zadara + MANAGECAST

WORRIED ABOUT RANSOMWARE?
DON'T LEAVE YOUR RECOVERY TO CHANCE.

Ransomware attacks make up over a third of all reported cyberattacks in 2020. Downtime from these attacks are only increasing for organizations. To learn more about the threat and techniques IT experts on the frontlines rely on, we spoke with cloud backup and disaster recovery expert, Nathan Golden, the owner of Managecast Technologies. An award winning Veeam service provider, Managecast specializes in data protection, cloud backup and disaster recovery, and offers Zadara with Veeam Object storage immutability.

"Over the last three years the number one reason for restores within our customer base has been ransomware related," Nathan Golden, owner of Managecast reports. You don't need to look far to hear about the latest successful ransomware attack. Organizations are taking this threat seriously; nearly 80% of new customers or prospects that come to Managecast are looking for proactive ransomware protection. "Ransomware is an issue that we all see on the news. Companies that contact us want to make sure it is not impacting their environments," he shares.

> *"Over the last three years the number one reason for restores within our customer base has been ransomware related."*
>
> **Nathan Golden**
> **Owner, Managecast**

EMPLOYEE EDUCATION IS THE FIRST STEP

So how do you protect your organization against these types of attacks? Golden says it starts with employee education. In 9 out of 10 cases, organizations are affected when a well-intentioned user clicks on a malicious link that they shouldn't have, introducing a payload, says Golden. For this reason, he recommends employee education as the first step to protect your company. There are great resources out there like KnowBe4 that can help employees identify and avoid human errors, he shares. Employee access is another important element as is creating a culture of data protection, says Golden. It is all too common for employees, especially at small to mid-sized companies, to have more access than is required. Organizations can mitigate risk to their environments by limiting employees' permission so that in the case of a ransomware attack, you've now limited how far the malware can travel.
But the prevalence of successful ransomware attacks reminds us that backup and recovery must be core to your defense strategy. "When all else fails, even if you've invested in the right technologies, backup and restore is your last resort," says Golden.

WHAT TO LOOK FOR WITH BACKUP AND RESTORE

While many recommend air gaps and tape, to disconnect the media from the backup, Golden recommends limiting the need for human intervention. Make sure you model isn't introducing other risks and the potential for human error, he cautions. "Anytime you are introducing human intervention that is a step backwards," says Golden. Veeam + Zadara Object Storage Immutability offered by Managecast ensures backup integrity by stopping stored objects from being deleted or overwritten during a specific retention timeframe. With Object Storage Immutability enabled on a container, it is impossible to modify or shorten the retention period for an existing object. Immutability ensures object version integrity and availability throughout the retention period – no matter how long.

Having a longer retention policy so you can go back to a version of your data is also a critical step, says Golden. This is because ransomware can remain dormant and undetected, in some cases for months. "In most cases, they [impacted companies] are not detecting it until it has impacted their environment." For this reason, if you're doing your regular backups, you could be introducing undetected malware to your offsite backup.

BACK IN BUSINESS FASTER WITH BACKUP + DISASTER RECOVERY

“What is eye-opening to many organizations today, is that when they are hit, if they only have backups they are usually down for a minimum of a couple of days,” says Golden. Many underestimate the level of effort it takes to do recovery. While backups give you the ability to recover, with a disaster recovery (DR) solution your recovery will be much faster. If you need your recovery time to be quicker than a few days, this is where DR comes in. “It can mean the difference between minutes or days,” shares Golden.

THINK ABOUT RECOVERY BEFORE YOU SEE THE FIRE

Beyond ransomware, natural disasters also serve as a reminder of the importance of backup and DR. Golden shared, “I’ve had customers calling us after physically loading servers in the back of their cars to outrun a fire as they are being evacuated.” This is why we help our customers proactively think about their Recovery Time Objective (RTO) and Recovery Point Objective (RPO). “We want to help companies through these things before they see the fire.”Our customers have had several ransomware events during the pandemic, says Golden. Many customers are seeing how their risk profile has changed with more employees working from home and how their environments have changed. “I have not heard of any of our customers that had to pay the ransom,” he shared.

DATA IMMUTABILITY AND AIR GAP PROTECTION FOR BUSINESS-CRITICAL DATA

Managecast takes on the ownership of managing backups and DR to help take the load off of the IT teams. “We know that in IT your work is never done. So, we help our customers think through things they have not thought of,” says Golden.

Zadara is proud to partner with Managecast and Veeam to offer users the ability to create a scalable, cost-effective backup repository with multiple tiers of storage that can be optimized for performance or capacity. Thank you, Nathan, and Managecast for this interview and perspective.To learn more about how Managecast protects customers with Veeam + Zadara visit: https://www.zadara.com/solutions/veeam-backup/. And check back later this month for details on an upcoming webinar with the Managecast team.