COLORTOKENS

CASE STUDY

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 is 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 needed a security solution to protect their business information as well as their patient data. 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, and an immediate need to resolve this.

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 when they reached out to ColorTokens.

The Challenge

The biotechnology company needed a solution that could easily fulfill the internal and external mandated regulatory and compliance requirements while protecting their patients and business. The presence of active Windows XP and Windows 2003 systems in their environment meant they were in dire need of immediate protection of their susceptible legacy systems. During their analysis, they came up with four outcomes they wanted to gain from a partnership.

Desired Outcomes:

1. Protect legacy systems that could no longer be patched by restricting connectivity from pertinent systems to other systems, thereby reducing the likeliness of exploitation
2. Reduce the attack surface across their server infrastructure by restricting the lateral movement
3. Reduction of the blast radius if in fact there was any malicious software or a bad actor in their environment
4. Ease of visibility and management for this solution

The Approach

ColorTokens produced a well-defined Proof of Concept (POC) in five working days. Our efficiency and detailed POC showed the quality and value of our product, meeting all the specified desired outcomes.

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

EXTENSIVE UNDERSTANDING: After deploying to all their exposed assets, we were able to begin capturing flow data immediately to provide a complete holistic view of communication. A complete understanding of their asset inventory and flow data gave us the ability to quickly understand the need for policy and begin writing a communication policy that enabled their business but maintained the principle of least privilege.

> “Biotechnology company 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 well structured and experienced 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. Early enablement of the teams supporting their security concerns allowed them to follow our professional services teams through initial onboarding of the product and quickly become self-sufficient.

LEGACY MAP: The company was very impressed by the legacy map we produced 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 intracity 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, reducing the need for extensive analysis of their environment and allowing them to adopt existing naming conventions.

POLICY CREATION: Using the captured flow analysis, we were able to quickly lock down existing enabled communication paths and shut down all other potential vectors, while providing an agile method to add, modify or remove assets from a defined policy group.

Results and Benefits

The leading biotechnology company has achieved immense improvement in security posture 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 were immediately installed and enforced. The drive to protect their legacy environment had the ancillary benefits of highlighting how many legacy servers they had in their estate, resulting in an upgrade program for the servers that required it. The remaining licenses were then earmarked for use on assets reaching end of support in the current year, kicking off an ongoing improvement program that permeated their whole business.

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 further security partnership. We are currently in process with a program to protect connectivity from their overseas user base using our Xaccess product, which will be managed from the same platform interface as their existing deployment. After seeing the results and metrics associated with microsegmenting their legacy environment, they are kicking off a program to deploy the same solution to their business-critical assets, beginning with Active Directory. Finally, our agentless solution is being positioned to support their assets that cannot accept an agent (Operational Technology such as manufacturing equipment and biotechnology machinery). The continued partnership and growth of our business together displays the magnitude of the trust relationship between ColorTokens and our customers, the quality of our security solutions, our ease and pace of deployment, and the lasting impact we continue to have for our customers.