RIMAGE®

RANSOMWARE: WHAT IT IS, WHY IT EXISTS AND HOW REMOVEABLE, ON-PREMISE DATA MANAGEMENT FITS INTO THE DATA SECURITY STACK

Executive summary

The technical world is in the midst of a cyber pandemic. Every level of global government, industry vertical and global citizen are at risk. Ransomware is just one of the tools that bad actors are leveraging. We are in a new normal driven both by the biological and cyber pandemics.

In the last year, businesses have seen a surge in ransomware attacks. According to research by CheckPoint Software, in the third quarter of 2020, organizations worldwide experienced a 50% increase in the daily average of ransomware attacks, compared to the first half of 2019. And nowhere is that more evident than in the U.S. which according to the report, has experienced the biggest increase in attacks.

Recent data reported in Bitdefender's Mid-Year Threat Landscape Report shows a shocking 715% year-on-year increase in detected and blocked ransomware attacks in 2020. Despite this, there doesn't appear to be a silver bullet in sight to effectively respond to and prevent the attacks. Possibly that is because the real problem is not just a technology issue. The more we learn, the clearer it becomes that employee behavior is an organization's greatest vulnerability.

Whether employees intentionally flout security protocols or mistakenly open a gateway for ransomware to infiltrate a system, their unpredictable actions make it impossible for companies to guard against ransomware with 100% success. That's why a comprehensive solution that includes all layers of the data security stack is critical to ransomware prevention. One element of the data security stack that organizations must utilize is removeable, on-premise data archiving technology. By its very nature, removeable storage is one of the more secure data archiving options because it can be stored separately from the internet and the cloud. For prevention, storage, backup and recovery, a removeable, on-premise data management solution is a must-have part of the data security toolbox for organizations today.

What is ransomware?

Ransomware is used by malicious actors to target an individual or organization to extort a ransom from them. It is a set of tools that encrypts the data, systems and/or tools, making that data inaccessible. Without advance planning, the only option a target of ransomware has is to pay the ransom, typically with cryptocurrency, to restore access to their data.

Why do bad actors use ransomware?

- Extortion
- Revenge
- To prove I can
- Disruption of your capabilities
- Undermining trust in your company, its services and its value in the market

How is ransomware deployed?

- A malicious actor (internal or external) trolls for a way to access the network or individual devices such as:
  - WAN/LAN/cloud/mobile vulnerabilities
  - Social engineering tactics such as phishing
  - Access via a stolen or lost device
  - Current or legacy technology not wiped prior to disposal
  - Disgruntled contractor or employee
- Malicious actor circumvents or disables the network or system's anti-virus protection software
- Malicious actor opens a "back door," either something that was coded in the past or a new operation that was installed when the anti-virus software was no longer enabled
- Malicious actor can then utilize other vulnerabilities to escalate access to more systems' privileges
- Malicious actor then gains full control over the network or devices, and can steal data or install malware, such as ransomware
- In the case of ransomware, the malicious actor then tries to extort the company/individual into paying to restore data and access to the systems. However, even if the company does resort to payment, there is no guarantee access will be restored, or that other backdoors or malware won't be left behind
- Malicious actors target all operating systems (OS) including BYOD (bring your own device), phones or professional services automation systems. The days of Microsoft OS being a sole target are gone.

What options do you have to prevent or respond?

Industry leading companies are deploying funds, resources and solutions to continue to defend and prevent attacks. There are two key elements to an organization's ransomware protection strategy:

Employee training and communication. Within any technology system, the greatest vulnerability is the humans involved. Companies need to train and communicate the risks to individuals, outlining clear work-from-home dos and don'ts to limit unauthorized access to networks, systems and data.

Technology. There is no one silver bullet to prevent ransomware or offset its effects when it does happen. That's why a data security stack that includes layers of defense and recovery options is critical. One layer of the security stack companies often overlook is removeable, on-premise data management. These systems are in operation in tens of thousands of systems globally on a daily basis. These systems are being leveraged to back up, store and distribute data across a wide spectrum of markets, including healthcare, manufacturing, marketing, training, military and government. These systems provide low cost, fast access to recorded data. This is critical to start to rebuild your data baseline as an event is unfolding.

What files should you back up?

First and foremost, your IT teams have the insight and background and critical recovery schedules to know what is needed to recover from an event. Even though the new malicious actors are always changing the rules, the basic recovery point objectives hold true. Every industry has a different risk profile but focusing on the fundamentals of your system's building blocks is a strong first step.

- Active directory (AD). Malicious actors target areas of control. Backing up your AD each day will allow you to have a version to quickly access and start your recovery.
- Facility access. Malicious actors do not usually try to access a facility but this does occur in some industries. Disrupting your building's access, HVAC controls or physical and video tracking security technology stack can cause a distraction, allowing other areas to be compromised or allowing the removal of tracking actions.
- Third-party applications access tools. These may be using SSO (single sign-on) tied to your AD, but they have dedicated user access and control files. Backing these up daily will also allow you to access recovery point capabilities.
- Custom automated scripting that your teams or third parties have developed for you. These internal unifying processes may also be exploited, so making sure they are documented and backed up is critical. Every company has team members that are inquisitive. They build processes to make jobs easier, move files and restart failed manual tasks. You need to acknowledge that they exist and add them to your recovery process because anything can be exploited.

How do removeable, on-premise data management systems work to back up and recover files?

- These systems are or can be attached to a LAN segment
- You should be able to set up an IT user group using an autoconductor interface
- Your IT team is provided access to your system
- A dedicated access and file area is set aside just for the IT team to leverage
- The IT team writes incremental data files that would be critical to recover if a malware or a data compromise event were to occur
- These files are burned with write once, read many (WORM) technology to CD/ Blu-ray or USB formats
- The media is stored per your IT or company's recovery protocols

What are the benefits of removeable, on-premise data management?

WORM data archiving technology is used to ensure data integrity, from both accidental alteration and malicious actors using tools like ransomware. Once data has been written, it cannot be changed or deleted, but it can be read as many times as needed.

- This technology is one of the tools companies can use to add an additional layer of defense against ransomware or like events.
- Backup data written to optical or a USB device with read-only memory cannot be altered in any way—by a virus, a malicious actor using ransomware or accidental deletion.
- Snapshots of data can be written to optical or USB using our technology to provide a lifecycle version control solution
- These devices allow you to recover a set of point-in-time files as well as restore a whole server or Virtual Machine (VM) image

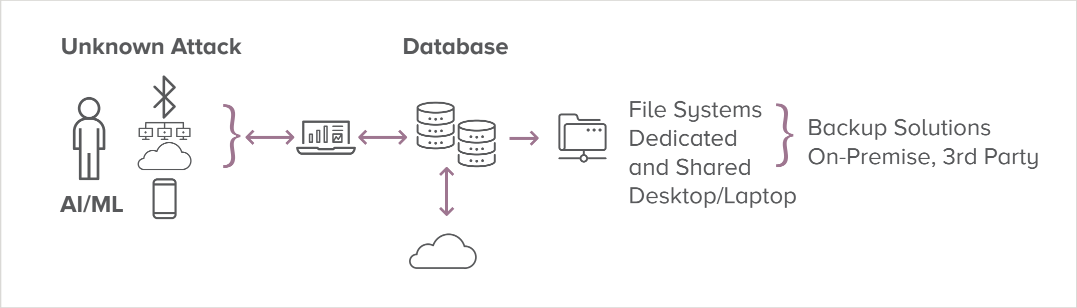
What should an organization look for in an on-premise, data management solution?

- The solution should combine the latest in robotics, software and engineering.
- It should be able to be tailored to any volume and workflow requirements.
- It should have the specialized technology and customized architecture solutions that allow it to process all data types, providing flexibility to transfer data to other form factors.
- It should be constantly iterating new versions of API (Application Programming Interface) and SDK (Software Development Kit) DevOps tools to enable processes and communications for improved usability to meet industry standard and regional technology needs around the globe.

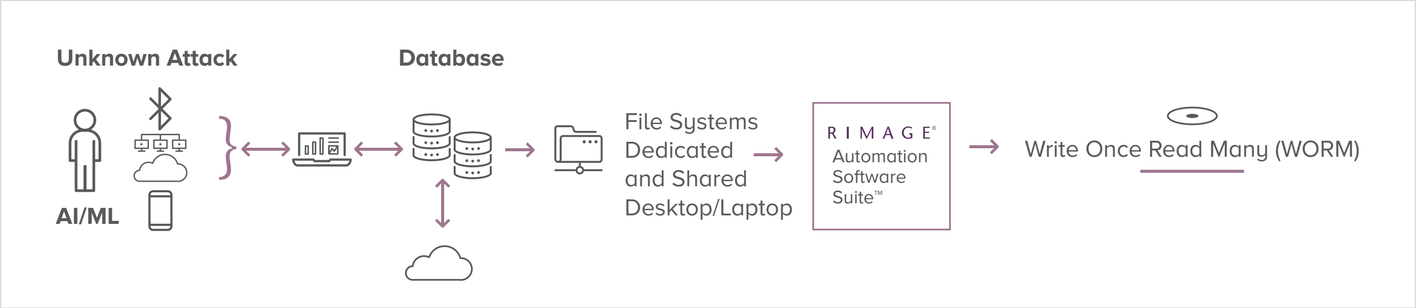
Conclusion

It's impossible to prevent ransomware attacks with 100% success. That's why it's critical to have a comprehensive data security strategy that allows you to back up, store and archive your data in multiple formats and locations. One of the key elements of the data security tool set is removeable, on-premise data management. Organizations should look for a removeable, on-premise data management solution with global reach, a proven track record, and a commitment to continuing innovation. Rimage offers a product portfolio to address concerns with ransomware. Contact our solutions team to learn more about how to leverage the Rimage technology suite as a part of your defense¬¬¬ to combat ransomware attacks. Contact Us.

Common Scenario



RIMAGE Solution



RIMAGE®

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