Solution Brief

Tenable and Microsoft Azure

Securely Deploy and Operate your Assets in Azure Cloud

Key Challenges

Organizations are moving their IT infrastructure to the cloud to improve business agility and decrease spend. However, by going to the cloud and leveraging cloud infrastructures like Microsoft Azure, IT departments can lose control and visibility of their full security posture.

Customers with vulnerability and compliance scanning solutions have successfully protected their on-premises IT assets. Can these same on-premises tools be deployed to the cloud to scan assets in Microsoft Azure? The simple answer is no, since Azure may construe such behaviors and actions as malicious, and consequently these security solutions will be blocked. To resolve that issue, you will need a security solution architected and purpose-built for the cloud.

To successfully reduce the attack surface and prevent compromise in Azure deployments, organizations must confidently answer these key questions:

- Which of my Azure virtual machines are running and how many subscriptions are enabled?
- Which cloud accounts have admin level privileges?
- Which of my websites and databases are enabled in Azure and which do not have SSL turned on?
- How many instances contain exploitable vulnerabilities and which are most critical?
- How many instances are infected with malware?

Solution Overview

Tenable™ enables Microsoft Azure customers to determine if their assets, workloads and applications are misconfigured or vulnerable to attack. This allows Azure customers to quickly and proactively prioritize resources in order to remediate threats and remove security weaknesses.

Tenable supports and secures Microsoft Azure with our Nessus®, SecurityCenter® and Tenable.io™ vulnerability management solutions. Over one million global users rely on Tenable's security solutions every day because they:

- Run in any environment: cloud, on-premises or hybrid
- Support multiple assessments including vulnerability scans, configuration and compliance checks, malware detection and web application scanning
- Scale from individual use to large enterprise and government deployments

Because Tenable solutions support both on-premises and cloud deployments like Microsoft Azure, organizations can employ a single technology for scanning and monitoring hybrid environments, thereby eliminating the need to buy, deploy and learn multiple tools.

Nessus: Audit your Azure environment remotely and non-intrusively with Nessus to identify deployed assets, databases, websites and account security settings that are in the cloud.

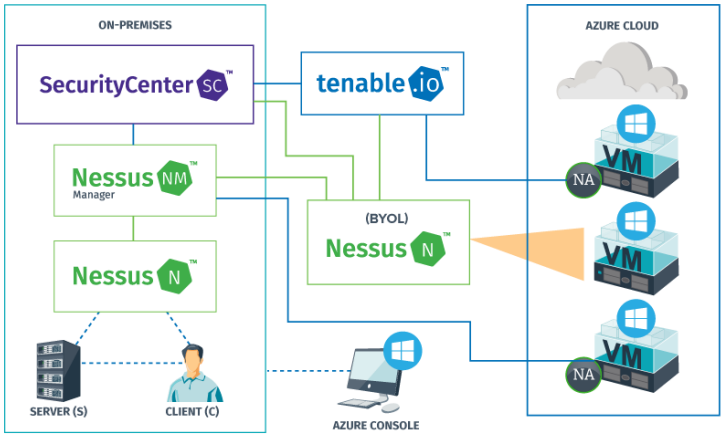
Microsoft Azure

Components:

- Microsoft Azure account
- Tenable.io™, Nessus Manager 6.5 vor higher, Nessus Agents or Nessus (BYOL) 6.5 or higher
- Tenable SecurityCenter 5.x or higher

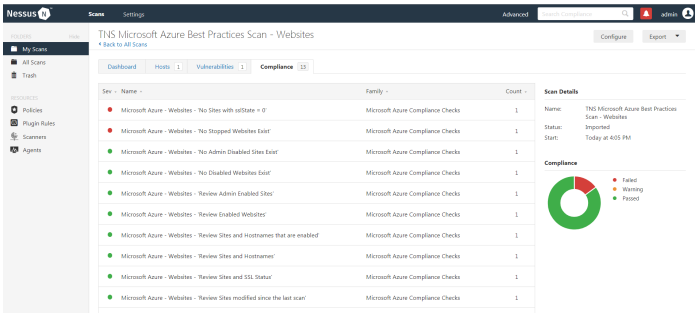
Benefits:

- Gain complete visibility into the resources deployed both on-premises and in the Azure cloud
- Reduce the attack surface by inspecting cloud virtual machines for misconfigurations and poorly implemented security settings
- Identify vulnerable instances and compromised systems running in Azure and the remediation necessary to mitigate risk
- Scan cloud virtual machines at regular intervals to ensure systems have not drifted out of compliance
- Improve ROI and reduce complexity by using a single technology to scan both on-premises and cloud deployments



Nessus Agents: Nessus Agents installed in your Azure instance provide vulnerability detection, configuration assessment, malware checks and compliance auditing. Nessus Agents can be managed by Tenable.io or Nessus Manager, and scan results can be viewed in Tenable.io, Nessus Manager or SecurityCenter.

Nessus (BYOL): Alternately, Nessus can be run directly in the Azure cloud. This pre-built appliance eliminates the hassles of installing an OS and then the Nessus software. If you are a current Nessus customer, you can apply your existing Nessus licenses to Nessus (BYOL) to perform Azure environment auditing or scanning.



Azure Best Practices Scan

SecurityCenter Continuous View: SecurityCenter Continuous View® (SecurityCenter CV™) provides continuous network monitoring to achieve total visibility of your security and compliance posture. SecurityCenter CV uplevels security and compliance management by providing real-time asset discovery, network traffic and anomaly detection, threat intelligence, extensive security analytics, trending and reporting capabilities.

Best of all, the Nessus scan results from any Nessus solution can be imported to SecurityCenter CV to get a complete view of both on-premises and Azure cloud assets. This empowers organizations to track and trend security and compliance issues, providing C-level measurement and metrics on the effectiveness of remediation and response programs for on-premises, Azure cloud and hybrid environments.

How It Works

Nessus:

- **Step 1:** Log in to your Azure account and define an application name and a redirect URL. A client ID will automatically be created in Microsoft Azure.
- **Step 2:** Enable Nessus access using the "Audit Cloud Infrastructure" template and configure Microsoft Azure user name, password, client ID and subscription ID (optional).

Nessus Agents:

- **Step 1:** Download your Nessus Agents and install on your Azure virtual machines per the instructions in the Nessus User Guide.
- **Step 2:** Manage your deployed Nessus Agents with Tenable.io or Nessus Manager

Nessus BYOL:

- **Step 1:** Deploy a Nessus (BYOL) instance from the Azure Marketplace
- **Step 2:** Apply the appropriate Nessus license (existing or newly purchased via Tenable Store). Depending on your license configuration, your Nessus (BYOL) can be used independently as Nessus Professional or be centrally managed by SecurityCenter, Nessus Manager, or Tenable.io.

NOTE: Before scanning your Azure virtual machines, you must first request authorization permission from Microsoft Azure.

Benefits

The benefits of a joint Tenable-Microsoft solution are compelling:

- Enables security administrators to gain complete visibility into what resources are deployed in both the Azure cloud and on-premises
- Removes the burden of manually verifying each cloud virtual machine for misconfigurations and poorly implemented security settings
- Identifies vulnerable instances and any compromised systems running in Azure to help prioritize remediation required to mitigate risk
- Scans cloud virtual machines at regular intervals post-deployment to ensure systems have not drifted out of compliance
- Delivers immediate ROI and ease of deployment with a single technology to scan both on-premises and cloud deployments

About Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact