Kaseya Case Study

MSP Avoids Data Exposure and Recovers Stolen Laptop within 48 Hours

Kaseya IT services automation solution remotely tracks system, wipes the hard drive and leads police to the thief's front door

Bad things happen to good people all too often in this world, a lesson that "Marla" found out recently. A social worker for Work Opportunities, a publically-funded non-profit that helps the physically challenged find employment, exited an appointment she had scheduled with a client and found that her car had been broken into. Not the thanks you'd expect for someone who dedicates her life to helping the disabled lead a normal life through an honest day's work. In addition to some personal items and several dollars of change from the ashtray the thief managed to steal Marla's work laptop that contained personally-identifiable information (PII) about her clients, their medical histories and the work she was doing for them.

In the world of social services, this is a big problem. Work Opportunities is required by law and common decency to ensure its clients' information is always protected from public exposure, and the government takes careful steps to ensure companies dealing with PII have taken the steps to protect their clients' privacy. The risk of non-compliance includes a lack of public trust, the cost of compensating victims, loss of funding, heavy fines, and, in extreme cases, jail time for executives.

Luckily for Work Opportunities, Marla and her clients, the organization relies on managed service provider True North to protect it from data loss and recover equipment that is stolen or misplaced.

A Mission to Protect Business Information

Work Opportunities' security and data protection requirements are not unique. Nearly every company needs to protect its customer data for compliance, privacy and business continuity reasons. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that healthcare organizations protect patient records at all times, and the state of Washington—where True North operates—has a law on the books that requires all companies to inform customers if their personal information is compromised. As an IT service provider that focuses on small businesses and earns more than 70 percent of its business from the healthcare sector—True North needs to assure its clients that it has their back when it comes to protecting personally-identifiable information.

As desktops and servers give way to laptops, iPads and cloud services, IT service providers are struggling to maintain and enforce dynamic data security needs. According to Matt Murren, CEO of True North, many IT service providers don't have robust IT policies in place to adequately protect their clients' information and often lack the technology necessary to identify, track and secure information stored on increasingly-mobile infrastructure. As a result, they often use point products or legacy tools like LogMeIn. These systems management solutions enable administrators to remotely maintain distributed machines but often require permission from users to execute commands. In the case of theft or loss, it's hard to imagine the administrator getting that kind of access.

"If you don't have an active connection initiated by the user there's really nothing you can do," Murren said. "You can't wipe the machine and delete the data. Nor can you track an IP address. Your hands are tied, and the system is most likely gone."

An Integrated IT Systems Management Solution from Kaseya

Realizing that an MSP is only as good as its tools, True North relies on an IT services automation solution from Kaseya that gives administrators complete visibility into and control over its customer systems. Kaseya consolidates IT management on a central Web-based management console, allowing True North administrators to monitor, maintain, update, back up and secure any machine in their customers' environments anytime from anywhere. The solution's policy-based management architecture allows administrators to set pre-determined policies for groups of systems—whether they are

Kaseya Customer

True North ITG
Seattle, Wash.
www.truenorthitg.com

Industry

Managed Service Provider

Business Challenges

- Proactively manage and track increasingly mobile customer environments
- Protect and secure customers' business data
- Recover lost or stolen equipment and get users back up and running quickly
- Ensure customers remain in compliance of federal, state and industry regulations and can easily prove they are meeting standards

Solution

- Kaseya Managed Service Automation Solution

Service Category

- Business Continuity Services
- Security Services

Core Benefit(s) Delivered

- Higher quality of IT service for users
- Better service delivery for users
- Better Control of IT systems for compliance

Kaseya

www.kaseya.com

sorted by site, platform, operating system, business unit or any other criteria—and push them out across the entire environment with the push of a button. Kaseya then monitors the machines to make sure they remain in compliance of those policies.

True North previously used an IT systems management solution from N-Able but found that it didn't provide the level of control the service provider needed over its customers' distributed systems. A lack of reliable real-time auditing and a robust reporting mechanism also made it difficult to provide, audit and prove the level of service True North promised its customers.

"We wanted a tool that worked," Murren said. "N-Able just couldn't scale enough for our needs or provide the visibility and control we needed to effectively manage and maintain our clients' IT environments."

Recognizing that Kaseya's integrated and automated solution provided operational efficiencies that increased total cost of ownership while improving service delivery, True North made the switch and now has the Kaseya agent installed on more than 5,000 customer machines. Auditing and reporting provide invaluable management data on each system—such as model number, operating system, installed applications and drivers and user data—enabling proactive maintenance and quick remediation. Kaseya also fully integrates with Connectwise, True North's help desk solution, helping the company automate ticketing and billing.

"Kaseya is our core offering," Murren said. "It allows us to be proactive and to provide quality IT services to our customers in a cost-efficient, effective manner."

In addition, Kaseya combines agent technology and agentless monitoring, ensuring that distributed systems are always connected to a central management server. No system is able to fall through the cracks—regardless of theft or loss. If the machine logs onto the internet, True North can identify, track and control it. And that's exactly what they were able to do for Marla's laptop.

Take Control of Your Distributed Systems— No Matter Who Holds Them

Per their disaster recovery plan, Work Opportunities immediately called its IT service provider True North upon realizing the laptop was stolen. True North's Field Sales Manager Ted Grandpre then instructed the client to immediately file a police report, including a statement that said True North would be working on tracking down the stolen equipment electronically.

Using Kaseya, True North created a script that would alert an administrator if the agent on the laptop tried to connect to the management server—which it would automatically do if anyone turned on the machine. Sure enough, the machine popped up within several hours, and an administrator surreptitiously did a remote wipe of the data without alerting the user. He made sure to do it under the radar while keeping most basic functions operational so the thief wouldn't recognize they were being watched.

Over the next 24 hours, True North used Kaseya to remote in and capture screenshots of activity on the missing laptop, including updates to the user's Facebook profile, timeline and social gaming. The coup d'état came when the user posted: "YES got a new lap top today!!!!and I'm lovin it". A photo of the user was posted along with the status update, putting a face with the profile. Google and White Pages queries provided an address and revealed a long criminal record with 49 arrests.

A representative from True North then contacted the police, identifying himself as an IT service provider for Work Opportunities and as a certified and licensed cyber security expert. He updated the previously-filed police report and handed over the screen shots and address information. Less than 48 hours after first reporting the stolen laptop, the device was recovered by the police and returned to Work Opportunities. A quick cleanse and restore later and Marla had her fully-functioning laptop back in hand.

"Complete visibility and absolute control through Kaseya allows us to keep tabs on all our customers' systems, monitoring them, maintaining them and protecting them—all from a central management console."

Matt Murren
CEO, True North ITG

Summary Benefits

- Improve margins by managing thousands of customer systems with fewer administrators
- Improving customer stickiness through quality systems management, business continuity and security service offerings
- Preserve customers' corporate reputation by preventing their data from being exposed
- Recovered customer's laptop 48 hours after it was stolen, getting employee back up and working quickly

Kaseya

www.kaseya.com

A Two-Pronged Security Strategy that Protects Data and Recovers Hardware

Kaseya allows True North to formulate and execute on a two-pronged security strategy, effectively ensuring that its customer's systems and business data remain protected at all times and its clients remain in compliance of any regulations set up to protect consumers. Intuitive reporting ensures regular maintenance is completed and the client is aware of the work True North is doing on its behalf.

"Our clients have complex compliance requirements that if unchecked could be costly to their business, their employees and their customers," Murren said. "True North needs to act as a reliable business partner that is dedicated to keeping data safe. Complete visibility and absolute control through Kaseya allows us to keep tabs on all our customers' systems, monitoring them, maintaining them and protecting them—all from a central management console."

The ability to remotely wipe systems protects business data from falling into the wrong hands while the capability to track devices wherever they are enables equipment recovery. Combined with the ability to restore data, applications and settings quickly and efficiently through policy-based management, the entire business continuity strategy speeds up the process of getting that system back into production quickly and efficiently. The result is less risk and more productivity.

In the case of Work Opportunities, True North was able to wipe the device as soon as it was booted up, preventing its data from being compromised. Not just an embarrassment, the non-profit could have been forced to inform its clients their personal and medical information was exposed, harming its reputation and ability to execute on its mission True North was also able to recover the cost of a replacement laptop, a savings of $2,000.

The true value, says Murren, is peace of mind. True North customers know that their data is safe and can focus on its core mission. In the case of Work Opportunities, their mission is helping people and making the world a better place.

And the laptop thief? Well, she went to jail.

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to www.kaseya.com/download for a FREE trial.

Visit: www.kaseya.com | Email: sales@kaseya.com | Like: Facebook.com/KaseyaFan | Follow: @KaseyaCorp

Kaseya

www.kaseya.com