

# Leading Biotechnology Company Selects ColorTokens for Legacy Infrastructure Protection

INDUSTRY:  
Pharmaceutical

HEADQUARTERS: U.S.A.

## Overview

A leading biotechnology and development company with over 10,000 employees are in the business of helping people. Their primary focus is on researching devastating neurological diseases along with enhancing the quality of life for their terminal patients. The prominent biotechnology company yearned for a way not only to protect their employee's information, but their patients as well. As a business that works closely with people, they prioritize caring for those individuals and ensuring the security of the entrusted data. However, the company had legacy systems that put them at higher risk for malicious cyberattacks.

With their vendor no longer providing security updates for these legacy systems, the company found themselves vulnerable to security breaches and ongoing cyber threats. To address this concern, they searched for a cybersecurity company to assist them in the protection of their data, which is where ColorTokens came in.

## The Challenge

The biotechnology company needed someone who could fulfill the internal and external mandated regulatory and compliance requirements while protecting their patients and business. Their use of Windows XP and Windows 2003 systems meant they were in dire need of immediate protection of their susceptible legacy systems. Through their struggles, they came up with four outcomes they wanted to gain from a partnership.

### Desired Outcomes:

1. Restrict connectivity from pertinent systems to other systems to reduce the likeliness of exploitation
2. Reduce the attack surface across their server infrastructure by restricting lateral movement
3. Reduction of the blast radius if in fact there was any damage or a bad axel in their environment
4. Ease of visibility and management for this solution

## The Approach

When given the task, ColorTokens produced a well-defined POC in five working days. Our efficiency and detailed POC showed the quality and value of our product.

There were four ways we were able to show the ColorTokens value:

**EXTENSIVE UNDERSTANDING:** With a comprehensive understanding of their asset lists, we were then able to deploy all assets immediately. Our quick actions allowed the biotechnology company to begin receiving flow data quickly.

“Biogen is extremely happy with the results to date and are expanding their footprint to include additional systems within their infrastructure”

**PRODUCT EDUCATION:** As a company of their stature, it is no surprise they had a stand-up security team already in place. We were able to begin training their in-house security team as well as the third-party organization they use on our platform immediately. As a result of being able to start training immediately, we were able to save crucial time and the in-house team picked up the trainings quickly.

**LEGACY MAP:** The company was very impressed by the legacy map we produced as it showed the accurate communication happening between their systems. Not only did it show network connections, but also where a breach was occurring. The intricacy of our legacy map put us ahead.

**LEGACY TAGS:** The biotechnology company was especially happy with their new ability to use NLP (natural language policy) to configure and protect legacy systems with accurate tagging.

## Results and Benefits

The leading biotechnology company has gleaned immense improvement in security due to their implementation of ColorTokens products:

Desired Outcome Results:

1. **5 million** unauthorized network connections were proactively prevented from gaining access
2. **90 percent** reduction of the attack surface
3. **80 percent** reduction of the blast radius
4. **50 percent** of the licenses they purchased are installed and enforced—Remaining percentage is due to unused licenses they bought for legacy systems they were unable to upgrade.

## Conclusion

ColorTokens was able to secure the biotechnology's company's legacy systems, provide a comprehensive platform to see connections and breaches, and educate the security teams quickly. Yet, the true marker of their success was when the company confirmed they would be coming back to ColorTokens for other security help. They are now interested in Xaccess for their overseas locations, moving their unused licenses into their AD environment, and interested in our agentless solution. The investigations into our other products and uses display our efficiency within a company and the lasting impact we continue to have for our customers.

### Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit [colortokens.com](https://colortokens.com)