COLORTOKENS

CASE STUDY

Securing Critical Data and Operations for a Leading Fusion Energy Research Company

INDUSTRY: Energy

HEADQUARTERS: Global

Overview

A global company researching clean nuclear fusion energy was in need of deploying cyber protection software in order to protect critical data and computer systems from its biggest threats – that being modern ransomware attacks and research data exfiltration. Developing the fusion power plant of tomorrow involves valuable research data, over 50 families of patent information and equipment control systems. A compromise in any of these systems would have a debilitating impact on the organization and its leadership in the field.

The Challenge

The client deployed cyber protection on over 300 endpoints and servers. Their systems gather a large quantity of data at every instance the fusion reactor powers up. Furthermore, these systems analyze the data, model simulations of fusion reactions to study varying parameters in their research labs, and control critical machinery and equipment. All of this requires significant computing power. The systems also control parameters that safeguard key operations. The loss of this control will not only disrupt operations, but also put lives at risk. Loss of IP information would have national level impact on the research projects.

The main challenges to tackle are:

- Prevention as opposed to detection of cyber threats
- Ensure business continuity
- Ultra-high security with minimal impact on computing capacity
- Realtime monitoring of any suspicious behavior

The Approach

ColorTokens worked with the nuclear fusion energy organization to understand their IT systems, end points and their mission critical systems. Xprotect, ColorTokens' cloud-delivered platform which utilizes a preventive Zero Trust framework was a perfect solution to meet the client's objective.

- ColorTokens was able to exceed traditional security methods with intelligent algorithms to analyze every running process in their endpoint systems and servers.
- The application processes are now constantly analyzed in real time in four different ways and use contextual behavioral analysis to instantly stop suspicious activity and simultaneously generate alerts. And all this with nominal impact on compute or network capacity.

> Five years of zero cyber incidents with Xprotect

- ColorTokens' Xprotect locks down endpoints and servers with process control enforcement, and quarantines suspected devices until remediation. This was a significant benefit for the client.
- Updates to threat intelligence is seamless, as is update to the XProtect application. This reduces the burden on the IT staff to maintain the security system. Central remote monitoring also reduces the load on the IT team.

Results and Benefits

The leading fusion energy company has been completely secure from cyberattacks in the five years during this engagement with ColorTokens.

BLOCKED 141 MALICIOUS PROCESSES in past 12 months. Recently, 3 zero-day malicious processes which bypass anti-virus and are used for data exfiltration, were blocked by the behavior analysis algorithms.

XPROTECT BLOCKED MALICIOUS PROCESSES that would have led to JS injections and command execution vulnerabilities.

XPROTECT BLOCKED NEARLY 20,000 PROCESSES IDENTIFIED as unallowable due to the organization's policies.

OUR THREAT INTEL WAS AUTOMATICALLY UPDATED with over 7,000 variants of IOCs in past 12 months, so our client was protected from these new malware variants.

Conclusion

For the last 5 years, Colortokens has deployed its cybersecurity software to protect critical data and computer systems from their biggest threats – modern ransomware attacks and research data exfiltration. The company has not experienced a breach during these last 5 years.