Frequently Asked Questions

Answers to key questions about a Defense in Layers security strategy

What is Defense in Layers?

A Defense in Layers (DIL) strategy does exactly what its name suggests: it layers different protective tools and solutions over your most sensitive data to deflect as many types of cyber crime as it can. And it places a pragmatic emphasis on tools that help an organization quickly recover from cyber attacks, which are increasingly inevitable even with multiple layers of defense.

A Defense in Layers strategy requires a proactive focus that incorporates best practices in physical controls to an organization's IT systems, administrative controls like employee training, and technology solutions.

Why is Defense in Layers important to cyber security?

The truth is, it's not a matter of if you'll suffer a cyber attack, it's a matter of when. The news can feel dismal, but there is a silver lining: organizations aren't completely at the mercy of cyber criminals. While it's true that it's tremendously challenging to completely prevent a cyber attack, a Defense in Layers cyber security strategy can mitigate the effects of a cyber security incident.

The underlying premise to a DIL strategy is that there's no one tool or solution that's going to prevent 100 percent of cyber attacks. Because employees are an organization's greatest vulnerability, it's impossible to remove the human factor in cyber security.

Organizations' cyber security needs are only growing more complex by the day. That's why a Defense in Layers approach that incorporates tried-and-true technology that

helps to archive and restore data in an offline environment is the only strategy that makes sense for today's threat landscape.

What cyber security problems does Defense in Layers solve?

Organizations today are faced with innumerable cyber security pressures. From maintaining their reputation with clients and stakeholders, to protecting sensitive personally identifiable information, to concerns about financial repercussions to ransomware, to an evolving regulatory landscape, companies must now add the following to their list:

- The necessity to restore and archive data to get back up and running quickly after a cyber security incident.
- Difficulty getting cyber liability coverage, or getting a full payout when you do have a cyber security incident.
- The need to not only protect data from theft, but to ensure that it's immutable from tampering.

A Defense in Layers approach provides the best chance of recovery from a cyber security incident and addressing this varied list of security risks organizations face in today's threat landscape.

How does offline, removable data management help keep data safe?

Organizations often have tools and solutions already in place that they can repurpose into a Defense in Layers strategy to help restore and archive their data. One of the most critical is offline, removable media. Since the vast majority of cyber crime happens online, savvy organizations are taking a second look at some of the proven offline solutions they've used for years and strategically using them for cyber security disaster recovery. When data is stored in an offline environment, it's out of the reach of online cyber criminals.

What are the aspects of the offline security layer of a Defense in Layers approach?

The four core tenets of the offline aspect of a Defense in Layers security strategy are:

- **Removable data storage**. Offline, removable data management is taking an increasingly important role in the data security stack. Data stored on offline

media such as CDs, DVDs, Blu-ray and USB is kept safely out of the reach of cyber criminals.

- **WORM technology.** Write Once, Read Many (WORM) technology is a critical piece to any organization's data security strategy because cyber criminals aren't just interested in stealing data—sometimes they want to manipulate it. With WORM technology data is written immutably on removable media so it can be read any number of times but never manipulated or changed.

- **Chain of custody.** Chain of custody allows the movement of data to be tracked through its lifecycle to document each user that handles it. This provides accountability and the ability to trace any nefarious activity that might have occurred to any piece of sensitive data back to an individual.

- **Backup and recovery.** With air-gapped, offline backup and recovery, a copy of your data is kept offline and inaccessible to the internet so cyber criminals can't get their hands on it.

What is an air-gapped backup?

An air-gapped backup, as part of a backup and recovery strategy, is a copy of your organization's data that's offline and inaccessible. Without being connected to the internet or other network connection, it's impossible for your backup device to be remotely hacked or your data to be manipulated.

What's the difference between Defense in Layers and Defense in Depth?

Many in the cyber security industry use the phrase "Defense in Depth" to refer to a layered approach to security where many different defensive tools are stacked on top of each other. This creates intentional redundancies that make it more likely to thwart attack. A Defense in Layers approach does the same thing, but it adds an important component: at least one of the defensive mechanisms must be an offline data management tool. That's because an offline version of your data is not accessible to cyber criminals, who almost always access data online.

How can Rimage help?

Here at Rimage, we've been providing our clients with safe, reliable, proven offline backup solutions for more than 40 years. Rimage's suite of offline, removable data management products are uniquely suited to give organizations the Defense in Layers offline data security they need in order to keep their data safe, ensure "quick restart" business continuity when they're attacked, prove to insurers that they're compliant with

cyber crime liability policies, and ensure data is secure with immutable backup technology.

How can I get in touch with you to talk about my cyber security needs?

Call us today at 800.445.8288.