery for hybrid cloud (VMware, OpenStack, AWS and Microsoft Azure) is available in McAfee Server Security Suite Advanced and McAfee Server Security Suite Essentials.
- Cloud Workload Discovery for private cloud (VMware and OpenStack) is available as part of McAfee MOVE AntiVirus and McAfee Security Suite for Virtual Desktop Infrastructure (VDI).
- Cloud Workload Discovery for public cloud (AWS and Microsoft Azure) is available in McAfee Public Cloud Server Security Suite.

For more information, please visit **http://www.mcafee.com/us/products/data-center-security/server-security.aspx**

1. **Right Scale 2016 State of the Cloud Survey**

Intel and the Intel and McAfee logos, ePolicy Orchestrator, and McAfee ePO are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation. 2043_1216
DECEMBER 2016

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com