

# THE TECHSLAYER

## CHRONICLES

RISE OF THE  
IMMUTABLE HERO



 **ActualTech**  
MEDIA

BROUGHT TO YOU BY

 rubrik

 **NetApp**®



# The TechSlayer Chronicles

## Rise of the Immutable Hero

Copyright © 2022 by ActualTech Media

All rights reserved. This book or any portion may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

### ActualTech Media

6650 Rivers Avenue Ste 105 #22489  
North Charleston, South Carolina  
29406-4829  
www.actualtechmedia.com

### Author

**Scott D. Lowe**

Scott D. Lowe is the CEO and Lead Analyst for ActualTech Media. Since 1994, Scott has helped organizations of all stripes solve critical technology challenges. He has served in a variety of technical roles, spent ten years as a CIO, and has spent another thirteen as a strategic IT consultant in higher education. Today, his company helps educate IT pros and decision makers and brings IT consumers together with the right enterprise IT solutions to help them propel their businesses forward.

### Special Contributions From:

**Steven Fleischman** -Sr Alliance Marketing Manager  
**Ramesh Chitor** - Sr Director of Strategic Alliances  
**Bruce Shaw** - Busines Development Manager - Data Security Alliances, US Central  
**Sterling Wilson** - Busines Development Manager - Data Security & Management, US Public Sector  
**Andrew Paul** - Busines Development Manager - Data Security Alliances, US East  
**Numi Castillo** - Busines Development Manager - Data Security Alliances, US West  
**Pierre-Francois Gugliemli** - Field CTO, Alliances  
**Ben Kendall** - Alliances Technical Partner Manager  
**Blaine Schultz** - Global Alliances Sales, Data Protection and SAN Solutions  
**Chris Maino** - Sr Solutions Architect Manager

### Art & Illustration

**Eric M. Strong**

### Editors

**Keith Ward**  
**Wendy Hernandez**

### Senior Director of Content

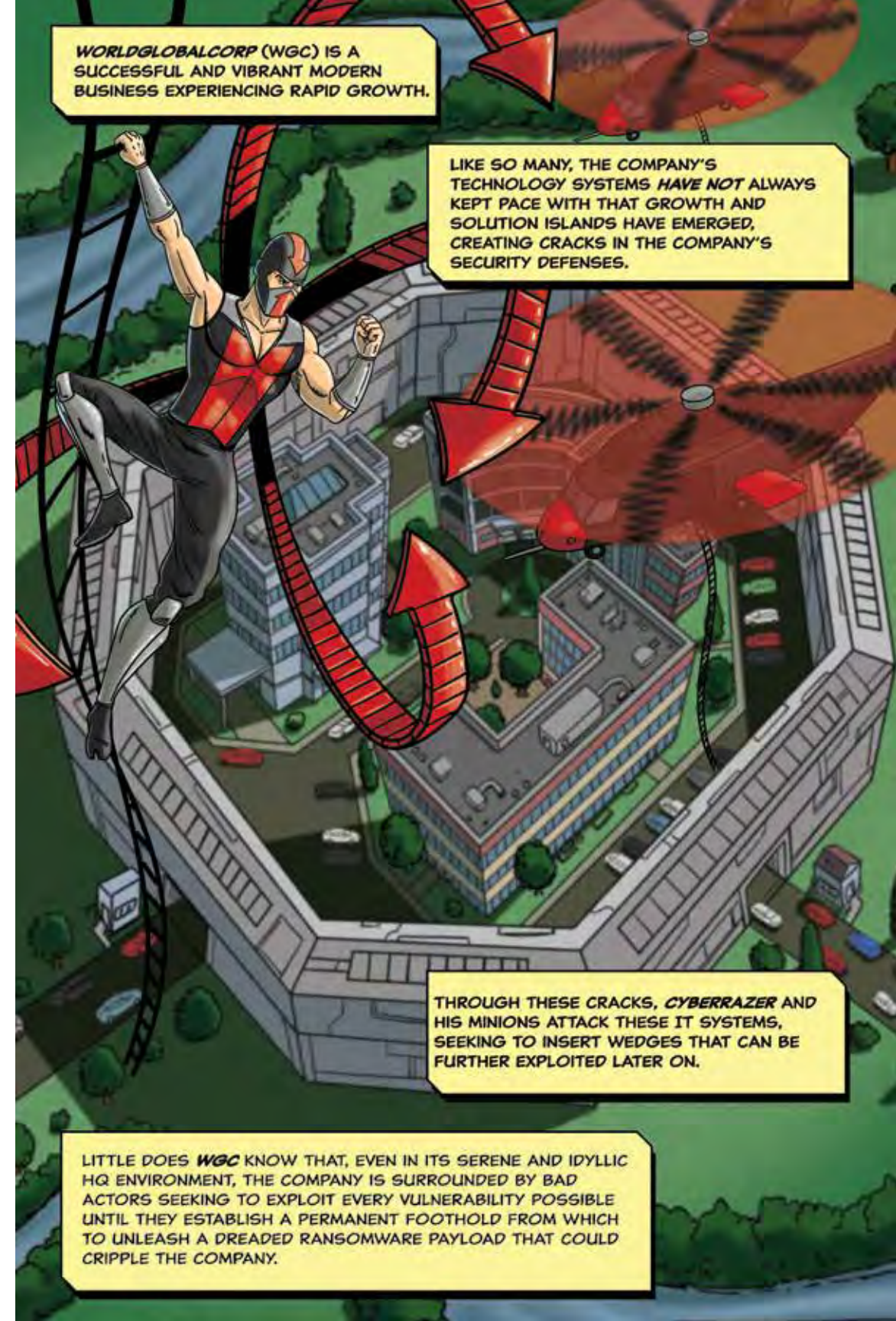
**Katie Mohr**



### About ActualTech Media

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services. ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience. Our leadership team is stacked with former CIOs, IT Managers, architects, subject matter experts and marketing professionals who help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you are an IT marketer and you'd like your own custom content, please visit us at [www.actualtechmedia.com](http://www.actualtechmedia.com).









TWO WEEKS LATER ...

THAT'LL DO THE TRICK!

WOW! THAT WAS QUICK!

ARE YOU SOME KIND OF SECURITY SUPERHERO OR SOMETHING?

THIS AUTOMATED SECURITY AWARENESS TOOL WILL GIVE USERS THE KNOWLEDGE THEY NEED TO FEND OFF PHISHING ATTEMPTS. IT WORKS FOR EVERYONE HERE, AS WELL AS OUR WORK-FROM-HOME TEAM MEMBERS.

IT WASN'T JUST THE DESKTOP ENVIRONMENT, THOUGH. ALL ACROSS WGC, INFRASTRUCTURE SILOS CREATED NEW RISK FOR THE COMPANY.

... AND THANKS TO OUR NEW AUTOMATED SCANNING TOOLS, WE'RE NO LONGER TWO YEARS BEHIND IN APPLYING CRITICAL FIRMWARE UPDATES TO OUR SERVERS.

I CAN'T BELIEVE WE'D NEVER DONE FIRMWARE UPDATES!

NO KIDDING! JUST THIS MORNING, A BRAND NEW ZERO DAY VULNERABILITY WAS DISCOVERED ON THE OLD FIRMWARE VERSION THAT WAS IN ALL OF OUR SERVERS.

THERE ARE SO MANY OPPORTUNITIES FOR INFILTRATION. CONSTANT VIGILANCE INTERRUPTED BY JUST ONE MISSTEP CAN HAVE TRAGIC CONSEQUENCES.

I NEED TO GO MEET WITH THE STORAGE TEAM.

THEY'RE REALLY STRUGGLING WITH HOW WE MOVE FORWARD WITH A NAS CONSOLIDATION PROJECT.

THAT ONE IS EASY!

YES IT IS!

DANSA! HAPPY YOU'RE HERE.

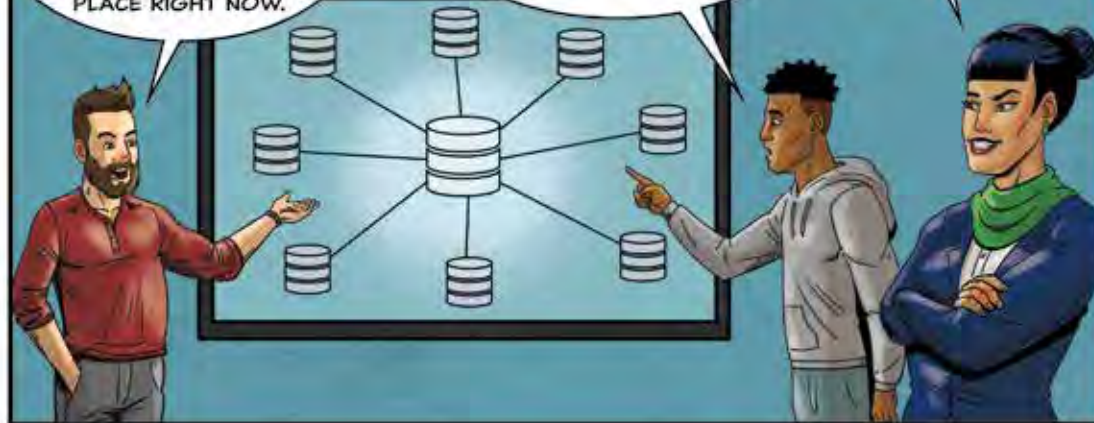
FOR THE LAST SIX HOURS, WE'VE BEEN STUDYING THE THROUGHPUT CHARACTERISTICS AND ARCHITECTURE SCHEMATICS FOR EVERY NAS SYSTEM ON THE MARKET AND WE'RE NO CLOSER TO A DECISION THAN WE WERE WHEN WE STARTED.

HI NOAH! SURE, THOSE ARE IMPORTANT, BUT LET'S CUT TO THE CHASE. WHAT DO YOU WANT TO ACTUALLY GET DONE?

WELL, WE NEED TO MAKE THIS WHOLE MESS SIMPLER. WE HAVE NAS SYSTEMS FROM EIGHT VENDORS ALL OVER THE PLACE RIGHT NOW.

WE HAVE ISLANDS OF NAS EVERYWHERE. IT'S EXPENSIVE. IT'S COMPLEX. SIMPLY PUT, IT'S INEFFICIENT.

FROM A SECURITY STANDPOINT, IT'S A TICKING TIMEBOMB.







LET'S HEAD TO THE COURTYARD AND GET SOME FRESH AIR.



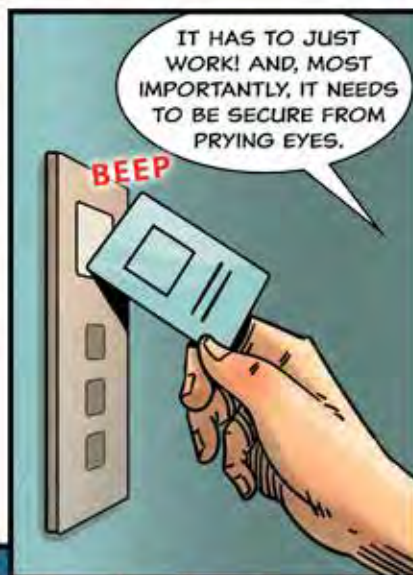
WE ALSO NEED A SOLUTION THAT WORKS AS WELL IN THE CLOUD AS IT DOES ON-PREMISES.



AND IT NEEDS TO SUPPORT 128GB FIBRE CHANNEL!

WHY?

OK ... YOU GOT ME THERE ...



IT HAS TO JUST WORK! AND, MOST IMPORTANTLY, IT NEEDS TO BE SECURE FROM PRYING EYES.



STORAGE IS JUST ONE NEED ON THE DATA FRONT, THOUGH. WE'RE ALSO HAVING SERIOUS CHALLENGES WITH BACKUP AND RECOVERY, AS WELL AS A LOT OF RISK.

WHAT KINDS OF RISKS AND CHALLENGES DO WE HAVE RIGHT NOW?



WHERE DO I BEGIN?!

FIRST, WE'RE NOT STAYING INSIDE OUR BACKUP WINDOW ANYMORE AND IT'S IMPACTING PRODUCTION. WHEN WE HAVE TO RECOVER A FILE, IT TAKES FOREVER; IF WE HAD TO DO A SIGNIFICANT RECOVERY, IT WOULD TAKE WEEKS TO GET EVERYTHING BACK.

IT DOESN'T REALLY SUPPORT USING THE CLOUD AS A TARGET, SO WE HAVE TO KEEP THROWING STORAGE AT THE BACKUP SYSTEM JUST TO KEEP UP WITH OUR CRAZY DATA GROWTH.

TO MAKE MATTERS WORSE, WE HAVE FIVE DIFFERENT BACKUP SOLUTIONS RIGHT NOW. NONE OF THEM COVER ALL OF OUR SYSTEMS.

ALL OF THESE SYSTEMS MEAN THAT WE'RE SPENDING ENGINEER TIME ON FIVE BACKUP TOOLS RATHER THAN ON OUR DIGITAL TRANSFORMATION WORK.

SERIOUSLY?

OH ... AND ... WELL ... OUR BACKUPS AREN'T AIR-GAPPED.





YEAH... IF LAST YEAR'S PAYROLL DEBACLE HAD BEEN RANSOMWARE INSTEAD, WE WOULDN'T BE HAVING THIS PLEASANT CONVERSATION RIGHT NOW.



WAIT FOR MY SIGNAL.

WE'D BE OUT OF BUSINESS AND SOLD FOR PARTS.



I KNEW IT WAS BAD, BUT NOT THIS BAD!



IT'S TIME FOR US TO MODERNIZE THESE SYSTEMS.



EVERY PART OF IT TODAY IS INTEGRAL TO A STRONG SECURITY POSTURE. OUR DATA MANAGEMENT AND DATA PROTECTION SYSTEMS ARE NO EXCEPTION.



DID I MISS A MEMO?



AS WE EVOLVE, OUR NEW INFRASTRUCTURE NEEDS TO TAKE A ZERO TRUST APPROACH FROM END TO END.



ZERO TRUST? WHAT DOES THAT MEAN?

IT MEANS TWO THINGS, REALLY.



FIRST, THAT WE ALWAYS ASSUME THAT THE INFRASTRUCTURE IS SOMEHOW COMPROMISED.



SECOND, THAT SYSTEMS COME OUT OF THE BOX WITH NOTHING ENABLED BY DEFAULT.



WELL, THAT DOESN'T SOUND ALL THAT POSITIVE ...

ZERO TRUST ISN'T MEANT TO IMPLY THAT INTERNAL TEAMS AREN'T DOING THEIR JOBS. INSTEAD, IT'S A TACIT ADMISSION THAT EVERYTHING—EVEN THE BEST SOLUTIONS ON THE MARKET—HAS FLAWS, A FACT THAT HAS BEEN PROVEN TIME AND AGAIN.



IT'S MEANT TO FORCE ORGANIZATIONS TO REALLY REFLECT ON THEIR ENVIRONMENTS.



RIGHT NOW, OUR OLD SYSTEMS ARE DEPLOYED AND TEAMS SHORE THEM UP BY LOCKING THEM DOWN AFTER DEPLOYMENT.



BUT, WE JUST SAW REALITY STRIKE! THE VERY FIRMWARE UPDATES THAT WE JUST UPDATED HAD A ZERO DAY ATTACK THAT WAS PUBLISHED RECENTLY.

WHEN WE DEPLOYED THOSE SYSTEMS, WE "HARDENED" THEM. WE TOOK STEPS TO CLOSE HOLES.



ZERO TRUST PRINCIPLES MEAN THAT WE HAVE TO TAKE ACTIVE STEPS TO MAKE THESE SYSTEMS ACCESSIBLE.

WE APPROACH IT USING A PRINCIPLES OF LEAST PRIVILEGE STANCE SO THAT SYSTEMS HAVE ONLY WHAT THEY NEED TO OPERATE... AND NO MORE.

YOU KNOW, AS WE CONSIDER NEW OPTIONS, WE REALLY NEED TO BE THINKING ABOUT HOW WE CAN BE MORE PROACTIVE IN IDENTIFYING POTENTIAL ATTACKS THAT WE MIGHT NOT EVEN KNOW ARE TAKING PLACE.

ABSOLUTELY, DANGSA! WE NEED A TOOL THAT HELPS US IDENTIFY PATTERNS THAT COULD INDICATE THAT A COMPROMISE HAS ALREADY TAKEN PLACE AND THAT CAN IDENTIFY OTHER POTENTIALLY MALICIOUS ACTIVITY.

SO MANY LEGACY BACKUP TOOLS ARE SINGLE-MINDED AUTOMATONS THAT JUST MOVE DATA FROM PRODUCTION TO BACKUP WITHOUT REALLY CONSIDERING MUCH BEYOND THAT.

OUR NEW TOOL NEEDS TO BE AN ACTIVE PARTICIPANT IN OUR SECURITY PROGRAM, HELPING US FLAG SUSPICIOUS ACTIVITY SO THAT WE CAN AVOID ATTACKS.

BUT THERE'S NO TOOL ON THE MARKET THAT CAN GUARANTEE THAT WE'LL NEVER FALL VICTIM TO A RANSOMWARE ATTACK.

YOU'RE ABSOLUTELY RIGHT, SAM. NO TOOL CAN EVER GIVE THAT IRONCLAD GUARANTEE.

AND, IF THEY DID, WELL... I DON'T THINK I'D BELIEVE THEM.

THAT'S WHY IT'S CRITICAL THAT WE THINK ABOUT ALL OF THIS IN LAYERS AND IDENTIFY WHAT STEPS WE WOULD TAKE IN A WORST-CASE SCENARIO WHILE WE'RE DESIGNING THE SOLUTION.

IN OTHER WORDS, WHAT HAPPENS WHEN THE WORST HAPPENS?

EXACTLY! IF OUR DEFENSES FAIL AND WE'RE HIT WITH RANSOMWARE, HOW DO WE RECOVER?

HE'S RIGHT BEHIND ME!

QUICK, CLOSE THE DOOR!

HURRY!

DO EITHER OF YOU KNOW WHAT WE SHOULD SELECT TO REPLACE OUR OLD SYSTEMS?

WE DO! WE'RE GOING TO DEPLOY RUBRIK AND NETAPP ONTAP AND STORAGEGRID!

SLAM!

WITH RUBRIK AND NETAPP SUPPORTING US, WE'LL GET BEST-IN-CLASS STORAGE AND DATA PROTECTION.

WE'LL GET AIR-GAPPED AND IMMUTABLE BACKUPS THAT CAN'T BE IMPACTED IF WGC IS EVER HIT BY RANSOMWARE.

EVEN BETTER, WE GET TO FIX THE BACKUP WINDOW PROBLEM WE'VE BEEN EXPERIENCING WITH OUR OLD SOLUTION. RUBRIK FULLY SUPPORTS NETAPP SNAPPDIFF 3.0, WHICH TAKES BACKUPS BASED ON FULL-VOLUME DELTA SNAPSHOTS.

THAT WILL MAKE BACKUPS FASTER BY ORDERS OF MAGNITUDE SINCE SNAPPDIFF'S FILE CHANGE API COMPARES JUST THE PREVIOUS BACKUP SNAPSHOT WITH THE CURRENT ONE AND ONLY BACKS UP WHAT'S CHANGED.

LET'S GET TO WORK!

SHOULD I GET A COSTUME?





NOW, WE JUST HAVE TO MOVE OUR DATA TO NETAPP AND RUBRIK.



AND THAT SHOULD JUST ABOUT DO IT.

MULTI-FACTOR AUTHENTICATION HAS BEEN ENABLED!



THIS WAS A LONG DAY, BUT I THINK WE'RE JUST ABOUT READY!

I'M JUST PUTTING THE FINISHING TOUCHES ON EVERYTHING ...



EXCELLENT WORK, TEAM! I KNOW EVERYONE WORKED HARD TO GET THIS DONE!

IT FEELS LIKE WE'RE FORGETTING SOMETHING.



RUBRIK WILL HAVE EVERYTHING, INCLUDING ALL OF OUR METADATA, AND WE'LL BE FULLY PROTECTED!

YOU'RE THE HERO, SAM!



YOU'RE SURE YOU DIDN'T MISS ANY STEPS ON THE NETAPP DEPLOYMENT, RIGHT?

OF COURSE!

WOULD YOU LIKE TO CHANGE THE DEFAULT PASSWORD? (YES/NO)

LITTLE DID THE TEAM KNOW THAT HUMAN ERROR ISN'T LIMITED TO END USERS. IT PROS, EVEN IT SUPERHEROES ARE ONLY HUMAN, AFTER ALL...



A FEW DAYS LATER ...

WHAT THE HECK?

MY COMPUTER JUST FROZE AND THERE'S A LOCK ON MY SCREEN.

WE'RE ON IT!

DO YOU SEE THAT? IT LOOKS LIKE SOMEONE FORGOT TO CHANGE A DEFAULT ADMIN PASSWORD.

WOULD YOU LIKE TO CHANGE THE DEFAULT PASSWORD? (YES/NO)

I SAW IT AND WE'LL FIX IT, BUT WE'RE PREPARED FOR THIS! FOLLOW ME.

OUT OF THE WAY! I'LL TAKE CARE OF THIS ONE MYSELF!

CYBERRAZER IS ATTACKING!

WE CAN'T DESTROY THIS ONE!

IT'S TIME TO DEPLOY OUR RECOVERY PLAN.

WHAT'S HAPPENING?

IT'S STARTING TO REBUILD ITSELF!

THIS RUBRIK IS UNSTOPPABLE! LET'S GET OUT OF HERE!









## TOP 5 TAKEAWAYS

1. DATA IS THE LIFEBLOOD OF EVERY MODERN ORGANIZATION.
2. IT'S NOT A QUESTION OF IF A RANSOMWARE ATTACK WILL HAPPEN, BUT WHEN. THE ONLY WAY THAT ORGANIZATIONS CAN SURVIVE ONE AND NOT PAY THE RANSOM IS TO HAVE CUTTING-EDGE SECURITY AT THE POINT OF DATA AND AN IMPENETRABLE LAST LINE OF DEFENSE BACKUP.
3. EVERY ORGANIZATION'S LAST LINE OF DEFENSE NEEDS TO BE BUILT ON A ZERO TRUST, IMMUTABLE ARCHITECTURE WITH DEFAULT SETTINGS AND FEATURES TO GUARANTEE THE AVAILABILITY OF DATA EVEN IN A FULLY COMPROMISED ENVIRONMENT.
4. STATE-OF-THE-ART DATA PROTECTION IS ABSOLUTELY CRITICAL, BUT IT DOES LITTLE GOOD WITHOUT STATE-OF-THE-ART RANSOMWARE REMEDIATION, THREAT HUNTING, SENSITIVE DATA DISCOVERY, AND ORCHESTRATED DATA RECOVERY BUILT IN.
5. CONSOLIDATION OF DISPARATE SILOED SYSTEMS FOR SUCH THINGS AS NAS AND DATA PROTECTION INTO INDUSTRY-LEADING, INTEGRATED SOLUTIONS PROVIDED BY JOINT PARTNERS WILL REDUCE RISK AND LOWER TCO. RUBRIK AND NETAPP TOGETHER CHECK ALL THE BOXES NEEDED FOR DATA MANAGEMENT, PROTECTION, VISIBILITY, AND RECOVERY.

