JUNIPER NETWORKS CUSTOMER PROFILE

INDUSTRY Networking Equipment

LOCATION Sunnyvale, CA

EMPLOYEES 9,500

FOUNDED 1996

Juniper Networks: Innovation, Security, Defensibility

Read how Juniper used e-discovery technology and tracking metrics to gain security, defensibility, and affordability for the entire company.
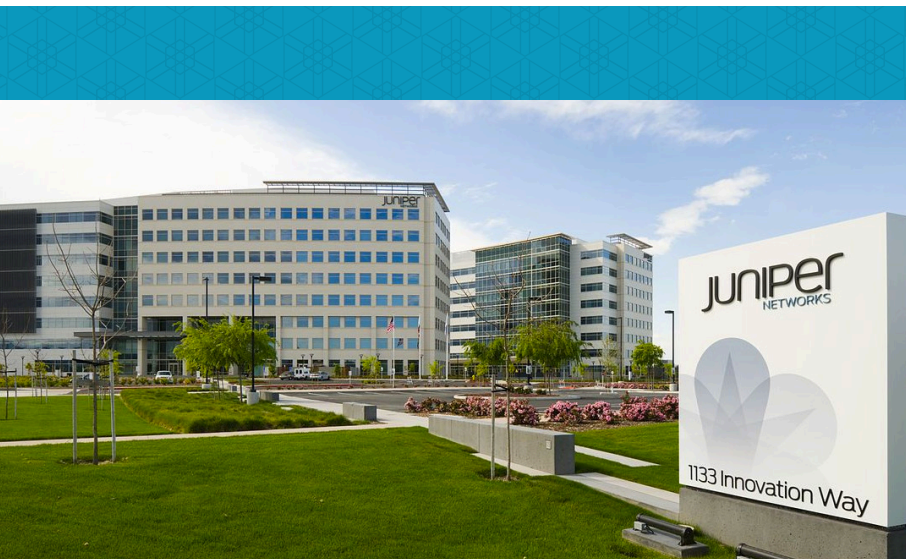
Tracking Metrics, Reducing Data, Adding Efficiency Equals Reduced Spend

When it comes to e-discovery activities, the primary goal of the legal department is defensibility. For IT, it's security and accessibility. For anyone in business operations, it's return on investments.

"Juniper Networks prides itself on innovation," says Chris Sitter, Head of Global E-Discovery & Digital Forensics, Juniper Networks.

> "Every time you check Facebook or Instagram or What's App on your phone, it's going over our equipment, so we have a very important job to do. This also presents several legal and regulatory challenges, because facilitating innovation means you can't overly constrict engineers, and engineer culture is typically one that is very open. With Juniper based in Silicon Valley, it's already very difficult to attract and retain talent, so you don't want to be known as the company where legal and information security are breathing down your neck all the time, and you can't enjoy the work that you do. So, it's a very interesting dance meeting all of our legal and regulatory obligations while continuing to further innovation and meet business requirements."

ABOUT JUNIPER NETWORKS

Juniper Networks is an American multinational corporation headquartered in Sunnyvale, California that develops and markets networking products. Its products include routers, switches, network management software, network security products, and software-defined networking technology.

Sitter has been at Juniper for a little over two-and-a-half years, and says, "Back then, Juniper was the typical company when it comes to e-discovery—they had some connections with information security, they had a general understanding of where data might reside, but they were entirely reliant on the custodial interview, which creates issues with defensibility. On top of that, all of the technology components were outsourced. So, other than email, a vendor had to come in, which made the cost of e-discovery very high."

When Sitter started, he was an individual contributor with no budget. But once he took a snapshot of how much the company spent on vendor fees and the head count needed to manage the spreadsheet tracking legal holds, he took that information to the business stakeholders, and he said, "We're spending XYZ on this, give me a half million dollars and I will give you an 800% ROI in six months. The key, of course, was that I had to deliver on that."

Once that happened, Chris and his team started getting additional support to continue to build out their operations, working with shareholders to create a vision for the future, while reducing operational spend.

The end result is an entirely cloud-based e-discovery and forensic environment which spans the entire EDRM.

Utilizing existing e-discovery tools, Chris and his team can process over 1,000,000 emails a minute while maintaining compliance with all international data privacy laws. Juniper also defensibly deleted their legacy data volume from 22 petabytes to 14 terabytes. All of which saved the business $7 million year-over-year.

Along with utilizing technology, Juniper went through the process of mapping data and bringing information governance policies into compliance. Sitter gives this example of one of the more difficult parts of that process:

"There was a misunderstanding about ten years ago, no one knows who said what, but the belief was that all email had to be retained for two years. So they started pulling hard drives from laptops and putting yellow sticky notes on them, often with illegible handwriting as to what was on that drive. They were stored under people's desks, in cabinets, in lockers, until they overflowed, and then they were put on pallets. When I came on, there were over 14,000 hard drives from former employees. So we inventoried all the drives and analyzed them, took a snapshot of the metadata, then went through the process of shredding the drives once we determined that none of the data was on hold. If anything was on hold, we simply followed our standard process."

"As a company that innovates, Juniper wants to keep control of their data as much as they can, for security, defensibility, and affordability. Using systems that automate that process, coupled with the latest user-friendly tools and technologically savvy attorneys, Juniper found that e-discovery rapidly moved from the forensic realm to the project management realm."

Christopher Sitter
Head of Global E-Discovery & Digital Forensics
Juniper Networks

The Search for the Right Solution

Chris Sitter's Tips for Selecting the Right E-Discovery Technology:

- Check their defensibility profile. Exterro comes in beautifully on this. Everything must be documented and easily tracked so that company can show they did their due diligence.

- Make sure it can handle all of your potential data sources—email, Office 365, workstation, work shares, sharepoints, mobile, etc.—Juniper has over 17, 000 different applications currently in use. Then bring in legal, IT, and compliance to make sure everything is integrated.

- Make sure they are strong when it comes to information security. You want to make sure they protect your data.

- Make sure the technology vendor understands international privacy laws so that your company isn't put at risk.

- Make sure the system integrates with your existing business systems.

E-Discovery through Forensics

Something that sets the Juniper team apart is that rather than reporting to the legal department, they instead report to information security and the Chief Information Security Officer, so they operate more like an internal consultancy providing services to the company. Chris Sitter describes it as such:

"Our team is the central hub for all investigations, litigation, and federal inquiries for the entire company. So, besides standard e-discovery related to litigation, we also can have HR investigations or compliance investigations, from someone claiming a little too much on their expense reports to potential FCPA violations where a sales individual is being accused of bribing a foreign official.

All of these come through our office, and we partner with a rock star of a paralegal to help keep everything straight by using the Exterro Litigation Hold Suite. The system is set up so that the moment we receive any indication of activity, we can do published or unpublished holds through the Exterro system, and the greatest benefit of this is the automation. It powers us to start preserving data within a matter of seconds of receiving that email."

From the beginning, the goal for the Juniper team has been to do everything in-house, except for a few key areas where it is more beneficial to outsource, such as outside counsel and document review. But Juniper handles 100% of all investigations and processing, and 95% of all collections in-house. An outside vendor allows Juniper to host data, so that it can be viewed anywhere in the world. And there is a backup forensics vendor in case there is trouble accessing data in places where the regional political climate might make it difficult for the Juniper team to travel.

"About one year in," Sitter says, "once I had visibility into all of our invoices, I used that as justification

to build out a formal forensics lab, which included in-house processing and hosting capabilities. From there, I started to interact with the different groups in Juniper to identify the key stakeholders and their challenges. And then, we went into a lot of education in order to simply understand the entire process, and how we could make people's lives easier."

This setup allows the team to interact directly without the use of a liaison between IT and Legal. The key is for all parties having the ability to communicate with an understanding the case life cycle, and then being able to translate those requirements into actual work product.

Chris continues, "When I started building my team, this was the culture I implemented with them. I interact with the GC and all the VP's directly, as well as with my team. And they know that they can reach out to anyone at any moment and get a rapid answer. We usually have people respond to preservation requests in less than half an hour. We also make sure that the team is not only up to date on the latest legal trends, but also on the latest global security trends, since we're the ones who are getting access to the data."

The Future of E-Discovery at Juniper

Chris Sitter sums up where Juniper has been and where they're going in this way: "We're the first company to take all of our e-discovery and forensics systems and put them in the cloud. We've developed a case intake system that provides transparency to all the key stakeholders about when they receive the notification of reasonable litigation, as well as notifying our team, so we can help guide them through the preservation process. We have an entirely virtualized forensics lab sitting in Amazon web services. We can process millions of emails in a matter of seconds. And we keep expanding our capabilities."