adaptiva™

WHITE PAPER

Endpoint Management Powered by Your Edge

INTRODUCTION

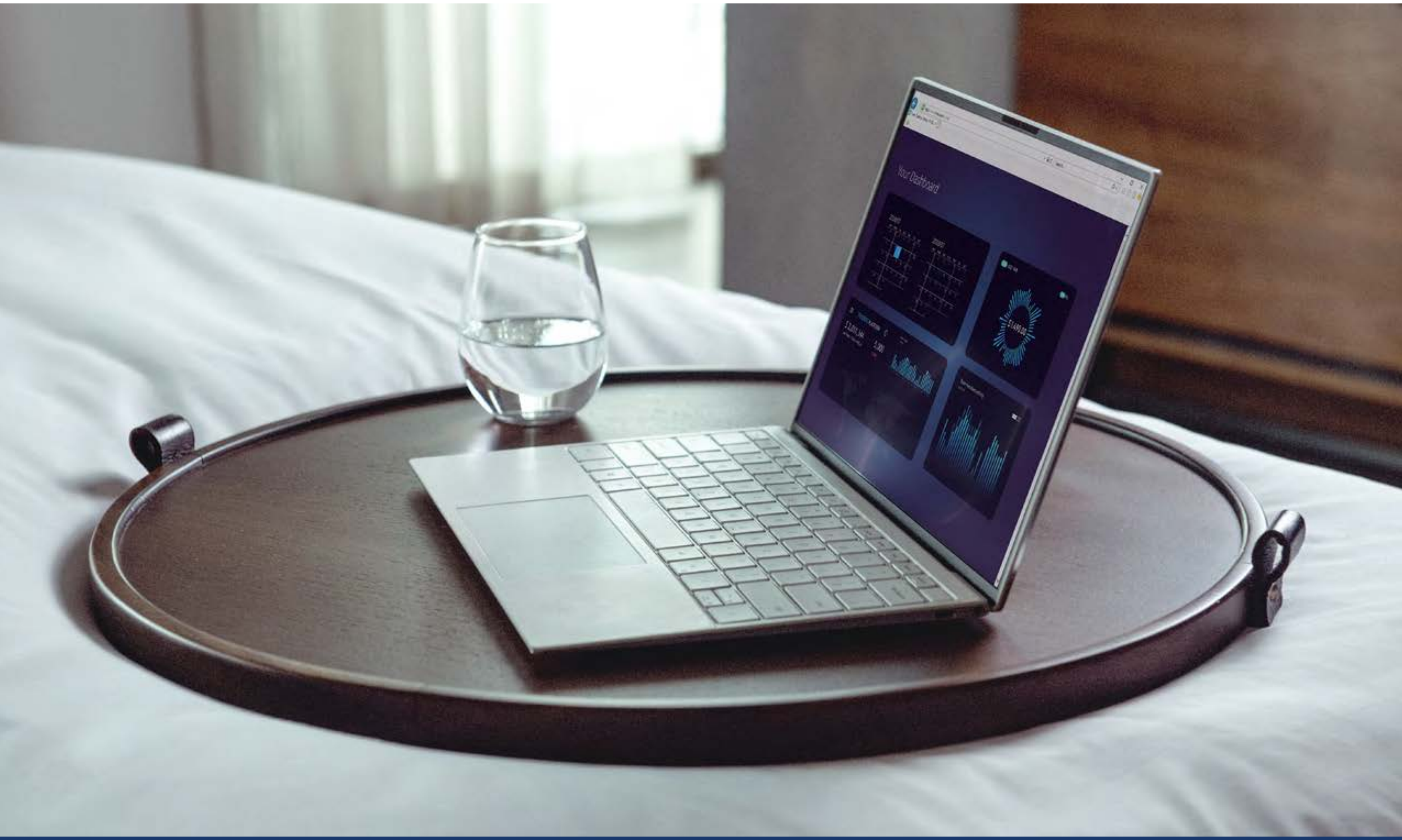
The future of endpoint management is here, and it’s serverless.

IT professionals face more challenges than ever before, especially when it comes to endpoint management.

As organizations move to digitally transform their business models, **IT faces the complex job of implementing, maintaining, and scaling efficient and secure content delivery systems,** all while providing technical support to an increasingly mobile workforce.

Until recently, the only option for content delivery has been a solution that requires centralized, physical servers that offer little flexibility, have high costs to maintain and scale, and are susceptible to security breaches. The server-based model was moderately effective, but only for employees using a limited selection of devices on specific, controlled networks — but times have changed.

As organizations plan for the future of work, endpoint security is a top concern. Transitioning to remote and hybrid work structures has opened the door for increased security breaches, with ransomware attacks on the rise.[1] Investments in global endpoint management solutions that amplify data security measures are essential for organizations to ensure that internal information stays safe and day-to-day operations can run smoothly.



Time is of the essence.
If companies don't take steps to implement sufficient risk prevention or vulnerability monitoring, the impacts on businesses might be staggering. The 2022 Cybersecurity Insiders Report reveals that:

20%

OF CYBERSECURITY PROFESSIONALS

report that their organization experienced a "successful" endpoint attack in the last 12 months, which compromised data asset and IT infrastructure.

Additionally, the cost of an endpoint attack has increased

FROM $7.1 MILLION TO

8.94 million dollars.[2]

85%

OF ALL ORGANIZATIONS SURVEYED

expect a compromising attack within the next 12 months.

46%

OF EXISTING ENDPOINT SECURITY PRODUCTS

fail to stop an increasing number of threats.

66%

OF ORGANIZATIONS

experienced increased threats to their endpoints in the past 12 months.

Adaptiva is the only company that offers a full-service, scalable P2P solution for endpoint management.

In addition to cybersecurity, **IT departments must maintain endpoint health while monitoring an increasingly mobile workforce**. Organizations can no longer count on having everyone at a designated location to control variables. At the same time, IT managers need a solution that fits within budgeting constraints.

With many enterprise organizations embracing flexibility across their businesses, now is the time for IT to lead digital transformation efforts with endpoint management configurations that are fast, accurate, automated, scalable — and cost-effective. By eliminating unnecessary, fragile content distribution infrastructure and maximizing edge networks with a peer-to-peer endpoint management solution, **IT can effortlessly scale and improve compliance and endpoint health.**

The future of endpoint management is here, and it's serverless. Adaptiva is the only company that offers a full-service, scalable P2P solution for endpoint management.

What is P2P? The ideal method for widespread content distribution.

Peer-to-peer (P2P) technology is not new, in fact, it has been readily available since the 1990s. A P2P network is created when two or more PCs are connected and share resources without going through a separate server. Doing so requires a client platform that starts this process as the file you're trying to download is hosted on another computer. Because there is no centralized server to maintain there is no significant cost to building or maintaining a P2P network.

Today, the edge is a cobbled-together mess for most enterprises, driven by three factors that could be completely resolved with the use of a P2P endpoint management model:

- Device proliferation
- An expanding threat landscape
- Rapid decentralization of the workforce

With a client-server model the more clients you add the more servers you need (which limits scalability and creates a vicious cycle of distribution point sprawl, which costs significant dollars and resources to maintain). One server will not have enough compute power to manage the increasing number of devices added to its network; and **with a rapidly decentralized workforce and increasingly sophisticated threats this model is nearly impossible to maintain.**

For Your P2P Playlist:

Podcasts

The Endpoint Management Podcast
by adaptiva

You Need to Start Using P2P with UDP Transfer Protocol for Endpoint Management

Take a look under the hood at the transfer protocols used for endpoint content delivery.

The Endpoint Management Podcast
by adaptiva

How Enterprise Orgs Save BIG with P2P Endpoint Management Architecture

Learn how P2P architecture leads to cost savings and *better* performance.

The Endpoint Management Podcast
by adaptiva

Serverless P2P Architecture has Revolutionized Endpoint Management

P2P is all the things: it's simpler, easier, cheaper, more performant, and more efficient.

A P2P file-sharing method is a successful model for content distribution.

When it comes to endpoint management the most critical first step to securing your network is have **complete observability over all your endpoints;** a feat that most organizations cannot achieve with a client-server model. According to data collected in our 2022 Ponemon Institute research (coming in June 2022) the average enterprise manages 135,000 devices at the edge. And despite $4,252,500 of IT budget ($31.50/endpoint) spent on endpoint protection - on average, 48% of those devices are at risk because they aren't detected by IT or the OS is outdated. This means that nearly 50% of the enterprise is unprotectable in the current state, and only 34% of organizations have enough resources to minimize endpoint risk.

IT departments have historically followed a different content distribution model when it comes to the devices they support. Instead of treating each machine on the network as a point to host and transfer data, endpoint management has utilized servers, with each device having a direct connection to its parent server. This means there are limited "libraries," and they are:

- Confined to a number of physical locations.
- Prone to the inconveniences of being tethered to said physical location.
- Hard to upgrade or update if the organization wants to grow.

A client-server model relies on a server to deliver information to each individual digital device and requires information to be accessed and stored in a particular way. So, the equation becomes simple: The more devices (laptops, desktops, mobile phones, ATMs, and point of sale (POS) machines) you add to your company's network, the more servers you need. In fact, according to recent research conducted with The Ponemon Research Institute, companies, on average, have one distribution point for every 5.8 endpoints. This is an unnecessary investment some of the world's largest organizations are making just to maintain the health of their network. **Turns out, with the right technology, you actually have surplus capacity at the edge of your network to manage and secure your endpoints. No need for more servers.**

Today's serverless P2P architecture can leverage the power of the cloud for a dynamic, flexible network that can adjust to capacity, freeing endpoint management from all of the constraints of a location-based setup.

Get more insights about the benefits of P2P with our free eBook: The ABCs of P2P.

Serverless P2P is dynamic, just like the networks it runs on.

Networks aren't static, but legacy systems operate as if they are.
A P2P endpoint architecture is adaptable and forgoes constant hands-on configuration enabling it to keep up with network and bandwidth changes on its own.

While legacy systems are limited to location or capacity and rely on many tasks that are initiated by humans, P2P is better because it enables an endpoint management solution that can offer:

→ **Dynamic bandwidth usage.**
Content delivery can ebb and flow, adjusting to traffic.

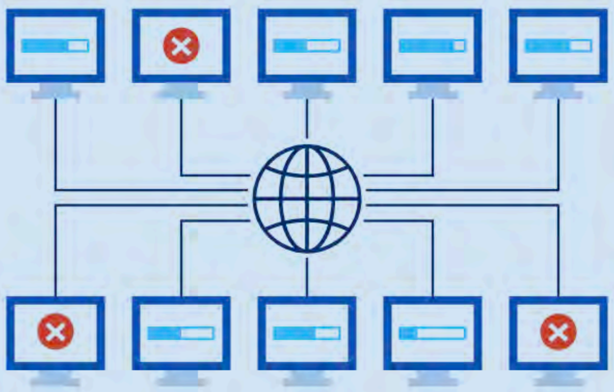
→ **Flexible configurations.**
As conditions change, a single global boundary setting can dynamically create and reconfigure content distribution channels.

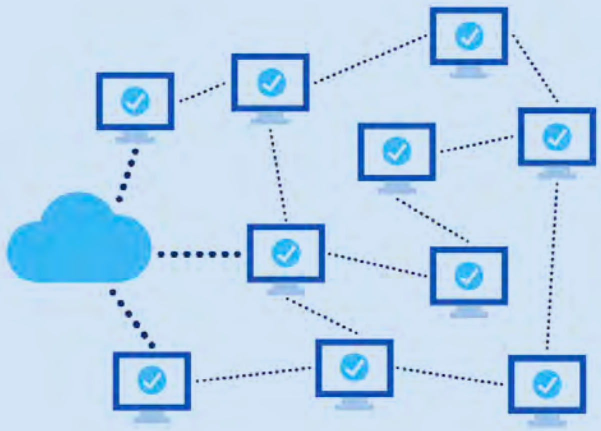
→ **Workload capacity sensing.**
Automatic hard drive space detection across devices to leverage space and complete updates across the entire network efficiently.

→ **Infinite scalability.**
A growing network can easily adopt as many endpoints as needed, requiring zero hardware to scale.

EXAMPLE:

If 10 computers have 100 gigs of free space each, that means there is 1 TB of available capacity to use for storing updates and content sent out over WAN. In this model, all machines update almost simultaneously via P2P transfer, and devices with more capacity can absorb the burden to receive the initial content transfer.





THE COST OF TIME

When organizations with antiquated systems want to roll out a patch, the timeline to apply, test, and deploy can creep out over days, weeks, or even months. Waiting for this can cause delays in productivity and exacerbate weakness in security, resulting in costly repercussions for organizations.

Instead of depending on location-based server infrastructure, **P2P enables the creation of virtual groups where devices connect to their peers automatically** based on their auto-detected location. If one machine goes down, a new leader is automatically identified and creates a new group of healthy devices that stay up-to-date with zero downtime. When a device comes back online, it automatically joins up with its peers and begins receiving content whenever it last left off.

Today's enterprise organizations with global and mobile employees require cloud and endpoint environments that always work with little to no human intervention. IT teams need endpoints managed without fear of stacking up charges for content distribution, overloading the corporate VPN with large content downloads, or distribution failure over unreliable network connections.

With serverless P2P architecture, **IT gains the capability to continuously deliver software, configurations, and patches to endpoints in real-time across a distributed network,** without the manual work of constantly adjusting around network changes, capacity, and server maintenance windows.

P2P networks are more resilient, and better at keeping a mobile workforce compliant.

Protecting internal data from ransomware, hackers, and phishing attempts is a top priority for enterprise organizations. 71% of IT professionals are concerned that remote workers are putting their organization at risk of a data breach, and 85% expect a compromising attack in the next 12 months.

TIME IS MONEY.

Only 21%

of organizations surveyed said they typically **deploy critical security patches in less than one day.**[1]

71%

OF IT PROFESSIONALS

are concerned that **remote workers** are putting their organization at risk of a data breach.[3]

85%

OF IT PROFESSIONALS

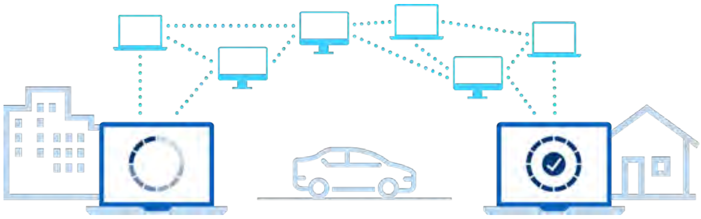
expect a **compromising attack** in the next 12 months.[1]

Maintaining device compliance with security patches is crucial to the safety of an enterprise network. To keep remote devices compliant, your endpoint management solution has to work over varying connectivity conditions experienced by a workforce on the move.

Most legacy endpoint management systems use TCP and BITS, requiring sessions that are prone to packet transfer failure, especially over spotty networks. **This can leave organizations vulnerable.** P2P leverages sessionless UDP and, if interrupted, can pick up where it left off, ensuring content is delivered even over poor networks or after lengthy disruptions to connectivity.

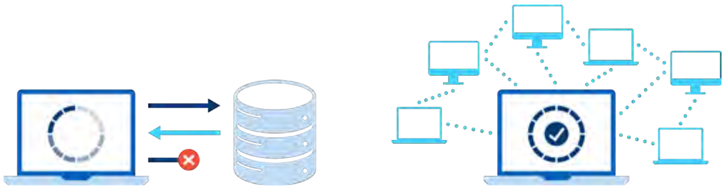
EXAMPLE:

Morgan is at the office and starts an update late afternoon. At 5:00 p.m., she closes her laptop and packs up to go, intending to work from home the next day. Later that evening, she opens her computer to check her email at home. The update she started can resume exactly where it left off, whether or not she is connected to VPN, internet, or an on-prem network.



EXAMPLE:

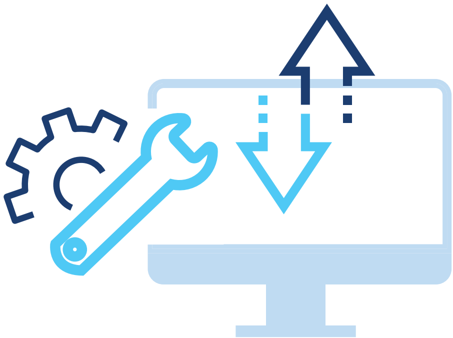
Craig is traveling for business in a country with poor infrastructure, and an update is pushed out over a product that uses TCP/IP with a 2–3 second latency between packets. But, the TCP sessions keep dropping, and it takes forever to push updates out. Meanwhile, Craig's devices are not secure, and the constant update transfer failures make his device run slowly so he is less productive. The next time Craig travels, the company has already made the switch to a P2P solution that uses UDP. UDP enables latency between packets with no dropped sessions. Because it is a sessionless transfer, it can pick up and send the next packet right where it left off. Craig's devices stay up to date as he moves about the world, even over spotty networks.



With a P2P endpoint management solution, each machine becomes a source of content for other devices the minute it starts receiving information.

Once one machine gets a block of data, it can host others, which means quicker data transfer, more coverage, better resilience, and higher compliance rates to keep the data safe.

Without adequate monitoring and security protocols in place, organizations risk a successful endpoint attack.



The bottom line: Serverless P2P frees up IT resources to focus on cybersecurity.

Today's IT departments are often stretched thin and can get bogged down resolving technical difficulties for the workforce. Keeping up with help tickets can get in the way of monitoring and resolving incoming cybersecurity threats, resulting in costly and catastrophic endpoint attacks.

The Cybersecurity Insiders' 2022 Endpoint Security Report uncovered that though 51% of surveyed companies have dedicated teams responsible for responding in real-time to security incidents, they do not perform steady-state monitoring. **Only around a fifth of surveyed organizations can perform ad-hoc monitoring with IT professionals** as the need arises when responding to incoming cybersecurity threats.

So what happens with insufficient cybersecurity monitoring? Without adequate monitoring and security protocols in place, organizations risk a successful endpoint attack. Last-gen endpoint management systems rely on expensive server infrastructure, which is challenging to monitor, maintain, troubleshoot, and repair. Additionally, If an enterprise organization can't keep its most valuable assets (its employees) online, the cost associated with loss of productivity can ripple significantly.

The most expensive consequence of a successful endpoint attack is IT and end-user productivity loss.

AUTOMATION IS THE FUTURE OF CYBERSECURITY

According to LearnBonds, 68% OF MAJOR GLOBAL COMPANIES plan to increase spending on automated cybersecurity solutions.[4]

Further studies[5] suggest enlisting AI for cybersecurity can decrease the detection and response time to phishing attacks by AS MUCH AS 70%

In today's fast-paced, mobile world, **IT resources need freedom from administrative tasks** allowing more time to focus on pushing quality content to all devices quickly and keeping the network safe.

P2P serverless endpoint architecture allows for real, hands-off automation and workflows so configurations, infrastructure maintenance, and boundary management aren't dependent on human interaction, freeing IT departments to tackle more significant matters. **A P2P solution allows the construction of workflows for just about anything imaginable.**

- → CONFIGMGR CLIENT CONFIGURATION CHECKS
- → CONFIGMGR CLIENT HEALTH CHECKS
- → CONFIGMGR CLIENT STATUS CHECKS
- → WMI HEALTH CHECKS
- → SECURITY HEALTH CHECKS
- → SYSTEM PERFORMANCE HEALTH CHECKS
- → WINDOWS UPDATE AGENT HEALTH (WUA) CHECKS (IF WINDOWS UPDATE IS BEING USED)

Automation enables the network topology to define P2P content distribution rules.

For example, if a device is unable to retrieve content from a designated node, it will automatically choose a new parent machine based on the rules established for the network. This flexibility enables API integrations that allow the addition of workflows to existing support dashboards or solutions, **allowing organizations to integrate new functionality into existing maintenance systems.**

Last-gen endpoint management systems are difficult to automate — they are not workflow-friendly and require human intervention for simple yet tedious functions. Simply put, they clog up your IT staff with tasks that could and should be done by technology. **A serverless P2P network can be configured to automatically complete tasks** by leveraging automation, allowing enterprise organizations to build resilient, human-error-proof infrastructure that continuously scans for issues and can scale in seconds.

What was the most significant impact of endpoint attacks against your organization?

47%
LOSS OF END-USER PRODUCTIVITY

40%
SYSTEM DOWNTIME

39%
LOSS OF IT PRODUCTIVITY

36%
REPUTATION AND BRAND DAMAGE

32%
THEFT OF INFORMATION ASSETS

Spotlight on Adaptiva's OneSite Health

WHEN YOUR DEVICES ARE OUT OF COMPLIANCE, YOUR NETWORK IS AT RISK.

A "successful" endpoint attack occurs when an organization's endpoints become compromised, generally via phishing, ransomware, or another form of a data breach. More than 50% of IT professionals (Ponemon Institute, 2020) consider endpoint attacks to be successful because their endpoint security solutions aren't effective enough at detecting threats.

Adaptiva's OneSite Health is a comprehensive monitoring and remediation tool that can help bring devices back into compliance and keep them that way, drastically reducing help desk tickets.

How does it work? OneSite Health first scans to identify problems, such as misconfigurations and software versions or threats like Log4J. After identifying the issue you can use over 100 pre-configured auto-remediations or create a no-code auto-remediation helping get all your devices in compliance without disrupting end-user productivity.

You can learn more about how Adaptiva's OneSite Health saved our customers time and resources during the Log4J vulnerability in our recent webinar, How Breaches Like Log4J Are Making IT Teams Rethink Their Lines of Defense.

OneSite Health allows organizations access to big picture data to identify which machines are performing well. It also enables IT to determine factors like: Are you making an impact on compliance rates? How many hours were saved by running health checks? Are there any recurring remediations that indicate a bigger problem?

With OneSite Health, machines that have been dark for years can be brought back online, compliance rates increase rapidly, and devices stay healthy. It also levels up support desk capabilities with repeatable checks, workflows, and outcomes.

Conclusion

For organizations ready to embrace digital transformation across their business, it's clear: when it comes to content delivery, endpoint management can and should happen at your network's edge.

The traditional work model has evolved, and **it's pivotal that IT is lockstep with the future of work and the growing threat landscape.** With enterprise organizations embracing flexibility yet still requiring speed, security, and efficient content delivery from their endpoint management solution, it's time to say goodbye to the costly and limited capabilities of an on-prem setup.

Serverless P2P architecture frees enterprise organizations from outdated systems that rely on costly infrastructure, human intervention, and slow transfer protocols. **Adaptiva is the only company that offers a full-service, automated P2P endpoint management system** that can scale with your organization to eliminate administrative work and infrastructure costs.

Visit **adaptiva.com** to learn more.

CITATIONS

1. **Cybersecurity Insiders** (April 2022). Cybersecurity Insiders 2022 Endpoint Security Report. Adaptiva. https://adaptiva.com/resources/report/endpoint-security-report

2. **Ponemon Institute** (January 2020) The Third Annual Study on the State of Endpoint Security Risk. The Ponemon Institute LLC. https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf.

3. **Ponemon Institute** (October 2020) Cybersecurity in the Remote Era: A Global Risk Report. Ponemon Institute LLC. https://www.keepersecurity.com/en_GB/ponemon2020.html

4. **Ilic, J** (October 9, 2020) Almost 70% of Major Organizations to Increase Cybersecurity Spending Following Corona Virus Outbreak. LearnBonds. https://learnbonds.com/news/almost-70-of-major-organisations-to-increase-cybersecurity-spending-following-coronavirus-outbreak/

5. **EY Global** (July 22, 2021) How Do You Rise Above the Waves of a Perfect Storm? Ernst & Young Global Limited. https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

ABOUT ADAPTIVA

Adaptiva provides **unrivaled serverless endpoint management** that eliminates the need for a vast IT infrastructure and monitors itself by automating traditionally manual tasks. Leveraging innovative peer-to-peer protocols, the Adaptiva OneSite Platform is powered by the surplus capacity of existing devices already on the network – in the office or working from home. This enables IT to continuously deliver software, configurations and patches to endpoints no matter where they are.

The world's largest enterprise organizations and government agencies rely on Adaptiva for best-in-class, real-time endpoint visibility and content delivery, as well as automated compliance checks, remediations, and patching without ever throttling the network or the end user experience.

Learn how at **adaptiva.com.**