Guardicore

7 Best practices for data center security

The last couple of years have seen one headline after another announcing a major cyber attack on large enterprises. All organizations must address their cyber security road map and implement best practices for cyber security readiness.

We've gathered these 7 best practices for data center cybersecurity, to help you close unguarded ports and fix vulnerabilities.

1 Address your present and future environments

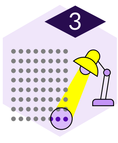
Effective data center security means addressing every part of your ecosystem

Whatever process or tool you deploy, it's crucial that it addresses every corner of the modern data center. That includes your on-prem servers, cloud environments, PaaS processes, the works. Make sure that it encompasses your current infrastructure, as well as anything you might add or develop in the near future.

2 Harden your systems

System hardening can prevent breaches, when it's carried out on time and done right

Seek out a reliable process for hardening your systems. Simple attack surface reduction is not enough. Look for something that includes vulnerability management, file integrity monitoring, and other hardening configuration management.



3 Gain visibility

If you can't see it, you can't adequately protect it

Clear visibility into your data center environment is a prerequisite for effective cybersecurity. Only 2.5% of enterprises have full visibility across all their infrastructure[1]. Once you have clarity about your applications and interactions, you'll be able to appropriately handle risk management, policy configuration, and incident response processes.

4 Segment your network

Perimeter security is not enough

Segmentation reduces risk in a simple and measurable manner, by containing cyber threats from spreading throughout your ecosystem. Strive towards ever-smaller segments that divide up your data center into defined and protected sections, leveraging new technologies that allow you to do this quickly across all your infrastructures.

5 Automate everything

Only automation can keep your cybersecurity up to date

Data centers are dynamic, and applications change rapidly. Any security process which is not automated will eventually become outdated and irrelevant. You need to automate all of your security processes, so that they remain fit for purpose even under changing conditions.

6 Deploy effective detection

Data centers need a different strategy from end-points or desktops

Best security practices for data centers have to be tailored to different attack vectors and a more critical, monitored performance. You need to deploy detection technology to deliver value that is cost effective relative to the resources it consumes and the complexity it introduces. Reduce complexity as much as possible by focusing on lateral movement detection and converged tools.

7 Simplify, Simplify, Simplify

If it's not simple, it won't survive

Simplicity should be the touchstone for every tool or process that you consider. If it's too complex, it won't stand up to your everyday life. Most organizations get far more value from a small set of tools that they understand thoroughly than from a huge toolkit of best-in-breed tools that they don't fully understand.

Implementing cybersecurity best practices, like the 7 we've outlined here, is a key step in securing your data center and business systems. Read more about securing your modern enterprise at **www.guardicore.com**

1.https://www.datacenterknowledge.com/security/why-traditional-security-info-and-event-management-tools-no-longer-cut-it

---

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security — for any application, in any IT environment.

www.guardicore.com