FORTRA

# When Downtime Takes A Bite Out Of Your Budget

# When It Comes To Downtime, You Need To Ask Yourself, "Can I Afford To Lose Access To My Mission-Critical Resources And Processes—Even If Only For A Few Minutes?"

In this eBook, we'll take a look at some of the causes of downtime, where you will find the biggest risks of downtime, and how you can minimize downtime as well as the potential cost of an incident.

Downtime can easily take a huge bite out of your budget without the right data management strategy and solutions in place.

## Downtime has a negative effect on the following:

Compliance with legal and regulatory requirements

Service-level agreements (SLAs)

Staff productivity and IT support resources

Business operations and opportunities

Brand reputation

Consumer confidence

# The Three Biggest Risks Of Downtime

## 1 Downtime Affects The Bottom Line

**One minute of downtime can cost an organization $8,851, on average.** (Emerson Network Power, 2016 Cost of Data Center Outages)

In 2016, Delta Airlines experienced a nationwide system outage that created massive delays for travelers. The system outage cost Delta an estimated $150 million USD. When core systems fail, business operations can come to a halt until resources are up and running again. Even if downtime lasts only a few minutes, it can have wide-reaching ramifications for your business. The Cost of Downtime:

- **$1.25 billion to $2.5 billion per year** for unplanned application downtime
- **$100,000 per hour** for infrastructure failure
- **$500,000 to $1 million per hour** for critical application failure

## 2 Downtime Can Lead To Data Loss

**75 percent of surveyed organizations reported data loss as a result of unexpected downtime.** (Globalscape, Report: Dangerous File Sharing Practices Put Sensitive Data at Risk)

When critical systems unexpectedly go down, the risk of losing important information and communication increases. Depending on the type and amount of data lost, the effects can be crippling, affecting everything from sales and customer service to compliance, security, and productivity. In the EMC® Global Data Protection Index, enterprises reported a loss of $1.7 trillion dollars in the past year, as a result of downtime and data loss. Unplanned downtime and data loss will ultimately affect an organization's bottom line.

## 3 Downtime Affects Security And Compliance

**50 percent of the organizations surveyed reported that downtime made it so that their workforce was unable to send or receive critical and timely files.** (Globalscape, Report: Dangerous File Sharing Practices Put Sensitive Data at Risk)

System availability issues can have a negative effect on the workforce's ability to send or receive critical and timely files securely and within established compliance mandates. Not only is this frustrating for end users, but also it's also dangerous, considering the information-sharing behavior of today's employees.

# The Four Most Common Causes Of Downtime

**90 percent of organizations have experienced downtime and a third deal with it at least once a month.** (Globalscape, Report: Dangerous File Sharing Practices Put Sensitive Data at Risk)

System downtime plagues organizations throughout every industry. Losing access to core systems, including email servers and backend processors, is more than just frustrating. It cripples employee productivity. When there are so many interconnected elements in a network, all it takes is one critical component to fail and cause an outage.

# Hardware Failure

**55 percent of organizations surveyed reported hardware failure as the number one cause of downtime.** (Emerson Network Power, 2016 Cost of Data Center Outages)

When there's a malfunction within your network, whether it's an inability to log in, access files, or transfer files, downtime problems are often the result of hardware failure, more than anything else. What's critical in this situation is whether or not you have the visibility over your infrastructure to catch the hardware failure before it becomes a problem and plan on how to handle hardware failure.

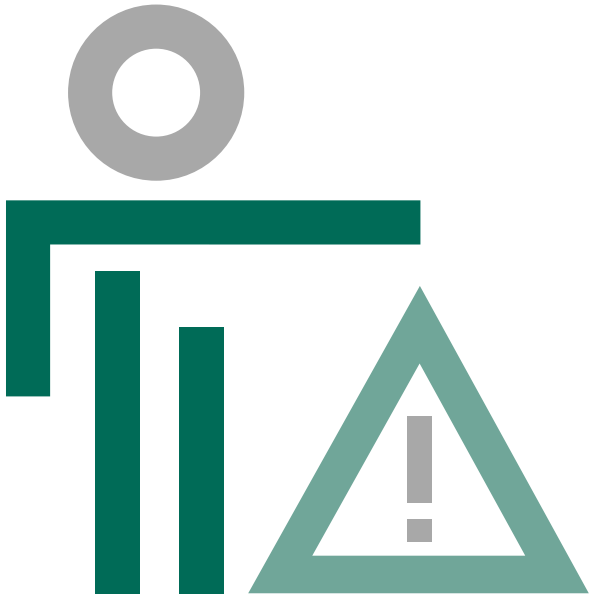
**Downtime Tip:** Minimize the downtime risk caused by hardware failure by selecting systems that support enhanced control and full infrastructure visibility, while still preventing hardware-related downtime. Look for a solution that offers a centralized platform, along with auditing, monitoring, and reporting capabilities to achieve full visibility of your data no matter where it resides in your network.

# Human Error

**22 percent of organizations surveyed reported human error as the cause of downtime.** (Emerson Network Power, 2016 Cost of Data Center Outages)

In 2016, JetBlue experienced a major outage at the Verizon data center that caused wide-spread flight delays. Media outlets reported that a maintenance operation knocked the Verizon data center offline. The outage brought to light that JetBlue didn't have a disaster recovery plan; that is, there was no automated backup plan or steps to take in case of such an emergency.

**Downtime Tip:** Minimize the downtime risk caused by human error by choosing data management tools that offer access controls in a centralized platform, which can further help for better management of your infrastructure and data.



# Software Failure

**18 percent of organizations surveyed reported software failure as the cause of downtime.** (Emerson Network Power, 2016 Cost of Data Center Outages)

Software failure-related downtime can happen during routine maintenance, system integration, or system updates. Additionally, software failure can happen as a result of a system overload, security updates, out-of-date software, or complex-fault recovery times.

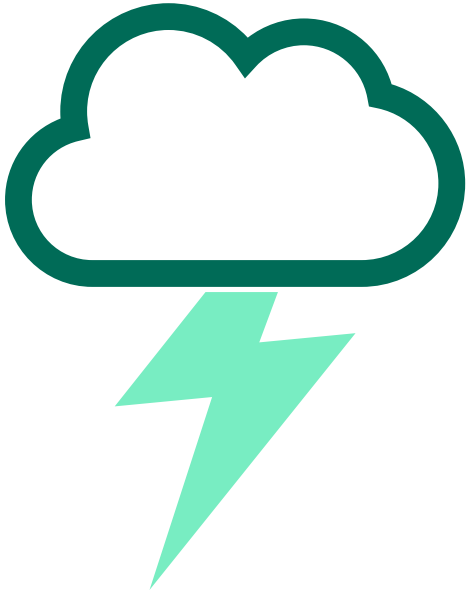
**Downtime Tip:** Protect your software and applications by being vigilant about monitoring your software and applications. Seek out a tool that offers a highly available environment in an active-active configuration to maximize uptime. Faults exist with applications, regardless of how good your infrastructure is designed.

# Natural Disasters

**5 percent of organizations surveyed reported natural disasters as the cause of downtime.** (Emerson Network Power, 2016 Cost of Data Center Outages)

The risk of downtime due to natural or manmade disasters, small accidents, rolling blackouts, or malicious intent grows exponentially every year. As we become increasingly dependent on technology, the costs and stakeholder frustrations associated with downtime increase right along with the causes and likelihood of a significant downtime event. It's enough to cause IT managers and business executives to lose sleep.

**Downtime Tip:** Have a disaster recovery plan in place and consider seeking out a data management solution to safeguard your data in the event of a natural disaster.



# A Proactive Approach To Preventing Downtime

**Before purchasing new technology and developing processes to mitigate the number and length of downtime events, it's critical to first understand the needs of your organization. How much would it cost your organization to be offline for 3 minutes? 30 minutes? 3 hours?**

In most cases, the cost outweighs the opportunity to proactively prepare and prevent downtime. You need a plan and a backup system. Business continuity (BC) and disaster recovery (DR) programs are important for every business to have in place, regardless of size, industry, or geographic location. While you may not be able to avoid downtime 100 percent, you can increase your uptime and have close to 100 percent service availability. From a disaster recovery server to a backup of configurations, here's how you can best prepare for downtime:

- **Know where you stand** – Evaluate last year's performance
- **Have a solid backup plan** – Evaluate your failover strategy
- **Do a configuration check** –Know the health of your databases and ensure that settings are compliant with your hardware
- **Analyze and resolve any recurring issues** – Uncover anything and everything that's slowing down your database, from patch updates, structural modifications, and anything that can be configured
- **Update statistics** – Archive old data if you're not using it anymore. This will dramatically reduce the amount of time to complete maintenance activities and enhance query performance
- **Scale infrastructure** beyond anticipated traffic spikes, such as installing load-balancing software to build resiliency if there's a system failure
- **Set up a robust system** – With a robust system, you can ensure a highly available solution that gives you a strategic advantage, with visibility, security, governance, control, and much more

# Reducing Downtime Risks: The Checklist

**Of course, the best downtime to deal with is no downtime. No IT team can guarantee 100 percent availability. However, there are several steps that organizations can take to minimize downtime and ensure better availability of core systems.**

- **Check The Slas Of All Key Vendors And Partners**
  Assess the level of availability promised in vendor contracts and if it doesn't meet business needs, explore alternatives. If your systems consistently come short of SLAs, consider implementing an active-active cluster.
- **Use Active-Active Clustering For All Core It Systems**
  Active-active clustering environments experience more uptime than active-passive clustering environments, with much less risk. When it comes to core IT systems, ensuring the highest level of availability is essential.
- **Deploy Load-Balancing And Highly Scalable Infrastructures**
  The ability to scale and balance workloads across multiple servers is critical to ensuring fast and efficient business transactions. That is, when one node is unavailable, such as when it is performing several actions on the same file, the other nodes can continue to process files.
- **Rely On A Single, Managed File Transfer Vendor**
  Using multiple file servers can create system-to-system integration vulnerabilities and issues, heightening a company's risk of downtime and system glitches. Using the same vendor ensures systems and processes are compatible, rather than competing.
- **Automate Backups Of Your Most Critical Data**
  Automating data backup to other servers or even off-site storage can minimize data loss due to downtime. Unrecoverable data loss can have far reaching effects on your business and customer or effects on your business and customer trust. Compliance can also take a hit: in February 2016, a hospital in Los Angeles was locked out of their email and access to health records for more than a week. No diagnostic test results or patient information was available. Some patients had to be transferred to other hospitals, which meant a loss of revenue for the hospital affected. An offsite backup of the data could've had that hospital back in service that same day.

# Benefits Of Managed File Transfer (MFT) With High Availability (HA)

**The technology and power behind MFT is built on a foundation security, visibility, and efficiency. With the right MFT solution, your organization can streamline your business critical processes, simplifying data management at every level, from controlling data access to preventing data loss, or managing workflows, all the while ensuring a secure and compliant environment. MFT plays a crucial role in an organization's data management strategy. For organizations that need uninterrupted uptime, MFT with High Availability offers the most benefits.**

Choosing an enterprise-ready MFT solution deployed in active active cluster provides High Availability using multiple MFT instances and a load balancer for non-stop availability or your network. What can you achieve with the right deployment of MFT with HA?

**Here's a look:**

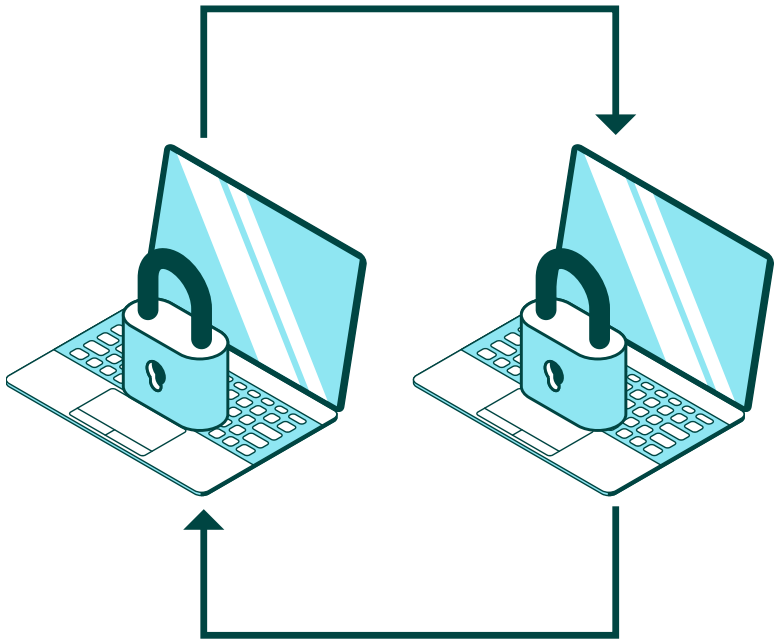
- **Maintain Availability:** Keep your network online in some capacity during any planned or unplanned outages
- **Stability and Flexibility:** Implement multiple nodes of MFT to help with load balancing of network traffic
- **Meet SLAs:** Achieve enhanced throughput that allows for a collective MFT environment to efficiently use available resources
- **Improves Scalability:** Sharing common configurations eliminates the challenge of setting up multiple servers with different configurations

The best type of MFT solution will simplify how you manage and protect your data infrastructure. The next few pages include questions and criteria to consider when evaluating MFT with HA for a data management strategy focusing in on downtime risk.

# Robust Security

**Is your data protected at rest and in transit? Do you have visibility over your data transfer activity?**

Security is critical for every company, in every industry. The aftermath of a data breach can quickly land your company in hot water—and severely affect your company's reputation and revenue. Whether you're trying to protect proprietary data, consumer data, financial records, and beyond; a solution that offers robust security measures will ensure that you protect your sensitive data every step of the away. Be sure that your MFT solution delivers enterprise level security for your organization's most sensitive data and supports compliance mandates for your industry.



# Meet Compliance Mandates

**Does the MFT solution help you meet compliance regulations like PCI DSS, FIPS 140-2, HIPAA, and SOX?**

An MFT deployment model can help you meet, exceed and maintain the highest compliance standards, including PCI DSS, FIPS 140-2, HIPAA, and Sarbanes-Oxley (SOX), among others. Operational visibility is a key benefit of a solid MFT solution, as it can help catch security vulnerabilities or compliance concerns before they become a problem.

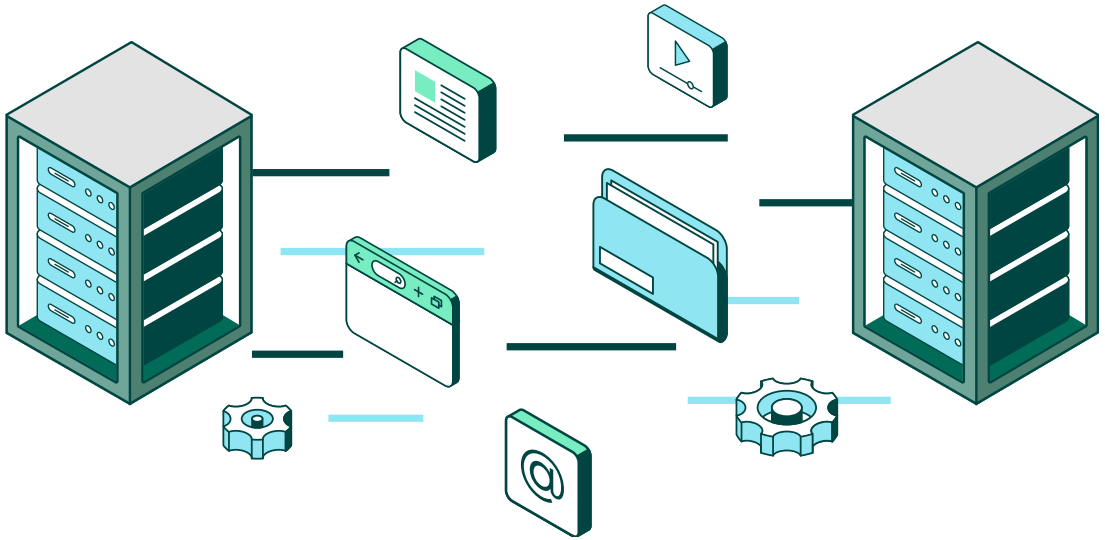
Consider a situation where you have failed data transfers or multiple login attempts. These are important pieces of information an IT professional should be alerted to so they can address problems quickly. Imagine the potential problems that a lack of transparency could cause an organization, such as a greater risk of failing compliance mandates or inefficient processes and slow file transfers. Failing compliance mandates can be expensive and time consuming.

# Simplify Data Management

**Can the MFT solution automate processes? If a managed file transfer platform doesn't simplify how you manage and protect your data and infrastructure, then you have to ask yourself if that's the best platform for your data transfer needs. A robust MFT solution offers an easy and efficient way to manage data through the use of automation tools and functionalities. As data increases in volume and flow, workflows and data management processes can become extremely complex and tedious to manage.**

If your organization lacks sufficient manpower, automation tools can keep workflows and processes going. Automation tools offered through a MFT solution provide:

- Easy administration and end-user interfaces
- Efficient and easy-to-use processes (employees are less likely to resort to Shadow IT)
- Advanced auditing and reporting features
- Easy-to-configure automation to prevent inefficient manual processes and human errors



# Take Back Control

**Downtime isn't just about a temporary inconvenience for a company, its employees, and customers. That's one drawback on top of many. The negative effects that follow unplanned downtime can have an expensive domino effect on an organization's budget across the board, which is why it's critical to understand where your vulnerabilities and risk factors lie.**

Additionally, having a thorough understanding about your business goals and how your organization manages data can help you determine the best strategy and tools your organization needs to prevent the problems that follow unplanned downtime. An MFT solution is a powerful tool to support your data management strategy.

The right MFT solution will not only be compatible with your organization's technology environment, but will also go beyond IT considerations to provide real opportunities to achieve greater operational efficiency, ensure regulatory compliance, and provide additional business results, including measurable impact on ROI. Globalscape can provide any organization—regardless of size or business volume—with the freedom to exchange information online quickly, securely, and reliably.

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.



fta-gs-wp-1122-r1-79d