

AUTUMN 2022

Solutions

by **ZONES**

**SECURING
YOUR BUSINESS**
in the Modern IT Landscape

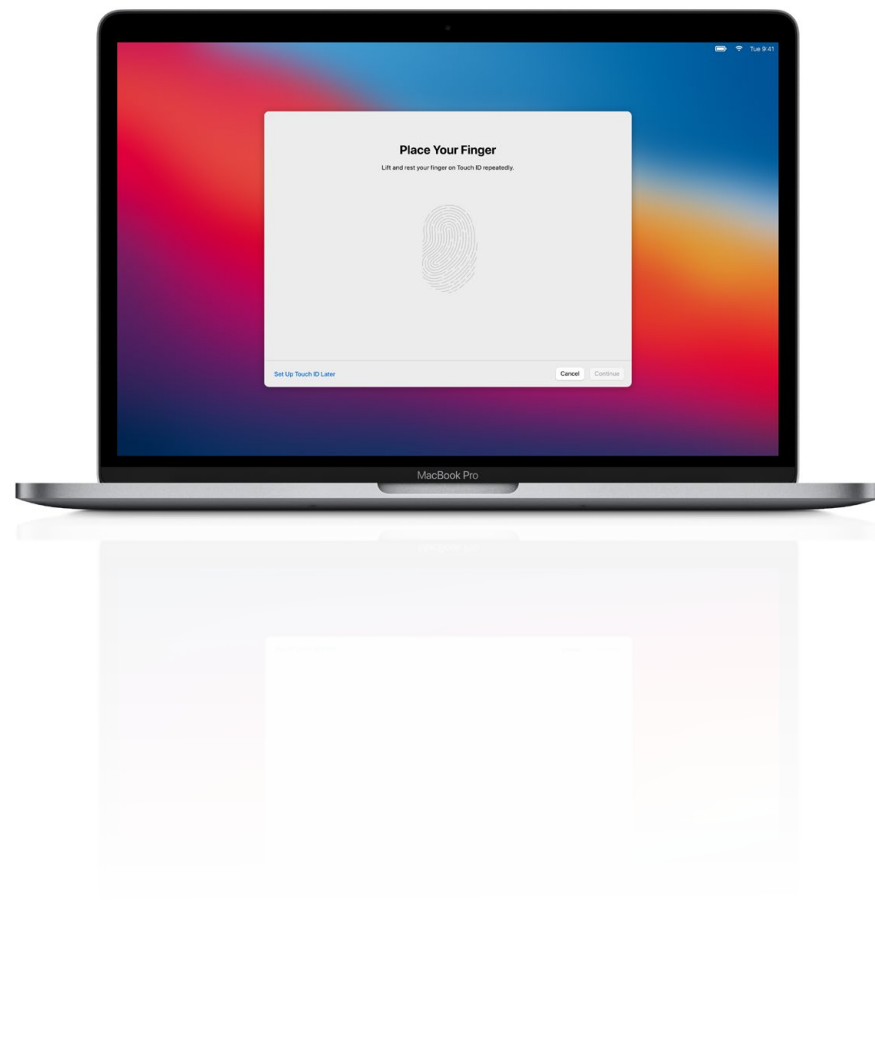
Zero-Trust
and the future of healthcare

Driving digital
transformation
in a next-generation workplace

Get the support
you need to address today's
supply chain challenges

Disaster recovery
and why it matters





Secure by design.

Security is built right in. Apple devices and platforms are designed to keep your personal data and corporate information secure. Mac is the most secure personal computer on the planet.

Key built-in security features, like hardware-verified secure boot, and on-the-fly device encryption, can't be disabled by mistake. Touch ID, Face ID, and Gatekeeper make it easy to secure every device. And because many of these features are enabled by default, employees and IT won't need to perform extensive configurations. Apple has you covered.

To learn more about Apple and Zones Apple services, visit uk.zones.com/apple.

Copyright ©2022 Apple Inc. All rights reserved.

contents



The world is rapidly changing – and your business needs to adapt accordingly. As more and more workers settle into remote and hybrid ways of doing business, IT leaders need to find strategies for managing their employees and giving them the technology tools they need to be successful. This issue of Solutions by Zones will explore how you can make that happen.

6 Securing Your Business in the Modern IT Landscape

The business landscape has changed dramatically in the last two years, especially from an IT perspective.

14 It's Time to Embrace The Future of Healthcare with Zero Trust

As cyberattacks evolve, there are concerns about lack of security standards across healthcare organizations.

20 Driving digital transformation in a next-generation workplace

Employers everywhere are working to find the right balance for the workplace.

28 Get the support you need to address today's supply chain challenges.

Right now, businesses all around the world are up against a wide range of supply chain difficulties.

34 Why does Disaster Recovery matter?

Ensure your business is prepared with a Disaster Recovery Plan.



New to Zones and don't have a dedicated Account Manager?
Contact us at **020 7608 7676**.
Our IT experts are available and ready to work with you.

First Choice for IT.™

Zones is a global services provider of end-to-end IT solutions with an unmatched supply chain. You can expect exceptional service and cost-effective, best-in-class solutions that improve efficiency, optimize workflows, and enhance your return on investment.

SECURING YOUR BUSINESS in the Modern IT Landscape

The business landscape has changed dramatically in the last two years, especially from an IT perspective. Managing IT in the modern era requires overseeing remote users, hybrid users, and a wide range of devices and endpoints. How do you secure it all? That's the topic of this panel discussion. Led by Andrew Reese, Cybersecurity Practice Head at Zones, the panelists go in-depth on the inherent challenges of cybersecurity today.

In this article, you'll find a partial transcript. For the complete transcript and to watch the panel discuss the Top Five Security Priorities for 2022, [visit our Zones TechHub website.](#)

*A cybersecurity panel
discussion from the 2022
Zones CustomerConnect
Virtual Conference*



Andrew Reese

Practice Head, Cybersecurity,
Zones

Andrew: I want to take the panelists through the list of **2022's top five security priorities**, as identified by Info-Tech Research Group in their report, "Security Priorities 2022: Securing the Workforce in the Remote Environment." Let's start with number five.

05 PROTECTING AGAINST AND RESPONDING TO RANSOMWARE

Andrew: Ransomware attacks have transformed in 2021 and show absolutely no signs of slowing down in 2022. There is a new major security breach every week, despite organizations spending over \$150 billion in a year on cybersecurity. (NASDAQ, 2021)

And now ransomware as a service (RaaS) is commonplace, and attackers are doubling down by holding encrypted data ransom and also demanding payment under threat of disclosure for the data that they have exfiltrated.

And they're actually making good on their threats.



Joel Jacobs

Ex-MITRE CIO, CSO,
Advisor & Consultant

[Our Info-Tech Research Group business partner] talks about five recommendations.

One of those is to be prepared for a breach. Because there is no guarantee that an organization will not fall victim to ransomware. So instead of putting all their effort into prevention, perhaps organizations should also put effort into planning and responding to a breach.

What additional steps do you think should be added to prepare for a breach, Joel?

Joel: The first thing is to make sure that you understand the status of your backups and whether you have immutable storage.

We're seeing in our clientele real concerns about making sure that their backups are workable and that they've been tested regularly. Insurance companies are beginning to insist on this.

The other part is making sure to decide how you're going to handle it. That means ensuring that you have an incident response plan that is tuned to ransomware.



Scott Foote

CISO, CPO/DPO,
Cybersecurity Exec & Advisor

Ransomware attacks were up 82% from 2020 to 2021, and as you say, there's no sign of it letting up.

Andrew: Security awareness training and phishing detection is the next recommendation from Info-Tech. You know, phishing continues to be the main point of entry of ransomware. Investing in an awareness and detection program among your end users may be the most impactful countermeasure that you can put in place.

What are some of the techniques you would use to properly configure your "Human Firewall," Scott?

Scott: It's interesting you bring this one up because I usually talk about patching the humans, right – vulnerabilities and the patching of the human – and that's what security awareness training does. And one of the biggest things we need to recognize is that humans are inherently helpful and they're inherently trustful. So, we'll talk about zero trust on the technology side later, but we endeavor to get humans to have zero trust in their interactions.

“

Ransomware attacks were up 82% from 2020 to 2021, and there's no sign of it letting up.

Be polite. Be engaging. But don't immediately trust.

You will be phished socially, whether it's on email, social media or even live via the phone. Train them to be sensitive to the fact that there are people trying to exploit their inherent trust.

Joel also talks about training in terms of snackable bites. We see a lot of vendors as we do assessments for the programs and the clients we work with, and we try to encourage them not to just queue up three hours' worth of security training at the end of the year, but [rather] to make it consumable in much smaller pieces and spread it out across the entire year. [You'll get] much better engagement with the workforce.

Andrew: [Info-Tech also recommends] encrypting and backing up our data – encrypt our data so even if there is a data breach the attackers won't have a copy of your data. And also, keep regular backups of the data and put it in a separate location so that you'll still have the data to work on after a breach occurs.

What are some key points a client should consider when looking at encryption and data backup solutions?

Joel: Make sure you're testing. Make sure you've got geographic distribution traffic separation as well. Making sure that your backups are restorable is the number one key. If you're able to encrypt and put multifactor authentication in front of your backup environment that's a big step forward, as well.

Scott: Yes, part of that testing should be to make sure that you can recover from the data within your objectives – your RTO and your RPO. Your recovery time objective, meaning what's the window; and the recovery point objective, meaning how much data can you afford to lose. It isn't sufficient to say, "I can get the backups back." Make sure you can meet those objectives.

04 ADOPTING ZERO TRUST

Andrew: The top reasons for building a Zero Trust Program:

- Enforce least privilege access to critical resources.
- Reduce attacker ability to move laterally.
- Reduce the enterprise attack surface.

Those are just some of the things. They talk about starting small. Don't put all your eggs in one basket by deploying zero trust in a wide swath. Rather, start as small as possible to allow for growing pains without creating business friction – or sinking your project altogether.

Where do you think is a good place to start small?

Scott: I would say look at network segmentation. We don't have to start with core business systems and dismantle them into microservices and put gateways, right? That's the vision of zero trust longer term. But in the near term, we can do network segmentation of the environment.

Very typically we'll see people that have rolled out IoT devices. It could be conference room equipment, the video screens that are in the break rooms, the HVAC components...but they don't have a separate IoT network. All of that equipment is on the exact same network as the general user traffic.

This idea of network segmentation is fairly straightforward to do, especially in today's world where we're using Wi-Fi rather than a [network] cable.

And understand that you want to isolate traffic based upon the types of information that traffic needs to have access to – always looking at isolating traffic that has the least privilege on its own networks.

Andrew: They also recommend being aware of "too-good-to-be-true" products. Zero trust is a powerful buzzword. A lot of people are using it and vendors know it. You have to be skeptical and do your due diligence to make sure your new security partners in zero trust are delivering what you need.

A holistic approach to cybersecurity is needed now more than ever.

Going back to you, Joel, what kinds of due diligence would you recommend?

Joel: The overpromising isn't unique to zero trust. We've had overpromising vendors for forever . . . and especially in security where they've got the one thing that will complete your defenses and reassure your environment.

Zero trust has become the next big thing, the next shiny object.

But I think making sure that you're starting with real criteria about what you're trying to achieve – define it from the start. And press for reference implementations. Reference accounts that the vendors and consultants have put in place already. See if they have been able to live up to their promises because there's a lot of overpromising.

Andrew: Yes, so basically you need to build a sensible road map of where you are and where you need to get to.

Zero trust principles can be applied in a number of different ways, so you need to find out where you need to start. Between identities, devices, networking, and data, decide on a use case that will be your pilot project and then refine your approach.

03 SECURING DIGITAL TRANSFORMATION

Andrew: Digital transformation is occurring at an ever-increasing rate these days.

As Microsoft CEO Satya Nadella said early in the pandemic, **“We've seen two years' worth of digital transformation in two months.”**

We've heard similar stories from Info-Tech members who deployed rollouts that were scheduled to take months that happen basically over a weekend.

Engaging the business early and often is kind of like a requirement. Despite the risks, organizations engage in digital transformations because they also have huge business value. So, security leaders should not be seeking to slow or stop digital transformations; [instead] they should be engaging the business early and then trying to get ahead of the risk to enable a successful transformation.

What are some good ways to engage stakeholders?

Scott: This is an important place to start with those stakeholders. We talk a lot about starting with the end in mind, meaning be explicit, don't rely on anecdotal drive-by conversations. Write the

concept of operation down in a document so that others can reflect on it as you go through the digital transformation.

A concept of operation is not a technical document. It describes the business:

- How are we going to transform the business?
- What are the assumptions? Let's be explicit and write them down.
- What are the dependencies?

Too often, digital transformation projects fail because we didn't start with what success looks like. We simply made the assumption and moved forward. When things don't materialize, of course, you wind up with almost 75% failure rate in terms of what, today, we call digital transformations. Overpromises usually wind up with under delivery.

“

Security leaders should not be seeking to slow or stop digital transformations; they should be engaging the business early and then trying to get ahead of the risk to enable a successful transformation.

Joel: Scott said, “start with the end in mind and understand what you're trying to achieve.” Combine that with the ideal principle of “start where you are.” Make sure that you understand your current condition and your current arrangements and what you're trying to change.

Almost no organization can start with a clean slate, but they really need to be very declarative about what they're trying to achieve. Then dealing with the security elements from the beginning not after the fact, so that they're not trying to retrofit the choices that you make.

Andrew: Yes, and they talk about when you're doing these things [it's important to] build and revisit your security strategy. You're making major changes and so the threat surface changes constantly as you're doing your transformation. This is the right time to revisit or rebuild your security strategy to ensure that your control set is present throughout the new environment. And it is also a great opportunity to show how your current

security investments are actually helping to secure your new digital lines of business.

How often should you review and consider rebuilding your security strategy?

Joel: In this day and age, I can't imagine looking at your security strategy less than annually and frankly probably more regularly. There's the notion that strategy has a very long-enduring horizon. I don't think that's very practical considering the level of threat and, therefore, the level of business risk that's associated with cybersecurity.

For the complete transcript, including security priorities 1 and 2, and to watch the panel discussion as it happened, visit our [Zones TechHub website](#).

PANELISTS

Andrew Reese, Practice Head, Cybersecurity, Zones

Joel Jacobs, Former MITRE Corp. CIO, CSO, Advisor, Consultant

Scott Foote, CISO, CPO/DPO, Cybersecurity Executive, Advisor

Contact Zones to learn how we can help you or call 020 7608 7676 today.

ZONES
First Choice for IT™

NEW ADVANCED CYBER DEFENSE TECHNOLOGIES

Discover how Zones Security Operations Center as a Service (SOCaaS) can proactively prevent, detect, and respond to security threats for you.

The pandemic turned into a windfall for cybercriminals. Remote and hybrid employees working outside the relative safety of the office network have unintentionally made your organization more vulnerable to cyberattacks.

Ransomware attacks. Phishing attacks. Formjacking attacks. Those are just a few of the cyberattacks that have risen dramatically across the globe. And no organization is immune.

Zones SOCaaS works around the clock using artificial and augmented intelligence, machine learning, and the latest threat feeds to monitor and protect your IT environment against cyberattacks.

[Click here to learn more.](#)

ZONES
First Choice for IT™



Embracing the Future of Healthcare With Zero Trust

By Brad Mateski, Solutions Architect, Cybersecurity

Why all the buzz about Zero Trust?

Zero Trust is a one-of-a-kind approach to security that centers on eliminating trust from an organization's network architecture. In a zero-trust model, trust is consistently verified each time before granting access, even for legitimate internal resources.



A recent executive order mandated that government agencies must achieve specific zero-trust security goals by the end of 2024. This move aims to improve security, and many healthcare organizations (HCOs) may follow suit. The reason is clear: Conventional security methods are inadequate and cyberattacks are more rampant than ever. We regularly see in the news the latest ransomware attacks, the effect on an HCO's operations, and the millions of dollars in ransom an HCO must pay to regain access to critical data held hostage by encryption.



The health scare in healthcare

Healthcare is the most targeted industry for cybercriminals, making up a third of all U.S. data breaches.¹ Phishing scams, misconfiguration of servers, lost laptops, and mistakes due to an organization's lack of proper training are risks that could lead to intrusion into other secure networks.

As cyberattacks evolve, there are concerns about the lack of security standards across healthcare organizations. Patient data breaches are considered a major security risk and carry severe financial penalties, as medical records contain protected health information (PHI) that healthcare organizations must protect under the Health Insurance Portability and Accountability Act. And HCOs can't afford a second of downtime or risk patient safety.

In addition, providers and patients are working and living remotely, making it cumbersome to manage the network and keep it secure while allowing access to third-party applications and data. And the challenges may grow exponentially as cyberterrorism continues to evolve, leading to increasing sophistication and frequency of cyberattacks.

The cybersecurity outlook in healthcare

HCOs are high-value targets for cybercriminals, so there's no such thing as too much caution when authenticating users and safeguarding access to critical data. This is the core principle behind zero trust, where the focus must be on securing the network and verifying trust for all equipment that may connect to a hospital's network, including electronics, IoT devices, and medical devices. For the latter, the U.S. FDA's draft guidance on cybersecurity in medical devices provides insight into how the agency wants to see regulatory requirements applied.²

Key principles for building a zero-trust infrastructure

Zero trust architecture (ZTA) is a set of cybersecurity principles that uses zero-trust concepts and encompasses **component relationships, workflow planning, and access policies.** The architecture is supported and enforced across various pillars (i.e., OMB ZTCSP 2022), tenets (i.e., DOD ZTRA 2021; NIST-800-207), and maturity models (i.e., NSTAC ZT-TIM 2022). A zero-trust enterprise includes both the network infrastructure (physical and virtual) and operational procedures that are put in place as a product of these applied principles.



Source: Info-Tech Research Group

Building a zero-trust infrastructure starts with understanding that it must benefit business, security, and IT, as well as knowing that while not everyone can achieve complete zero trust, everyone can adopt it. Organizations may not realize it, but they can build on their existing infrastructures to establish a ZTA.

Expert help at whatever stage you're at

Whether you're just starting to ramp up your cybersecurity, well on your way, or somewhere in between, the Zones Healthcare team will work

with you to assess, adapt, and continuously monitor your cybersecurity strategies. You can rest assured knowing you're mitigating threats now and in the future for all connected devices, including medical devices and IoT appliances.

From maturing security programs to control optimization, Zones applies industry best practices to consistently assess, design, implement, and manage intelligent, scalable security solutions across the different pillars of ZTA.

To learn more about how we can address your IT challenges, contact HealthcareIT@zones.com and set up a discovery call with one of our experts.

¹Top Cybersecurity Threats For Healthcare Practices In 2021 - Fastech Solutions (myfastech.com)
²Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions | FDA

ZONES
First Choice for IT™



Improving Security With a Zero-Trust Approach

Let's be honest: Your old security strategies aren't working anymore. Not today. Not with so many remote, hybrid, and otherwise mobile employees roaming around. To safeguard a modern workforce, you need a truly modern approach.

What you need is zero trust.

A zero-trust security framework is one that verifies the identity of every single user before allowing them network access. No one is trusted automatically, no matter who they are or where they come from.

Cisco and Zones, together, can help you establish a zero-trust approach to security. We'll help you protect your network, your data, and every single one of your users.

To learn more, [visit our website](#) today.

For more information about Cisco security, visit uk.zones.com/cisco

© 2022 Cisco and/or its affiliates. All rights reserved.





DRIVING DIGITAL TRANSFORMATION IN A **NEXT-GENERATION WORKPLACE**

By Mike Dennis, Vice
President, Partner &
Product Management

As we all collectively start to emerge from a global pandemic, employers everywhere are working to find the right balance for the workplace.

During COVID-19, remote work largely became the norm; as things begin to return to normal, many employees are making their way back to the office. The question now is how to reconcile the two.

How much remote work is the right amount?

THERE'S DEFINITELY RISK INVOLVED
IN ABANDONING REMOTE WORK

POST-COVID

For example, a recent Gartner study found that when organizations force their employees back to a fully on-site work arrangement, they could lose up to 33% of their total workforce. Clearly, people still like having the option to work remotely, at least at certain times – which means some sort of hybrid arrangement is worth considering.

There are always challenges with hybrid work, though. Chief among them: How do you make sure every employee, whether in-office or remote or both, has the technology they need to be successful? What about devices? What about network access? Collaboration tools? Security? And moreover, how do you guarantee that your physical infrastructure is ready for on-site employees? These are the key questions that organizations right now need to answer.

At Zones, we offer a solution that helps organizations address the workplace challenges of today:

NextGen Workplace Services. Our NextGen Workplace Services offering is focused on providing support and addressing issues in end users' work environments. Effectively, Zones serves as the client's first point of contact for all aspects of IT including device support, application management, and more.

One key aspect of this is mobile device management, and it's easy to understand why.

IF THEY FORCE EMPLOYEES BACK TO WORK

organizations could lose up to

33% of their workforce.

Employees today rely on mobile devices for completing countless tasks on a daily basis – and as such, their employers need effective solutions for managing those devices. That's why our NextGen Workplace Services include a multi-faceted approach to Mobile Device Management. We offer remote assistance for mobile users, MDM setup and configuration, device and patch management, compliance management, application management, and more.

But the features don't end there. Also at the heart of our NextGen Workplace Services is a Service Desk that's available to assist end users with any and all IT challenges. This offering includes a number of services – among them are a **24/7 Help Desk, cognitive chatbot, knowledge management services, executive support, and remote support.** Additionally, innovative new technologies like Artificial Intelligence and Digital Experience Management are there to make our solution truly "NextGen."

This is a core component of what we do at Zones. We make it a priority to drive digital transformation efforts for clients around the globe – and we know that right now,

as organizations navigate the challenges of hybrid work, enabling a truly digital workplace is crucial.

If you work with Zones to digitize your environment, there are numerous benefits waiting for you – including reduced downtime, a superior user experience, and end-to-end support for your whole business.

**To learn more about
this unique opportunity,
connect with a Zones
Account Manager today.**

**[Visit our website
to learn more.](#)**

IT'S TIME TO
**RETHINK THE TRADITIONAL
IN-HOUSE HELP DESK**



It's time for Zones NextGen Workplace Services – because a work anywhere, anytime digital age demands a more accessible and cost-effective approach to end-user support.

**The modern way to outsource
IT support for end users**

With NextGen Workplace Services, you'll have one comprehensive solution that benefits your people and your bottom line.

- 24x7 Service Desk Operations
- 8x5 Mobile Device Management
- Digital Experience Management

Get end-to-end support, reduce downtime by up to 90%, optimize support costs, and more. It's time.

[Click here to learn more about Zones NextGen Workplace Services.](#)

[UK.ZONES.COM](#) | 020 7608 7676



Welcome to the new era of work

The days of the traditional workplace are over.

Today's employees are everywhere – they're in the office, they're at home, and they're everywhere in between. We've entered the era of the hybrid workforce, and that means you need hybrid IT that's built to empower them.

HP and Zones can deliver just that. We create solutions that are designed for a truly hybrid workforce. With our help, you can ensure your users will be fully connected, highly productive, and always secure. Your people can work from anywhere with HP and Zones.

For more information about HP Hybrid Work, visit uk.zones.com/hp


©2022 HP Development Company, L.P.



GET THE SUPPORT YOU NEED TO ADDRESS TODAY'S SUPPLY CHAIN CHALLENGES

By Ed Moninger, Vice President, Supply Chain

There's no sugarcoating it: Right now, businesses all around the world are up against a wide range of supply chain difficulties. Global unrest, especially between Russia and Ukraine, has strained international relations, leading to price increases and other disruptions worldwide. Meanwhile, an economic slowdown is taking hold all around the world, driving up costs for suppliers. And all the while, a global pandemic continues. For all of these reasons, it's harder than usual right now for organizations to procure the supplies they need.



With Zones GSCaaS, you can **go where you want to grow.**

At Zones, we look to help clients address all of these difficulties and more.

That's the thinking behind our Global Supply Chain as a Service solution, which is purpose built for confronting the supply chain challenges of today.

Our inventory solutions enable us to stock items predictively using Zones-led forecasting and scheduling, prescriptive EOL verification and management, and clarity around inventory ownership.

We have tools and processes established that allow clients to outsource as much of the supply chain as they desire – your infrastructure can be Zones-owned, client-owned, or both.

When you invest in Zones Global Supply Chain as a Service, you gain access to a wide range of services designed to simplify your supply chain challenges.

These services include:

- Financial Services
- Import and Export Management
- Transportation Management
- Warehousing and Distribution
- Project Management
- Inventory Management
- Order Management
- Pre- and Post-Sales Support

All told, these services should bring a host of benefits for your business. For starters, outsourcing IT supply management is a great way to reduce the burden on your IT team, freeing your people up to focus on more strategic business initiatives.

Additionally, it will help with gaining greater inventory visibility, simplifying project management, extending the global reach of your business, and making for easier execution of complex requirements. All of these effects should leave a tangible imprint on your business' bottom line.

So is Zones GSCaaS the right fit for you? Let's run through it.

If you're currently dealing with overly time-consuming supply chain processes and outsourcing them would make your life easier, then signs point to yes. If you're struggling with a lack of supplies needed to run the business in an efficient manner, that's a yes as well. If you've undertaken major projects that are a strain on supply chain resources, or you're facing difficult geographic hurdles keeping the business from expanding or holding onto existing territory, then we can address that

as well. At Zones, we have the right tools in place to combat all of these difficulties.

At Zones, we understand that every business is different and comes with its own unique needs – especially where supply chain is concerned, and especially at times like these. But for us, that's not a problem. We are ready to roll up our sleeves and develop a custom GSCaaS solution that meets the needs of any organization.

We have an award-winning end-to-end solution that can support your supply chain team, and we have IT experts in our corner with over 30 years of global supply chain experience. We are ready to get to work, tackling any and all supply chain difficulties in front of you.

Reach out to a Zones Account Manager today or [visit our website](#) to learn more.



What is Azure Databricks?

Azure Databricks is a data analytics platform optimized for the Microsoft Azure cloud services platform. Azure Databricks offers three environments for developing data-intensive applications: Databricks SQL, Databricks Data Science & Engineering, and Databricks Machine Learning.

Databricks SQL provides an easy-to-use platform for analysts who want to run SQL queries on their data lake and create multiple visualization types to explore query results from different perspectives while building and sharing dashboards.

Databricks Data Science & Engineering provides an interactive workspace that enables collaboration between data engineers, data scientists, and machine learning engineers. For a Big Data pipeline, the data (raw or structured) is ingested into Azure through Azure Data Factory in batches or streamed near real-time using Apache Kafka, Event Hub, or IoT Hub. This data lands in a data lake for long-term persisted storage, in Azure Blob Storage or Azure Data Lake Storage. As part of your analytics workflow, use Azure Databricks to read data from multiple data sources and turn it into breakthrough insights using Spark.

Databricks Machine Learning is an integrated end-to-end machine learning environment incorporating managed services for experiment tracking, model training, feature development and management, and feature and model serving.

Azure Databricks Service can unlock insights from all your data and build artificial intelligence (AI) solutions with Azure Databricks, set up your Apache Spark environment in minutes, auto scale, and collaborate on shared projects in an interactive workspace.

Contact your Zones Account Manager to set up a discovery meeting with one of our Solution Architects to learn how our Zones Data Management Services can help your organization.

For more information about Azure Databricks, visit zones/microsoft-azure-data-management

© 2022 Microsoft



Disaster Recovery Planning Matters **More Than Ever**

By Tony Rylands, Director, Cloud Strategy

In the past year, many businesses around the country have been left to pick up the pieces in the aftermath of natural disasters. To cite just one example, Tropical Storm Alex wreaked havoc in South Florida in June. And the threat of natural disasters isn't likely to go away, either – major storms are only expected to increase with this coming hurricane season.

At times like these, it's crucial to ensure your business is prepared by drawing up a plan for disaster recovery (DR). Don't wait until a storm hits your city to start planning your recovery – get out ahead of the problem with a proactive solution, such as Zones' offering for Disaster Recovery as a Service (DRaaS).



Why does disaster recovery matter?

For many businesses today, the prospect of a disaster represents a true doomsday scenario. **According to data from Forbes and Cisco, a critical server outage for the typical enterprise results in financial losses of approximately \$400,000 every hour.** Most companies are simply not equipped to absorb this sort of damage – which is why about 60% of companies that lose their data shut down within 6 months, according to a survey conducted by FEMA (Federal Emergency Management Agency).

It's clear that the consequences of data loss are drastic – and that planning for possible disasters is crucial. But here's another disturbing statistic that FEMA found: **1 in 5 companies today do not have a plan for disaster recovery. This needs to change.**

Introducing Zones' solution for disaster recovery

Whether you're looking for a new disaster recovery solution or want to bolster an existing one, Zones can play a role. We're here to help you assess your environment, then design, implement, and manage a DR solution that will work across on-premises, cloud, and hybrid IT environments.

Whether you need to remedy an existing disaster recovery dilemma or consult an expert to create an entirely new DR solution, Zones has the expertise to help – and a client-first attitude to providing exceptional service.

With Zones DRaaS...

- › Choose the DR strategy that's a perfect fit for your business.
- › Protect your valuable data with minimal investment, and without purchasing any new on-premises equipment.
- › Save money by gaining greater flexibility and predictability with your data storage costs.
- › Reap the benefits of an extensive global network of DR sites.
- › Leverage our DRaaS solution as a guiding force to the cloud.
- › Restore your lost data from anywhere, with minimal effort and cost.
- › Minimize service disruption, ensure application mobility, and create a more flexible infrastructure.
- › Develop the IT resilience needed to withstand any disaster and confidently embrace change as your business evolves.

“1 in 5 companies today do not have a plan for disaster recovery.”

The many tiers of disaster recovery. Zones' solution for DR works on many levels. Here's a rundown of the many tiers to our DRaaS solution...

TIER 0:

No off-site data. Recovery is only possible with on-site systems.

TIER 1:

Physical backup with a cold site. The organization transports data stored on magnetic tape or another medium to an off-site facility, with no IT equipment installed. External companies provide secure above- and below-ground storage facilities for backup tapes.

TIER 2:

Physical backup with a hot site. Data is transported to a hot site, an offsite facility with the hardware to take over from the primary data center.

TIER 3:

Electronic vaulting. Data is electronically transmitted to a hot site. As network bandwidth and overall transmission speeds increased during the 1980s and 1990s, organizations could receive electronic data backups on their on-site storage devices.

TIER 4:

Point-in-time recovery. Point-in-time copies of storage volumes, files, or dates are created at a specific moment, such as the end of each day.

TIER 5:

Two-site commit/transaction integrity. Data is transmitted to this tier's primary and alternate backup sites. Organizations need substantial network bandwidth to maintain a constant data flow.

TIER 6:

Minimal to zero data loss. Recovery in this approach is instantaneous, often thanks to disk mirroring or data replication. These technologies back up files and databases as they are created.

TIER 7:

Recovery automation. Recovery automation is the newest tier of disaster recovery. In this tier, technology constantly monitors multiple aspects of data operations, looking for any situation that threatens those operations.

To bolster your organization's DR plans at any or all of these tiers, Zones is ready to help.

We can safeguard your organization's mission-critical systems and ensure uninterrupted availability under even the most adverse circumstances.

Disaster recovery is not a one-time thing – it's an ongoing process that requires proactive planning as the threat landscape continues to evolve. But by working with Zones, you can leave that work to the experts, freeing your employees to focus on doing the work they do best every day.

Zones equips organizations of all sizes to solve their IT challenges – and we're eager to work that magic for you next. **Reach out the Zones team today to [learn more](#).**

Contact a Zones Account Manager
or call 020 7608 7676 today.

ZONES
First Choice for IT™

Simplify your edge.

For businesses today, the challenge is to draw real-time insights from massive amounts of data, spread out across literally countless devices. And with the bulk of data you're dealing with, it's not cost-effective to be constantly moving it back and forth to a centralized cloud infrastructure.

Instead, it's time to live at the edge.

When you work with Dell Technologies and Zones, we can get you started with edge computing. An edge-based data architecture enables real-time insights and allows you to respond quickly and effectively to your IT needs, all in real time.

We'll help you set up a consistent, high-performing infrastructure that spans private clouds, public clouds, and the edge as well. As a result, you can unlock the value of your data and power all your applications, in all your environments.

Seize your opportunity. Simplify the edge with Dell Technologies.

DELLTechnologies
PLATINUM PARTNER

ZONES
First Choice for IT™

For more information about Dell Technologies, visit uk.zones.com/dell

©2022 Dell Inc.





The New Microsoft Surface Pro 9

Laptop power, tablet flexibility

Work, stream and play—Surface Pro 9 has the flexibility of a tablet with the performance of a laptop—all in one.

For more information on the new Microsoft Surface Pro 9 visit uk.zones.com/microsoft



TAKING ON THE CHALLENGE OF VULNERABILITY MANAGEMENT

These are uncertain times, and countless cybersecurity threats are out there lurking. In this landscape, you can never be too thorough – you need to have comprehensive knowledge of where your IT is vulnerable, what you need to do to protect it, and how quickly you can implement changes.

Zones can help with all of that – we offer comprehensive services for Vulnerability Assessment and Penetration Testing. With our help, you can size up your environment and figure out where your organization is most vulnerable, including both external threats and internal ones. From there, you can map out a clear roadmap to better secure your business.

Risk assessments are the cornerstone of every cybersecurity program. Zones is here to assist with yours.

To learn more, connect with a Zones Account Manager today.

[Visit our Vulnerability Assessment & Penetration Testing \(VAPT\) page to learn more.](#)

ZONES.COM | 800.408.ZONES



©2022 Zones, LLC. All rights reserved. Unauthorized duplication is a violation of federal laws. Zones, Zones Infrastructure, Zones.com, Infrastructure.com, Enterprise, The Mac Zone, Multiple Zones, and Zones Government & Education are registered trademarks of Zones, LLC. All partner product names throughout this publication are trademarks of their respective holders.

This publication may contain copyrighted material the use of which has not been specifically authorized by the copyright owner. Zones, LLC, believes that this constitutes a "fair use" of the copyrighted material as provided for in section 107 of the U.S. Copyright Law.