ActualTech MEDIA

THE TECHSLAYER CHRONICLES

DIGITAL DEFENDERS: SECURING HYBRID CLOUD INFRASTRUCTURE FROM ALIEN FORCES

BROUGHT TO YOU BY

Hewlett Packard Enterprise

intel

THE TECHSLAYER CHRONICLES™

DIGITAL DEFENDERS

SECURING HYBRID CLOUD INFRASTRUCTURE FROM ALIEN FORCES

AUTHOR

Lewis Helfand

Lewis Helfand is a comic book writer from Narberth, Pennsylvania. He is the author of *Wasted Minute*, *Unmasked Seeking Same*, and the award-winning, *Nelson Mandela: The Unconquerable Soul*. He spends his days either watching British Bake with his wife or watching his three cats destroy nearly everything.

WITH SPECIAL CONTRIBUTIONS FROM

Cole Humphreys, HPE Global Platform Security Product Manager

Rick Larsen, Intel Corporation Enterprise Marketing Director

ART & ILLUSTRATION

Eric M. Strong

GRAPHIC DESIGN

Olivia Thomson

EDITOR

Wendy Hernandez

SENIOR DIRECTOR OF CONTENT

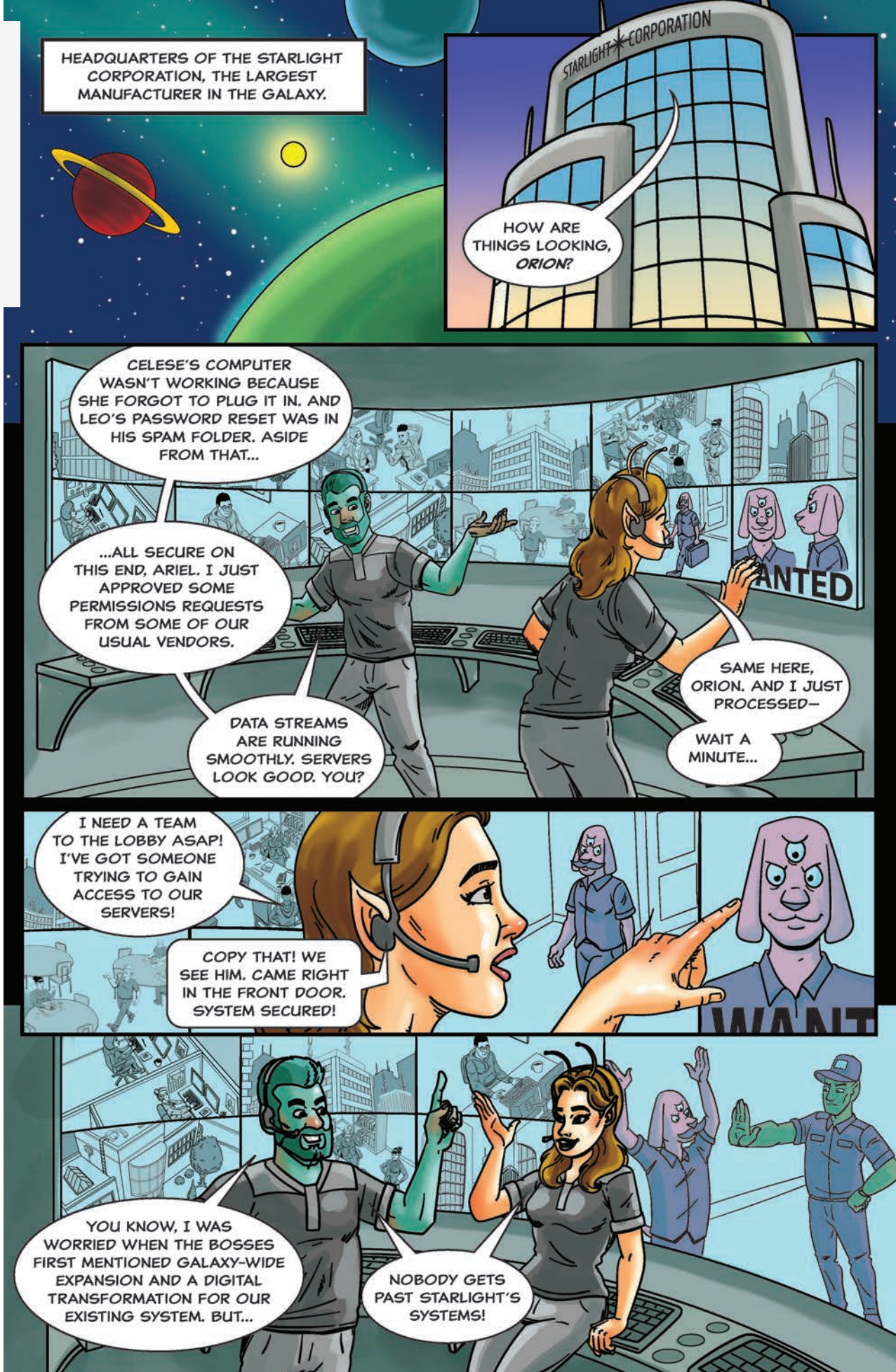
Katie Mohr

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future company, 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 a technology marketer and you'd like more information about our webinar lead generation programs and content opportunities, please visit us at www.actualtechmedia.com.

www.actualtechmedia.com



WE'VE GOT NOTHING TO WORRY ABOUT.

SOMEWHERE AT THE EDGE OF THE GALAXY...

LOOKS LIKE SOMEONE IS GETTING PAST STARLIGHT'S SYSTEM TODAY...US!

EVERYTHING'S READY ON MY END. LET'S DO THIS.

```
// instance calling static OK
  // instance calling instance OK
  public void i2() {
    s1();     // starlight systems.s1();
    //n;     // this.n;
    return;
  }
  // install virus versions of overload() based on their
  // list of parameters
  public void
    System.out.println("overloaded()");
  overload((byte)1);
  overload((short)1);
  overload(1);
  overload(1L);
  overloa (1.0F);
```

ACCESS GRANTED

WHAT'S WRONG?

I'M SHOWING THE NEBULA FACTORY IS SUDDENLY OFFLINE

WHICH PART?

THE SERVER ROOM?

THE FACTORY FLOOR?

SYSTEM OFFLINE

THREAT DETECTED

I MEAN THE WHOLE FACTORY WENT DOWN. OPERATIONS JUST...STOPPED.

THAT'S IMPOSSIBLE! LET ME GET COMET ON THE LINE. SHE WORKS OUT OF THAT LOCATION, AND SHE CAN GET US SOME EYES ON THE GROUND.

I DON'T KNOW WHAT TO TELL YOU, ARIEL.

SOMEONE TOOK CONTROL OF THE ENTIRE FACTORY. AND A RANSOM CALL CAME IN DEMANDING 12 MILLION.

STARLIGHT CORPORATION'S NEBULA FACTORY AT THE EDGE OF THE GALAXY.

12 MILLION?!? ORION AND I ARE WORKING ON THE PROBLEM, COMET. WE JUST NEED A BIT OF TIME TO—

TIME MIGHT BE THE ONE THING YOU DON'T HAVE. THE BIG BOSSES ARE PUSHING TO PAY THE RANSOM.

SAID WE CAN'T AFFORD TO LOSE EVEN A DAY OF PRODUCTION.

I'M GONNA SEE IF I CAN REBOOT NEBULA'S SYSTEM. CAN YOU FIELD THOSE OTHER CALLS, ORION? WHATEVER IT IS, IT CAN'T BE AS URGENT AS THIS.

DING!

DING!

DING!

DING!

PROBABLY JUST LEO FORGETTING HIS PASSWORD AND LOCKING HIMSELF OUT AGAIN. REMIND HIM THE RESET LINK IS IN HIS SPAM FOLDER.

I UNDERSTAND THAT YOU'RE LOCKED OUT OF ALL THE INVENTORY REPORTS. BUT EVERYONE AT THE NEBULA FACTORY IS HAVING SOME ISSUES AT THE MOMENT. WE'RE WORKING TO RESTORE—

I'M NOT WORKING OUT OF NEBULA! I'M WORKING REMOTELY JUST OUTSIDE OF MARS!! AND I CAN'T ACCESS ANYTHING!!

SALES REPORTS DOWN, TOO, ARIEL. AND THE VENUS OFFICES ARE LOCKED OUT OF OUR SYSTEM.

AND THE SERVERS JUST CRASHED. WE NEED HELP. WE NEED...

THE TECHSLAYERS!!!!

A FEW SECONDS LATER...

THANKS FOR GETTING HERE SO QUICKLY!

OUR PLEASURE. YOU FORGET YOUR PASSWORD?

IT HAPPENS TO THE BEST OF US. EVEN CAPTAIN OPS GETS LOCKED OUT OF HER EMAIL ON OCCASION.

TRY TO IGNORE THE SERVER. YOU MENTIONED STARLIGHT HAS EXPANDED A LOT IN THE LAST YEAR. YOU'VE GOT FACTORIES OPERATING AT THE EDGE OF THE GALAXY NOW.

CAN ONE OF YOU GET US A LIST OF ALL THE ADDITIONAL SECURITY YOU PUT IN PLACE TO MANAGE EVERYTHING?

WELL...UMM...OUR COMPANY EXPANSION DIDN'T REALLY FACTOR IN ANY ADDITIONAL SECURITY MEASURES. WE'RE SORT OF A SMALL DEPARTMENT, AND WE CAN'T BE EVERYWHERE.

BUT THE TWO OF US HAVE BEEN MANAGING JUST FINE LIKE THIS FOR A WHILE. AT LEAST...IT SEEMED LIKE WE WERE MANAGING.

SO, YOU'VE GOT SYSTEMS HERE AT HQ AND AT ALL YOUR FACTORIES AND DATA CENTERS AND WAREHOUSES.

ANY REMOTE WORKERS?

UHH... WE'VE GOT A FEW...

...THOUSAND.

50% OF OUR WORKFORCE HAS BEEN REMOTE FOR THE LAST FEW MONTHS. MOST ARE LOCATED ON THE OUTSKIRTS OF MARS AND MERCURY.

LET ME GUESS...THEY'RE ALL USING THEIR OWN DEVICES, TOO?

WELL...NOT ALL. WE KNOW THINGS HAVE BEEN CHANGING. WE KNOW THERE'S A NEED TO TRANSFORM OUR COMPANY. BUT THE WAY FORWARD...???

I GET IT. THE WAY FORWARD CAN BE LESS CLEAR. YOU'D BE SURPRISED AT HOW OFTEN WE ENCOUNTER THIS SORT OF THING.

COMPANIES START EXPANDING. THEY GROW THEIR DIGITAL FOOTPRINT. BUT THEY DON'T REALIZE THEY NEED TO EXPAND THEIR SECURITY WITH THAT GROWTH.

THERE ARE SO MANY MORE THREATS OUT THERE. VULNERABILITIES AND ATTACK SURFACES CAN MULTIPLY. YOU NEED TO MONITOR EVERYTHING.

SORRY, WHEN YOU SAY EVERYTHING???

I MEAN EVERYTHING! FROM THE EDGE TO THE CLOUD.

A WEBSITE IS ATTACKED ALMOST EVERY SECOND. AND ALMOST HALF OF ALL CYBERCRIMES ORIGINATE IN THE CLOUD. IT'S A BREEDING GROUND FOR ATTACKS.

SO, WHAT DO WE DO? IT LOOKS LIKE THEY'RE CRASHING OUR ENTIRE SYSTEM!

AND THEY'RE NOT JUST SLOWING DOWN OUR BUSINESS AND COSTING US MONEY, BUT THEY'RE COSTING US THE TRUST OF MILLIONS OF OUR CUSTOMERS, TOO.

WE ONLY KNOW ONE SUREFIRE WAY TO PROTECT YOUR SYSTEM...HPE PROLIANT COMPUTE SECURITY!

AND I KNOW JUST WHERE TO START! I NEED A LIST OF ALL OF STARLIGHT'S LOCATIONS—ALL YOUR FACTORIES AND WAREHOUSES AND DATA CENTERS AND OFFICES. AND I NEED IT NOW!

IS THIS THE FULL LIST OF STARLIGHT'S LOCATIONS? JUST GIVE ME A FEW MINUTES AND I'LL SWING BY ALL OF THEM AND—

SORRY...DID YOU SAY A FEW MINUTES? WE'VE NOW GOT DOZENS OF LOCATIONS SPREAD OUT ALL OVER THE GALAXY.

DOZENS, HUH? I GUESS IT WON'T TAKE ME THAT LONG THEN. I'LL BE BACK IN A FEW SECONDS!

IN ORDER TO REMOVE THE CONSTANT CONCERN ABOUT COMPUTE SECURITY IN TODAY'S COMPLEX ENVIRONMENT...

STARLIGHT CORPORATION

...YOU NEED SOMETHING WITH SECURITY FEATURES THAT COVERS EVERYTHING FROM THE SUPPLY CHAIN TO DELIVERY.

TRUE COMPUTE SECURITY HAS TO COME FROM THE GROUND UP.

AND THAT STARTS WITH A SECURE SERVER. IT STARTS WITH ADDING THE POWER OF HPE PROLIANT GEN11 SERVERS POWERED BY INTEL TO YOUR SYSTEMS.

SECONDS LATER...

SO...PROBLEM SOLVED? SYSTEM SECURED?

NOT QUITE YET.

WHAT YOU ALSO NEED IS VISIBILITY. AND CONTROL! CONTROL INTO EVERY USER AND EVERY DEVICE CONNECTED TO YOUR INFRASTRUCTURE.

WHAT THE SERVER DID WAS SET THE STAGE FOR THE FULL PLATFORM SECURITY THAT'S NEEDED.

BUT WE ALSO NEED TO ENSURE YOU CAN ACCESS YOUR ENVIRONMENT AND MAINTAIN CONTROL, SO THIS NEVER HAPPENS AGAIN.

REMEMBER THAT AS THE WORLD BECOMES MORE HYBRID...COMPUTE WON'T LOOK THE SAME.

CONNECTION RESTORED

YOU NEED DEVICE CONNECTIONS THAT ARE SECURE, AUTHENTICATED, AND ENCRYPTED EVERY TIME.

HPE GREENLAKE FOR COMPUTE OPS MANAGEMENT. TRUE "FLEET SECURITY" FROM FACTORY TO CLOUD. FROM THIS YOU CAN—

Overview

96 Server Groups

12

10

5280 Servers

48

Firmware Jobs

Activity

IT LOOKS LIKE WE CAN MANAGE THOUSANDS OF SERVERS AND EASILY ONBOARD THOUSANDS OF DISTRIBUTED DEVICES!

MANAGE USERS, THEIR ROLES, PERMISSIONS...VIEW THE HEALTH AND FIRMWARE STATUS OF ALL OUR SERVERS!

CRITICAL ISSUE DETECTED!

AND IT LOOKS LIKE A THREAT HAS ALREADY BEEN DETECTED THAT NEEDS TO BE DEALT WITH. IT'S GOT TO BE THOSE HACKERS THREATENING US AND DEMANDING A RANSOM!

YOU TWO JUST FOCUS ON GETTING THAT FACTORY UP AND RUNNING.

CAPTAIN OPS AND I WILL BE GLAD TO HANDLE THIS THREAT.

THE EDGE OF THE GALAXY...

OFFLINE

JUST A FEW MORE MINUTES AND WE'RE GONNA BE RICH!

YOU'RE SURE STARLIGHT IS GONNA PAY THE RANSOM?

OF COURSE, I'M SURE! WHAT CHOICE DOES IT HAVE?

HEY, IT LOOKS LIKE WE'VE SUDDENLY BEEN LOCKED OUT OF STARLIGHT'S SYSTEM.

THAT'S IMPOSSIBLE! GIVE IT A SECOND. OR TRY REBOOTING. DID YOU UNPLUG AND PLUG IN AGAIN?

IT'S PROBABLY JUST A GLITCH.

I'M AFRAID IT'S A BIT MORE THAN A GLITCH.

STARLIGHT'S ADMINS DECIDED TO REVOKE YOUR PERMISSIONS.

I'VE GOT TO HAND IT TO YOU. IT WAS SMART TARGETING A COMPANY LIKE STARLIGHT.

IT WAS, WASN'T IT? AS THE BIGGEST MANUFACTURER IN THE GALAXY, IT MEANT ITS IT INFRASTRUCTURE WAS ALSO THE BIGGEST AND THE MOST COMPLEX.

IT MEANT IT WOULD BE EVEN MORE CHALLENGING FOR THE COMPANY TO MONITOR INTERNAL AND EXTERNAL THREATS AND MANAGE EVERY SINGLE SERVER ACROSS ITS LANDSCAPE.

INCREASED BUSINESS AT MULTIPLE EDGES MEANS SIGNIFICANTLY MORE RISK EXPOSURE! EASY PICKINGS, RIGHT?

NOT ANYMORE!

I GUESS YOU DIDN'T COUNT ON STARLIGHT ADDING THE INTEL-POWERED HPE PROLIANT COMPUTE SECURITY.

YOU DIDN'T COUNT ON THE COMPANY BEING ABLE TO HANDLE THE COMPLEXITY OF MULTI-GENERATIONAL AND HYBRID IT ENVIRONMENTS.

NO! WE WERE RIGHT THERE! WE WERE IN ITS SYSTEM. WE WERE SO CLOSE!!

SO CLOSE, BUT SO FAR. YOU DIDN'T COUNT ON STARLIGHT REALIZING THAT HAVING A HIGHER LEVEL OF SECURITY AGAINST EVER-INCREASING THREATS IS NO LONGER JUST AN OPTION...

...IT'S ESSENTIAL!

THWACK!!

YOU KNOW WHAT THEY SAY...SECURITY IS ONLY AS STRONG AS THE LAYER BELOW THE POINT OF ATTACK.

AND I'D SAY STARLIGHT'S SYSTEM IS NOW STRONGER THANKS TO...

HPE PROLIANT COMPUTE DEVELOPED WITH INTEL. FUNDAMENTAL... UNCOMPROMISING... AND...PROTECTED!

DON'T FORGET DESIGNED WITH TRUSTED SECURITY IN MIND. I KNEW THEY'D SEE IT OUR WAY.

MONTHS LATER...

STARLIGHT✶CORPORATION

HOW ARE THINGS LOOKING, ORION?

THE NATURE OF THE EDGE INTRODUCES A WHOLE NEW SET OF ATTACK VECTORS.

INCOMING TRANSMISSION

DING DING!

SAME HERE. NOT SEEING ANYTHING TO WORRY ABOUT.

BUT LOOKING ALL SECURE ON THIS END, ARIEL. YOU?

PERHAPS I SPOKE TOO SOON.

IF IT'S CELESTE OR LEO...I'M NOT IN.

SHOULD WE BE CONCERNED? YOU TWO ONLY MAKE AN APPEARANCE WHEN THERE'S A PROBLEM, RIGHT?

HAHA! WE WERE JUST PASSING THROUGH. HAD TO DEAL WITH SOME MISCONFIGURED CLOUD STORAGE FOR A TECH COMPANY OVER ON NEPTUNE.

JUST WANTED TO CHECK IN WHILE WE WERE IN THE NEIGHBORHOOD. MAKE SURE STARLIGHT'S SYSTEMS ARE SECURED AND RUNNING SMOOTHLY.

I THINK YOU TWO CAN REST EASY...

OUR SYSTEM IS NOW TRULY SECURE FOR THE FIRST TIME. AND WE'VE GOT PEACE OF MIND AGAINST SECURITY THREATS.

THANKS TO INTEL AND HPE PROLIANT COMPUTE, TRUSTED SECURITY BY DESIGN.

BELIEVE ME, WE'RE NOW AWARE THAT SECURITY THREATS WILL CONTINUE TO EVOLVE, AND WE UNDERSTAND HOW CRITICAL IT IS TO UPGRADE LEGACY INFRASTRUCTURE.

WELL, IF YOU STILL HAVE ANY QUESTIONS, YOU KNOW WHAT TO DO.

VISIT THE HPE COMPUTE SECURITY PAGE AT WWW.HPE.COM/SECURITY/COMPUTE

OR TALK TO AN HPE SALES REPRESENTATIVE!

KEY TAKEAWAYS:

TAKE ACTION NOW: EVALUATE AND ASSESS YOUR HYBRID CLOUD ENVIRONMENT AND EXECUTE COMPREHENSIVE VULNERABILITY TESTS, INCLUDING AI-DRIVEN ATTACK SIMULATIONS TO PROTECT YOUR INFRASTRUCTURE.

ACT DECISIVELY: INITIATE AN INFRASTRUCTURE AUDIT TO ADD MORE CYBERSECURITY PROTECTION FROM ITS FOUNDATIONAL LEVELS. DO YOU HAVE LEGACY SYSTEMS THAT ARE VULNERABLE TO CYBER ATTACKS? IS IT THE TIME TO UPGRADE?

TAKE PROACTIVE STEPS: COLLABORATE WITH TRUSTED PARTNERS FOR ROBUST IT SOLUTIONS AND PROVEN COMPUTE SECURITY TECHNOLOGIES.