


Security Baseline metrics, indicators, and risk tolerance

02/11/2019 • 4 minutes to read • Contributors 

In this article

[Metrics](#)

[Risk tolerance indicators](#)

[Next steps](#)

This article is intended to help you quantify business risk tolerance as it relates to Security Baseline. Defining metrics and indicators helps you create a business case for making an investment in maturing the Security Baseline discipline.

Metrics

Security Baseline generally focuses on identifying potential vulnerabilities in your cloud deployments. As part of your risk analysis you'll want to gather data related to your security environment to determine how much risk you face, and how important investment in Security Baseline governance is to your planned cloud deployments.

Every organization has different security environments and requirements and different potential sources of security data. The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Security Baseline discipline:

- **Data classification:** Number of cloud-stored data and services that are unclassified according to on your organization's privacy, compliance, or business impact standards.
- **Number of sensitive data stores:** Number of storage end points or databases that contain sensitive data and should be protected.
- **Number of unencrypted data stores:** Number of sensitive data stores that are not encrypted.
- **Attack surface:** How many total data sources, services, and applications will be cloud-hosted. What percentage of these data sources are classified as sensitive? What percentage of these applications and services are mission-critical?
- **Covered standards:** Number of security standards defined by the Security team.
- **Covered resources:** Deployed assets that are covered by security standards.
- **Overall standards compliance:** Ratio of compliance adherence to security standards.
- **Attacks by severity:** How many coordinated attempts to disrupt your cloud-hosted services, such as through Distributed Denial of Service (DDoS) attacks, does your infrastructure experience? What is the size and severity of these attacks?
- **Malware protection:** Percentage of deployed virtual machines (VMs) that have all required anti-malware, firewall, or other security software installed.
- **Patch latency:** How long has it been since VMs have had OS and software patches applied.
- **Security health recommendations:** Number of security software recommendations for resolving health standards for deployed resources, organized by severity.

Risk tolerance indicators

Cloud platforms provide a baseline set of features that enable small deployment teams to configure basic security settings without extensive additional planning. As a result, small dev/test or experimental first workloads that do not include sensitive data represent a relatively low level of risk, and will likely not need much in the way of formal Security Baseline policy. However, as soon as important data or mission-critical functionality is moved to the cloud, security risks

increase, while tolerance for those risks diminishes rapidly. As more of your data and functionality is deployed to the cloud, the more likely you need an increased investment in the Security Baseline discipline.

In the early stages of cloud adoption, work with your IT security team and business stakeholders to identify [business risks](#) related to security, then determine an acceptable baseline for security risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how security metrics, such as those discussed above, can justify an increased investment in the Security Baseline discipline.

- **Mission-critical workloads trigger.** A company deploying mission-critical workloads to the cloud should invest in the Security Baseline discipline to prevent potential disruption of service or sensitive data exposure.
- **Protected data trigger.** A company hosting data on the cloud that can be classified as confidential, private, or otherwise subject to regulatory concerns. They need a Security Baseline discipline to ensure that this data is not subject to loss, exposure, or theft.
- **External attacks trigger.** A company that experiences serious attacks against their network infrastructure x times per month could benefit from the Security Baseline discipline.
- **Standards compliance trigger.** A company with more than $x\%$ of resources out of security standards compliance should invest in the Security Baseline discipline to ensure standards are applied consistently across your IT infrastructure.
- **Cloud estate size trigger.** A company hosting more than x applications, services, or data sources. Large cloud deployments can benefit from investment in the Security Baseline discipline to ensure that their overall attack surface is properly protected against unauthorized access or other external threats.
- **Security software compliance trigger.** A company where less than $x\%$ of deployed virtual machines have all required security software installed. A Security Baseline discipline can be used to ensure software is installed consistently on all software.
- **Patching trigger.** A company where deployed virtual machines or services where OS or software patches have not been applied in the last x days. A Security Baseline discipline can be used to ensure patching is kept up-to-date within a required schedule.
- **Security-focused.** Some companies will have strong security and data confidentiality requirements even for test and experimental workloads. These companies will need to invest in the Security Baseline discipline before any deployments can begin.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Security Baseline discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your Cloud Governance team.

Next steps

Using the [Cloud Management template](#), document metrics and tolerance indicators that align to the current cloud adoption plan.

Building on risks and tolerance, establish a process for governing and communicating Security Baseline policy adherence.

Establish policy compliance processes