RIMAGE®

# YOUR DEFENSE IN LAYERS PARTNER FOR CYBER SECURITY

RIMAGE® DEFENSE IN LAYERS PARTNER

**Cyber attacks and the cost of breaches are increasing, and there's no end in sight. That means your most valuable asset, your data, is at constant risk of attack.**

## How Cyber Crime Could Affect You

In 2021, the average global cost to remediate a ransomware attack rose to $1.5 million, more than double the previous year's average ($761,106).[1] Cybercrime will cost the world $10.5 trillion annually by 2025.[2]

Malware is the most expensive type of attack with the average incident costing U.S. organizations $2.6 million.[3]

New vulnerabilities for organizations that emerged from shifting to a remote workforce greatly expanded the cyber-attack landscape and added many vulnerabilities for hackers to exploit. Malware increased by 358% overall and ransomware increased by 435% from 2019 to 2020.[4]

[1] Sophos. (2021, April 27). The State of Ransomware 2021.
https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

[2] Accenture. (2019, March 6). The Cost of Cyber Crime.
https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[3] Accenture. (2019, March 6). The Cost of Cyber Crime.
https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[4] Deep Instinct. (2021, February 11). 2020 Cyber Threat Report.
https://info.deepinstinct.com/en/tof/cyber-threat-report

# Do you understand what you’re up against?

**Bad actors have many different motivations. Some criminals are out for economic gain, others are political activists and still others just want to destroy data for no reason other than mischief.**

There are many different types of cyber attacks, and by understanding the differences between them, you can see why a Defense in Layers strategy is so critical. Because each type of cyber attack exploits a different vulnerability in the system, organizations need numerous ways to protect themselves. And with the Dark Web essentially becoming a user-friendly ecommerce site, it’s simple and easy for hackers to find the tools they need to perpetrate cyber crime.

# Malicious Attacks

## Here are some of the most common types of malicious attacks:

**Malware.** This broad category encompasses spyware, viruses, trojans and worms. The common attribute is that all malware is developed solely to cause harm to computers, servers, or networks.

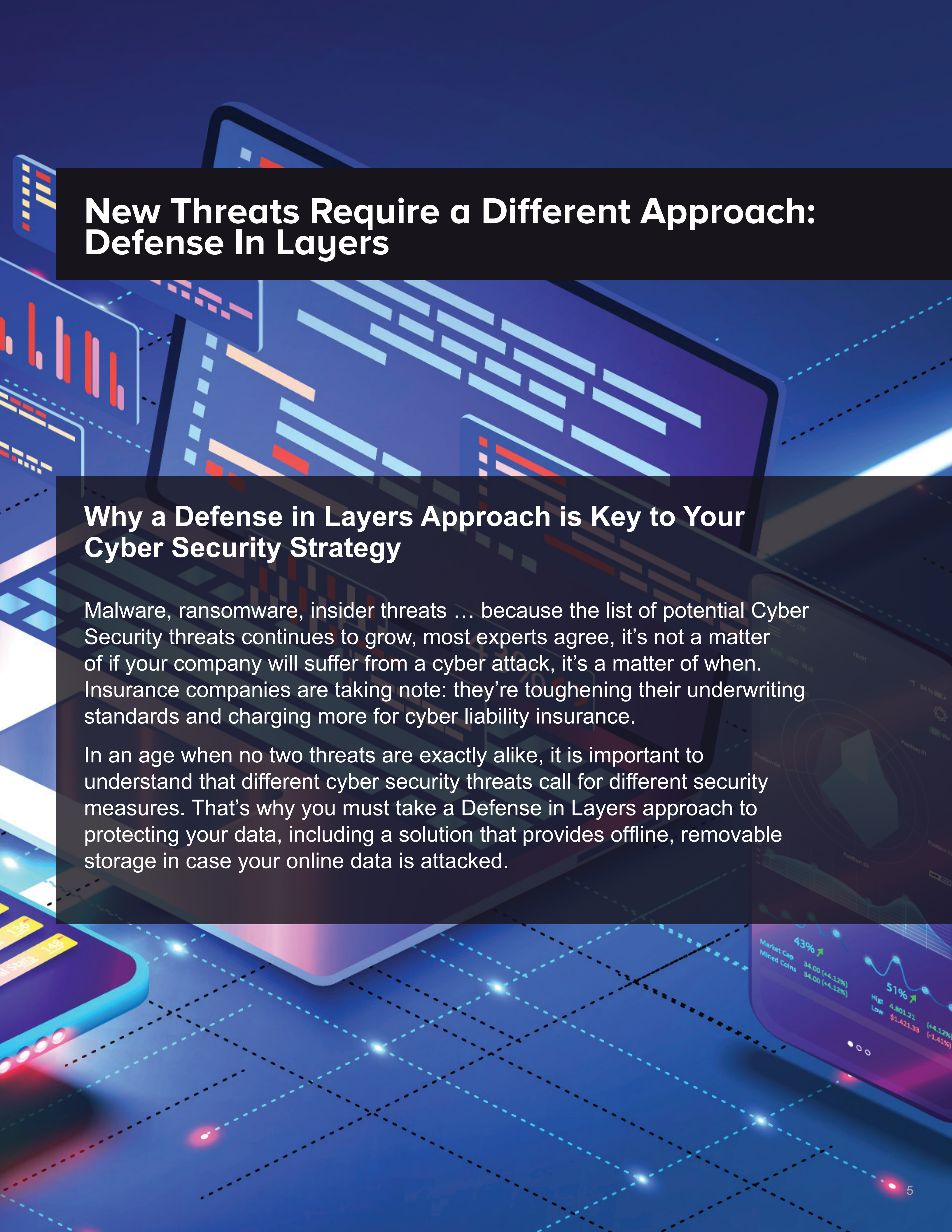
**Ransomware.** One of the most common types of malware that gets a lot of media attention, ransomware denies the victim access to their data until they pay a ransom to release it.

**Phishing.** In a phishing attack, the criminal sends fraudulent emails containing malicious files or scripts to unsuspecting users. This type of attack exploits an organization's point of vulnerability: its employees.

**Man-in-the-middle attacks.** These attackers exploit network security vulnerabilities by inserting themselves between someone's device and the network, thereby redirecting information to themselves rather than the legitimate destination.

**Denial-of-service attacks.** By flooding a system, server or network with traffic and requests, denial-of-service attacks can incapacitate a system or even take it completely offline, preventing it from fulfilling legitimate requests.

**Social engineering attacks.** In these attacks, the attacker uses social interaction and/or psychological manipulation to gain the trust of a human being, who then hands over login information or otherwise lets the attackers into the system.



# New Threats Require a Different Approach: Defense In Layers

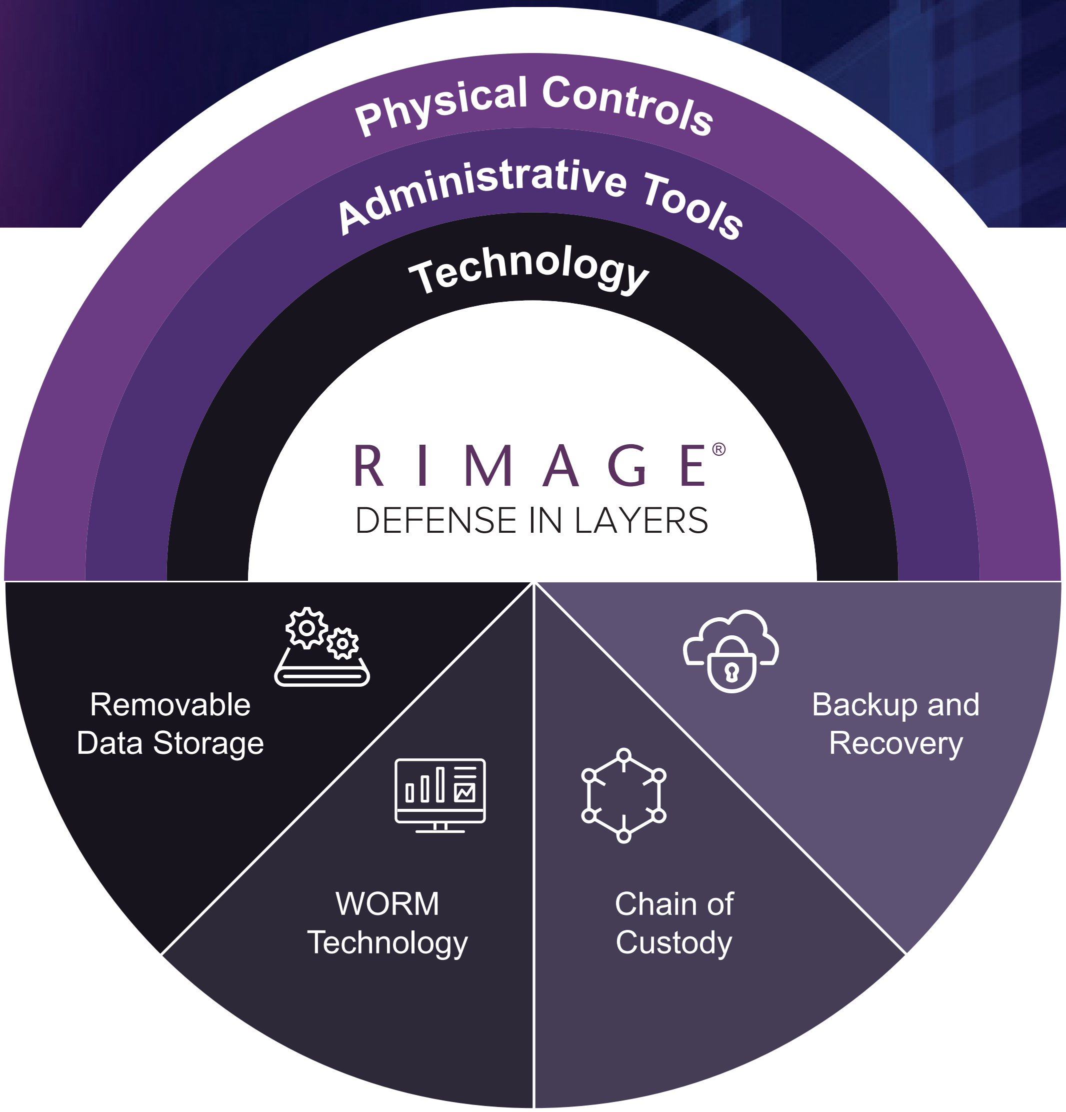
## Why a Defense in Layers Approach is Key to Your Cyber Security Strategy

Malware, ransomware, insider threats … because the list of potential Cyber Security threats continues to grow, most experts agree, it's not a matter of if your company will suffer from a cyber attack, it's a matter of when. Insurance companies are taking note: they're toughening their underwriting standards and charging more for cyber liability insurance.

In an age when no two threats are exactly alike, it is important to understand that different cyber security threats call for different security measures. That's why you must take a Defense in Layers approach to protecting your data, including a solution that provides offline, removable storage in case your online data is attacked.

# Defense in Layers Data Security

**There's no one solution that will protect against all forms of cyber attack. Rimage recommends organizations employ multiple types of data security to create a Defense in Layers security posture.**



Physical Controls

Administrative Tools

Technology

RIMAGE®
DEFENSE IN LAYERS

Removable
Data Storage

WORM
Technology

Chain of
Custody

Backup and
Recovery

## Defense In Layers Requires Proactive Focus

**Physical controls.**
These are tools that control physical access to an organization’s IT systems, such as security teams, locked doors with managed access, biometrics, fences, video security, and the like.

**Administrative tools.**
Employee training for both in-office and remote workforces as well as company policies, hiring practices and background checks are examples of administrative tools companies can use to protect data.

**Technology.**
Organizations should include several different types of data security technology tools, such as:

- Antivirus software
- Authentication/password security
- Encryption
- Firewalls
- Virtual private networks (VPNs)
- Multi-factor authentication
- Intrusion prevention software

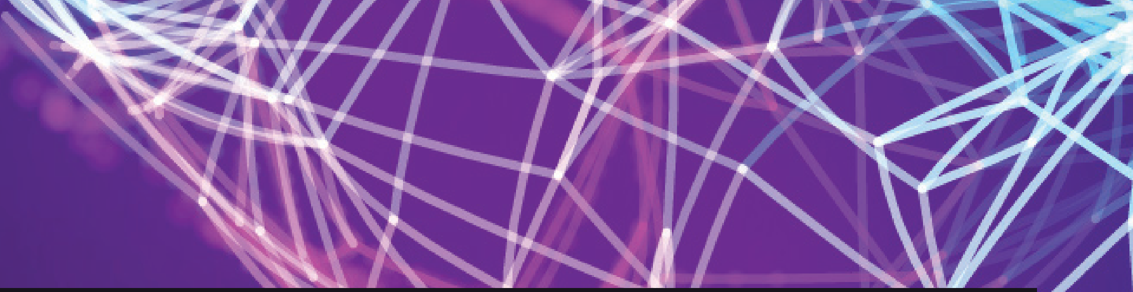
Critical technology components include:

**Removable data storage.** Data is stored on CDs, DVDs, USB or other offline media to keep it out of the hands of cyber criminals.

**Write once, read many (WORM) technology.** Data is written indelibly on removable management media so that it can be read any number of times, but never manipulated or changed.

**Chain of custody.** Maintaining the chain of custody increases transparency, enables accountability and supports risk mitigation by reducing the opportunity for malicious actors to tamper with important assets like data or evidence.

**Air-gapped, offline backup and recovery.** A copy of your data is kept offline and inaccessible from the internet so that cyber criminals can’t get to it.



# A Proactive Approach

## In a proactive approach to data security, organizations:

- Accept when data has been compromised, rather than trying to avoid the reality of the situation or deny what’s happened
- Understand and have planned for the cost of getting back up and running after an attack—which can be two to five times the cost of the ransomware demanded
- Know that they’ll likely recover only about 60% of the data once the ransom has been paid
- Are prepared for the impact to their revenue and brand with marketing and public relations crisis response strategies
- Take steps to mitigate the loss of partnership relationships and talent from their employees, their executive ranks and even their board

Escalation process and list

Data recovery and business continuity plan

Policy creation for tech stack

Emergency restart button

Puppet/chef scripts

Round table

# If Disaster Strikes, What Will I Need to Restore?

**With the risk of cyber attack increasing nearly to a certainty for many organizations, it’s important to understand what fundamental business functions you’ll need to restore immediately in order to ensure business continuity.**

License keys and encryption codes

Intellectual property

Customer and contractor information

Insurance policy information and AVL

Facility access controls

Server, virtual machine and system image

# Is Your Company At Risk for A Cyber Attack?

**The first step in developing a strategy to protect your data is to understand your risk level. This is important not just for your team but your insurance company as well, since insurers are toughening their underwriting standards for cyber liability insurance.**

Here are some of the things you should evaluate and audit to understand how vulnerable your organization is to attack:

- **Who has access to your systems?** When it comes to data security, the fewer cooks in the kitchen, the better. If most of your data is readily available to most of your employees or vendors, and they have no good reason for having access to it, that creates an unnecessary vulnerability.
- **Is your data encrypted?** Data encryption encodes data so it can only be accessed by a user with the correct encryption key. If you haven’t encrypted your data, and you suffer a cyber attack, cyber criminals can read your data as easily as you can.
- **Are your databases secured?** Databases are the heart of any business. Yet many organizations lack a clear understanding of who is accessing their databases and for what purposes. Not only does this subject you to cyber attack from outside, but employees can also accidentally delete or change important data.

# Is Your Company At Risk for A Cyber Attack?

- **How strong are your password and authentication protocols?** No one likes having to change their passwords or deal with two-step authentication processes. But companies that have lax password and authentication standards are at greater risk for cyber attack.
- **Do you have a remote workforce?** Even before the COVID pandemic, many companies were moving toward a hybrid or remote workforce. While there are advantages, remote workers can pose a greater security threat than their in-office colleagues. If all or part of your workforce is remote, it’s even more critical to develop a Defense in Layers security strategy, part of which is communicating best security practices to employees.
- **Do you understand your exposure?** If you suffered a cyber attack today, do you have a good understanding of potential lost revenue and damage to your brand? With cyber attacks on the rise, for most companies, it’s not a matter of if you’ll suffer a cyber attack, it’s a matter of when.

**Ready to bolster your Defense in Layers strategy?**
**Get in touch with us today.**

**Rimage.com**

With over 40 years of innovation, Rimage delivers offline, removable enterprise solutions for data security, archival, compliance and on-demand publishing. As the global leader in on-demand digital publishing, Rimage is an innovator in CD, DVD, Blu-ray disc and USB publishing. Over 22,000 Rimage workflow-integrated systems support businesses throughout the world, including day-to-day disc publishers and organizations that duplicate and print a variety of media as critical components of their daily operations. Throughout its history, the company has provided best-in-class workflow-integrated solutions that serve a variety of markets and applications.

RIMAGE®

201 General Mills Blvd, Golden Valley, MN 55427 USA
+1.800.445.8288 Email: sales@rimage.com

© 2021. All rights reserved.