proofpoint.

CUSTOMER STORY

# Major Cancer Center Safeguards Patient and Research Data With Proofpoint

## The Challenge

- Protect structured and unstructured data in an open academic environment
- Improve information security strategy
- Strengthen internal culture of security

## The Solution

- Proofpoint Managed Services for Information Protection

## The Results

- Deployed managed data loss prevention (DLP) program in phases
- Deployed and tuned DLP technology with minimal false positives
- Enabled ongoing alerting, reporting and incident response processes

## The Company

This well-known, nationally recognized cancer research and treatment center is affiliated with a state university system. Its mission is to treat and prevent cancer locally around the globe. It does this through programs focused on patient care, treatments and research, and education. This also means the center has a wide range of critical data to protect. The organization needed to ensure that it had a comprehensive program to address its data security and compliance challenges.

## The Challenge

**Making the case for information protection**

The cancer center had already made major cybersecurity investments to protect its perimeter. But it also needed to update its information security so it could comply with healthcare privacy regulations and policies. The center was committed to stopping threats from both inside and outside the organization.

Because of the open nature of the university network, the security management team was especially interested in DLP technologies for protecting both their structured and unstructured data. The team reached out to Proofpoint to help with several things. They wanted to identify and prioritize their critical assets. They also needed recommendations on technologies to help them meet their requirements. And finally, they wanted to set up and manage a comprehensive security program.

## The Solution

### Safeguarding critical assets and information

Proofpoint Information Protection Programs are deployed using a phased approach to help guide organizations in protecting their most important assets. The team worked with the cancer center to identify and prioritize its patient data, along with its other intellectual property, such as research. The team also helped establish security policies and workflows specific to the center's needs.

"One of our most important tasks was to work with Proofpoint in the planning phases. We wanted to learn and thoroughly understand how people use our information technology," said the center's information security project leader. "We both learned a lot about our business during that initial consulting and technology evaluation phase."

Proofpoint and the cancer center looked at several different DLP technologies using a 700-point use-case evaluation matrix. The results helped them to identify the best solution for the center's needs. This included technology for protecting data in motion, in use and at rest.

> "We were able to deploy a very complex set of technologies in a very short time. This is thanks to the expert skills of the Proofpoint Professional Services team. Not only are they experts in DLP, but they have an in-depth knowledge of how virtualization and network technologies operate, which has been valuable in helping us plan and operate our program."
>
> **Major Cancer Research and Treatment Center**

Going beyond the standard patient data and compliance security requirements, Proofpoint helped identify the cancer center's genomic research as a priority for protection. And together, Proofpoint and the center developed a set of DLP policies for all of the center's key assets.

Understanding how cancer center employees created, stored and transmitted their key data was critical. And it allowed Proofpoint Professional Services to fine-tune its technology from the start. This helped ensure the security staff would not be overwhelmed with noise from hundreds or even thousands of alerts. From day one there were very few false positives. Proper tuning also ensured that security analysts could review the information that was the most relevant to the cancer center. And do so as quickly and accurately as possible.

### Putting information protection in action

After helping the center deploy its solution, Proofpoint moved on to the next phase. It took charge managing the program through its Managed Security Services for Information Protection. The Proofpoint SOC includes two key teams that help. The cancer center worked with both security monitoring and analytics (SM&A) experts as well as a security platform engineering (SPE) group to manage its information protection program.

Proofpoint SM&A team members constantly observe, extract and correlate data on how information is moving in and out of the cancer center. Then they use these insights to provide the center with actionable recommendations as the program evolves. Knowing the business drivers for the client Information Protection Program is critical. It lets the team identify, triage, remediate and report any suspicious events. And it gives them the ability to do it much faster than traditional MSSPs.

The Proofpoint SPE group assists the SM&A team with technical support. This ensures that every component in the solution delivers 100% uptime. The group also helps the team to develop, maintain and configure adjustments in scope and policy governance.

The Proofpoint Managed Security Service also provides the team with in-depth reports. These show the center's overall security posture and intelligence issues. With policy reports, the organization's governance group can assess the accuracy of alerts and the severity of incidents. These reports also highlight trouble areas that may need more attention. And with compliance reports, the auditing stakeholders get the details they need to show compliance with policies and regulations.

### Strengthening internal best practices

Just days after deploying the solution, the center's SOC team spotted risky staff behavior at the center's campus. A doctor in the organization was violating policy by transferring proprietary research information to a university outside the United States. The SOC alerted the cancer center's legal and compliance team, who worked with Proofpoint to resolve the issue.

The SOC teams are constantly analyzing the impact of all incidents or violations of policy. This allows them to assess how existing policies may need to change to minimize or eliminate vulnerabilities. In this case, the policies no longer allow users to auto-forward specific documents.

## The Results

### Building insight and consistently protecting research and healthcare assets

Proofpoint Professional Services unlocked a variety of benefits for the cancer center. Proofpoint helped the center identify and prioritize critical assets; create workflows customized to its way of doing business; choose the best DLP technology; then operationalize its program. As a result, the cancer center gained:

- A proven, successful process for implementing and using DLP
- Strong expertise as an extension of its security team for regular monitoring of structured and unstructured data
- A clear, more accurate picture of its security posture and how data is moving in and out of the organization
- Analytics and reporting to help make better decisions about priorities and resource allocation for information security

"We have not had any problems in our initial implementation. This is thanks to the technical design and planning service from Proofpoint," said a cancer center security professional. "Proofpoint reports contain a lot of very useful information that helps us improve our operating performance. They give our non-technical stakeholders a way to understand the issues. And they give us a much higher level of confidence when we are making decisions."

## LEARN MORE

For more information, visit **proofpoint.com**.