

## Security Assurance

### Measure Security Assurance with SecurityCenter Continuous View®

- **Clear business insights** – Assurance Report Cards (ARCs) map security metrics to business objectives. Pre-built ARCs align with industry standards like the NIST Cybersecurity Framework.
- **Improved communication** – Report cards visualize effectiveness of security programs and investments, making it easy to show progress and identify gaps to business and technical executives.
- **Reliable metrics** – Unique combination of active scanning, agent scanning, host data monitoring, integrations with third-party systems, and continuous listening ensures that you have trusted data to measure security and compliance for your entire infrastructure.
- **Unified visibility** – Integration of security data from patch management, mobile device management, and other security systems provides a unified, real-time view of security effectiveness across the enterprise.

Defining success, identifying risks, and figuring out the “right” metrics for measuring cyber security programs are challenging. Do you know how effective your current security solutions are? Can you demonstrate the effectiveness of your security programs to executives? Do business executives in your organization and the board understand how and why investments are being made?

If those are hard questions to answer, you’re not alone. Measuring the effectiveness of your security program is a huge challenge. No two organizations are alike, meaning there is no standard template to follow. You have to understand the business needs of your organization, define and map security requirements based on the business needs, collect relevant metrics, and measure your success. If you do this well, the right security metrics – supported by solid underlying data – will help your organization understand cybersecurity risks and exposures, better assure organizational security and compliance with industry standards and frameworks, and drive appropriate action across the organization. On the other hand, choosing the wrong security metrics undermine IT security credibility and perceived value.

### Span the Gap Between IT and Business

In order to measure security effectiveness, you have to first define security goals that align to your business and objectives. For example, if you are a high-transaction retail business that only allows servers to be taken offline once a quarter for patching, delivering monthly reports on unresolved vulnerabilities isn’t terribly useful. These misaligned reports could even cause the security or IT operations teams to be viewed as not doing their job – because for two months out of three, you would have to report that vulnerabilities went unpatched.

To be successful, you need tools and processes that allow you to set security metrics that make sense. This requires not only defining the correct metrics, but having trustworthy data to back them up – and in a format that business users understand. When it comes to cybersecurity, there can be the perception that IT security teams are “crying wolf” because risks never seem to materialize. In other cases, CEOs may see the business value of security, but don’t have the knowledge to quantify the risk based on security metrics alone. What does having 20 unpatched vulnerabilities on critical systems mean? If it’s not clear, you’re not demonstrating your effectiveness.

As Paul Proctor, vice president and distinguished analyst at Gartner Group states: “If you want them to care, you have to give them something that influences their decision making, something that matters to THEM. That means you have to know something about them AND be able to link your metrics to their issues.” Security teams must give business leaders visibility and assurance that:

- Security investments made are the right ones
- Requests for increased spending are justified
- Security efforts support overall goals of the business

## Effectively Measure Security Assurance

Tenable gives organizations a way to measure security effectiveness by aligning security metrics with business goals. Tenable provides proactive measurement, analysis, and visualization of security metrics through customizable dashboards, reports, and the industry's first Assurance Report Cards (ARCs). ARCs allow you to communicate the status of your organization's security standards and compliance requirements to the business in terms they understand. Each metric is mapped to business objectives you define so executives can quickly grasp the impact of security efforts on your organization's cyber risk and compliance posture.

Assurance Report Cards visualize security effectiveness in terms of business impact.

ARCs complement Tenable's comprehensive data collection approach, which uses a combination of active scanning, agent scanning, host data monitoring, integrations with third-party systems, and continuous listening to assess the protection status of your complete infrastructure. Together, these capabilities provide organizations the ability to:

- Gain unparalleled visibility into the security posture for all systems and devices in your heterogeneous enterprise.
- Optimize your defenses by making sure that security systems are configured properly and performing as expected.
- Ensure compliance with security mandates, company policies, and industry regulations.
- Align IT Operations, Security Operations, and Business Operations to increase organizational efficiency and effectiveness.

## 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](https://www.tenable.com).