proofpoint

CUSTOMER STORY

Cancer Treatment Facility Employees Now Surf Safely with Proofpoint

Proofpoint Browser Isolation Enables Private Web Access while Strengthening Security

THE CHALLENGE

- Protect confidential patient information from all forms of attack
- Block targeted phishing and malware attacks
- Enable staff to access the web securely for personal email and browsing
- Increase productivity of staff, doctors and IT Team

THE SOLUTION

- Proofpoint Enterprise Protection and Email Fraud Defense
- Proofpoint Targeted Attack Protection and Threat Response Auto Pull
- Proofpoint Browser Isolation and Email Isolation

THE RESULTS

- Allowed employees to browse the web or access personal web-based email without jeopardizing patient or corporate confidential information
- Blocked virtually all phishing and malware attacks
- Increased productivity of staff and IT department

The Organization

This leading cancer treatment facility provides leading-edge treatment and compassionate care to those diagnosed with cancer or blood disorders. And it's done so for more than 30 years. With 10 treatment centers in its state, it's established relationships with renowned institutions such as MD Anderson and Memorial Sloan Kettering. These relationships allow the facility's patients to heal and recover at home while benefiting from regimens commonly reserved for medical teaching institutions.

The Challenge

Allow personal web and email use without jeopardizing company security

Attackers often try multiple ways to breach a user's account. These include brute-force attacks and key-logging software. But phishing emails remain the most effective way to steal a user's credentials. Often operating from multiple countries, these threat actors have become increasingly sophisticated in their attempts to lure users into clicking a malicious link and divulging confidential account credentials. And they often target specific "high value" individuals with customized attacks via both corporate and personal email.

Employee access to the internet has put many companies in an awkward position. This is especially true in highly-regulated industries such as health care. Laws such as the EU's General Data Protection Regulation (GDPR), and HIPAA in the US, guarantee personal privacy for patients and individuals. And the trend to protect privacy is growing. If a company blocks all personal access to the web, the IT department receives a torrent of employee complaints. But if IT allows free access to the internet, they open the company to more vectors of attack. This could be through dangerous links on unknown websites or phishing emails targeted at personal accounts. And if an attacker succeeds in breaching a personal account, they can often jump on to the corporate data system and steal privileged information. This exposes the company to financial losses and fines. Not to mention negative publicity and damage to its reputation.

The director of IT at the cancer treatment facility experienced this dilemma quite recently. The facility had adopted a policy that restricted universal access to the web, but employee complaints, including from C-level executives, were overwhelming.

"People were furious," said the IT director. "Once you start limiting usage in a medical setting, you pretty much render the internet useless for a healthcare organization."

In response to the adverse reaction, IT opened up access to the internet. Almost immediately they came under attack, primarily through private email accounts or links to malware on public internet sites.

> "Browser Isolation gave us exactly the balance we were looking for. It allows our employees to safely and privately access the web and view their personal email without jeopardizing our corporate security."
>
> Director of information technology, cancer treatment facility

The IT director described one attack: "We had an employee log on to their Yahoo email account and click on a bad link, which allowed malware into our corporate network. The malware, designed specifically to steal personal information, made it into one of our servers before we stopped it. Fortunately, we got it in time. But it was close."

This near-miss came after a successful ransomware attack on another health network in the state. This was done by criminals who successfully encrypted the organization's most sensitive patient information and demanded a ransom fee of nearly $500K. This incident forced the IT director and his team to start looking at ways to allow their employees to use the public internet without increasing the company's risk profile. They turned to Proofpoint for their answer.

The Solution

Proofpoint Browser Isolation

"Proofpoint had helped us tremendously in protecting our corporate email," explained the IT director. "Enterprise Protection and Email Fraud Defense block about 40,000 potentially malicious messages a day. We have a high degree of confidence in Proofpoint technology. When we needed a way to expand our security umbrella to cover employees when accessing their private email or browsing the web, turning to Proofpoint was an easy call."

Proofpoint engineers suggested that the organization try out Email and Browser Isolation.

According to a report by Osterman Research,[1] 60% of attacks in the enterprise come from private browsing or email use on corporate devices. Proofpoint Browser Isolation, which includes Email Isolation, is a cloud-based feature that works with your existing Proofpoint solutions and filters. Browser Isolation also leverages the intelligent threat technology of Proofpoint Targeted Attack Protection (TAP) to identify dangerous phishing links or other malware embedded in websites or attachments to personal email.

1 Osterman Research. "Why You Should Seriously Consider Web Isolation Technology." December 2018.

Browser Isolation allows the IT Team to send all private, non-corporate traffic into a virtual "container" that insulates the corporate network from personal use. Once in this protected sandbox, TAP analyzes the site or email for potential threats, removes or rewrites any malicious code, and then sends it back to the requestor in a "sanitized" format that the recipient can view without risk of triggering a phishing or malware attack. Users can view the contents of the site as usual. But they can't download or upload content. And if the content is restricted based on domain-specific settings, a user cannot input data into forms. If a phishing email does get through and the user tries to click the link, TAP prevents the user from going to the site and notifies the security team that the user's machine might be affected. And if TAP deems a URL safe, users are given the option of leaving the isolated container environment and loading the full version of the website.

Browser Isolation takes a tailored, risk-based approach to keeping users safe while browsing or accessing web-based email accounts. Private email or URL requests can be handled in multiple ways. While most companies choose to direct all personal traffic into the Browser Isolation container, users can be placed into various categories of risk and have their traffic treated differently depending on several key risk factors. For example, for highly-targeted individuals, or people with special access privileges, the system can divert all private email and browsing traffic into the isolation container. On the other hand, for users who don't have access to sensitive information or may not require this level of security, IT can direct a subset of their traffic—email from known-bad sites, block-listed locations, or URLs deemed "risky"—to the isolation container. This risk-based approach gives IT the flexibility to support a variety of user types, no matter their risk profile, without endangering the corporate network. Also, as regulations protecting employee privacy increase, Proofpoint Browser Isolation gives the company the option to anonymize and encrypt all personal employee information, thus maintaining employee privacy and significantly reducing compliance costs.

"Browser Isolation gave us exactly the balance we were looking for," said the IT director. "It allows our employees to safely and privately access the web and view their personal email without jeopardizing our corporate security. We send all traffic into the container except for allow-listed sites that people regularly use for work purposes. If not, the email or URL goes into isolation. They can't download from there; they can't print from there; they can't upload from there unless we are sure the message or link is clean."

The Results

Browser Isolation increased security while allowing outside access

After a successful trial involving a handful of heavily-targeted accounts, the organization rolled out Browser Isolation to all of its employees. By implementing Browser Isolation, the IT Team effectively killed two birds with one stone. Their employees could surf the web for personal business. Or they could access their cloud-based email accounts without worrying about accidentally triggering a malicious link.

The results were immediately apparent, to both employees and the IT team.

"The feedback has been extremely positive," said the IT director. "Our users were tired of submitting requests to IT to access a particular website or view their cloud-based email. Not only has Browser Isolation made the staff and doctors more productive, but it's also saved the IT team a significant amount of time."

Before using Browser Isolation, the IT team investigated 15-20 potentially compromised accounts weekly, with each one taking from 10 minutes to an hour to resolve. Now, the number of suspect accounts is near zero. Browser Isolation has dramatically reduced the size of the organization's attack surface.

"Phishing has always been our biggest concern," emphasized the IT director. "Bad actors have gotten very good at fooling people into thinking a fake email is genuine and safe. No matter how much training you do, sooner or later someone will hit a bad link and download something nasty. It's just human nature. Part of our job is to protect people, no matter how or where they are working. Browser Isolation from Proofpoint has given us a much more secure network."

LEARN MORE

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