Secure the Shadows and Unknown Assets

See everything with greater focus. Then take decisive action.

Your organization is under constant siege from a wide range of threats that are adapting and evolving almost as quickly as they're identified. It's a daunting challenge to secure the assets and data you know about against these attacks, but the simple fact is that you can't defend assets that you're not even aware of. "Shadow IT"—unknown devices, applications, and services that function outside the official scope of IT—represents a significant problem because these assets are not properly monitored, maintained, or protected.

The proliferation of mobile devices, cloud services, and virtualized infrastructures makes it simple for employees to introduce new devices or apps without the knowledge or consent of IT. Employees can introduce new devices to the network, or store sensitive company data on unauthorized cloud services without the knowledge or consent of IT. Individuals who take initiative in the interest of productivity or efficiency at the expense of security expose you to increased and unnecessary risk.

SecurityCenter Continuous View® Shadow IT Capabilities

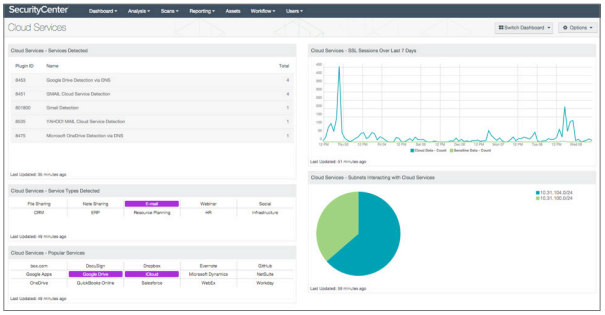
- **Active Scanning** – Periodically examine assets to determine their level of risk to the organization.
- **Intelligent Connectors** – Meta data matters most—put your investments to work in your security program with closed-loop, real-time connections to the business
- **Agent Scanning** – Nessus agents provide speed to discovery and remove challenges such as credentials
- **Continuous Scanning/Listening** – Better context faster by knowing instantly why and how known/unknown assets are communicating and then prioritize your response
- **Host Activity Data** – Tenable's host data logs what's changing and what's being added across any environment or asset

Build on Foundational Security, and Fast

Unfortunately, traditional security solutions can't provide the continuous visibility you need to identify shadow assets.

For you to answer questions about your security posture with confidence—particularly in a highly-distributed and ever-changing IT environment—you need to be sure that all assets and data are identified and protected. This isn't just because you should; the IT landscape today is highly regulated with multiple frameworks and standards requiring assets to be managed. Understanding first and foremost what devices are on your network is a crucial foundation for security, with the rest of a program building upon that knowledge. Discovering software and third party services is not far behind as one of the fundamental building blocks of defense. You cannot secure what you can't see.

More recently, not having visibility into cloud services and mobile devices provides a significant opportunity for data loss or compromise. Personal cloud storage services, and personal or BYOD mobile devices are blind spots for security without the use of intrusive (and expensive), specialized products dedicated to those environments. Relying solely upon point-in-time snapshots of the network can also create blind spots, or missing devices present between scans. For example, transient laptops that aren't continuously connected create blind spots.



Even if unknown devices and services are identified, another concern is prioritization and context. With limited security resources—both in terms of the personnel available and the tools at your disposal, it is important to determine the security impact of those assets. Assessing the weaknesses and trust relationships of an asset provide crucial context about security risk and helps you prioritize assets for protection. Without that contextual information, there is too much noise for IT to make informed decisions.

Attackers know that the easiest path to compromise your assets is to go after the entry points you don't know about. While a locked door will keep threats out, it only works when you haven't left the windows open as well.

While you are vigilantly watching and diligently securing your known devices and data, these shadow assets are left unpatched and unprotected, just waiting to be hacked; providing that pivotal entry point to move through your network and reach critical assets and sensitive data.

Solving the Shadow IT Problem

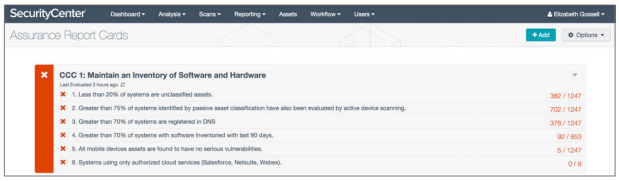
Tenable Network Security can help you continuously find known and unknown assets across your environment so you can ensure they are properly secured and no longer pose a risk. Tenable's comprehensive security solutions address the challenge of identifying unknown assets to minimize the impact of shadow IT in your environment.

Tenable SecurityCenter Continuous View (SecurityCenter CV) delivers total visibility of all known and unknown assets on a network. Tenable's passive traffic and event monitoring tools detect all devices, services, and applications in use, and identify associated vulnerabilities so you can quickly and easily determine the relative risk they expose you to. SecurityCenter ActiveSync and Mobile Device Management (MDM) integration also enable SecurityCenter CV to detect and identify unknown and shadow assets, including transient laptops, personal mobile devices, and rogue cloud applications. When new mobile devices are detected, Tenable also pulls policy and software information about the device from integrated MDM systems.

Simply realizing that shadow assets are out there is not enough to protect them and your environment. Security teams need visibility into the posture of these devices and services, in order to reduce the attack surface. As SecurityCenter CV discovers unknown, mobile, and cloud assets, their vulnerability exposure is also assessed to determine which pose a greater relative risk.

Tenable SecurityCenter CV secures the IT shadows by bringing unknown assets to light. When hosts are discovered, it can automatically scan them and distribute reports of what's present on your network.

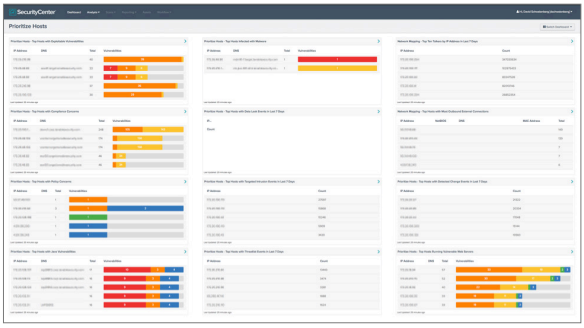
Tenable's library of dashboards provide a lens into the unknown by breaking down detections and the vulnerabilities they present, in the context of your greater security program, so you can make informed decisions for effective and rapid response . When communicating the status of your findings, Assurance Report Cards are an essential tool to report up the chain using business language so that everyone across the organization, especially business decisions makers, can see at-a-glance if your organization is achieving your objectives.



Assurance Report Cards visualize your comprehensive security effectiveness

Bring Unknown Assets Out of the Shadows

You need the right tools to continuously monitor your environment to detect and identify these shadow assets. Tenable SecurityCenter CV provides a comprehensive solution that gives you the visibility and context you need to protect your network and secure your assets effectively with decisive action.



About Tenable

Tenable Network Security 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 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses 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