Solution brief

Labyrinth Deception Platform and beyond SSL Remote Access Solution

Zero Trust Remote Access from any device with a browser

In today's digital landscape, where remote work is becoming increasingly prevalent, the need for robust cybersecurity measures has never been more critical. Organizations must ensure that their sensitive data and systems are protected from malicious actors seeking unauthorized access. One of the key concepts that can significantly enhance security is the integration of Zero Trust Remote Access and Deception platforms.

Joint solution benefits:

- Clientless secure remote access from a browser
- Enhanced threat detection in a BYOD environment
- Detection of malicious insiders inside the corporate network
- Avoid software roll-outs and bring client support to an absolute minimum
- Highly scalable and easy to deploy infrastructure
- A unique user experience, e.g., seamless access to Windows, Linux and applications from iPads, Android tablets and smartphones

JOINT SOLUTION

beyond SSL and Labyrinth have partnered to offer organizations an enhanced cybersecurity solution to detect and defend against targeted cyberattacks, advanced threats, and malicious insiders. By combining the capabilities of both platforms, organizations can strengthen their security posture, protect their network, and gain valuable insights for effective threat detection and response.

COMPONENTS

SparkView

SparkView by beyond SSL provides a secure and straightforward method to connect untrusted devices to desktops and applications. Using Zero Trust Network Access (ZTNA) technology, SparkView allows remote access from any device with a browser, eliminating the need for client-side installations.

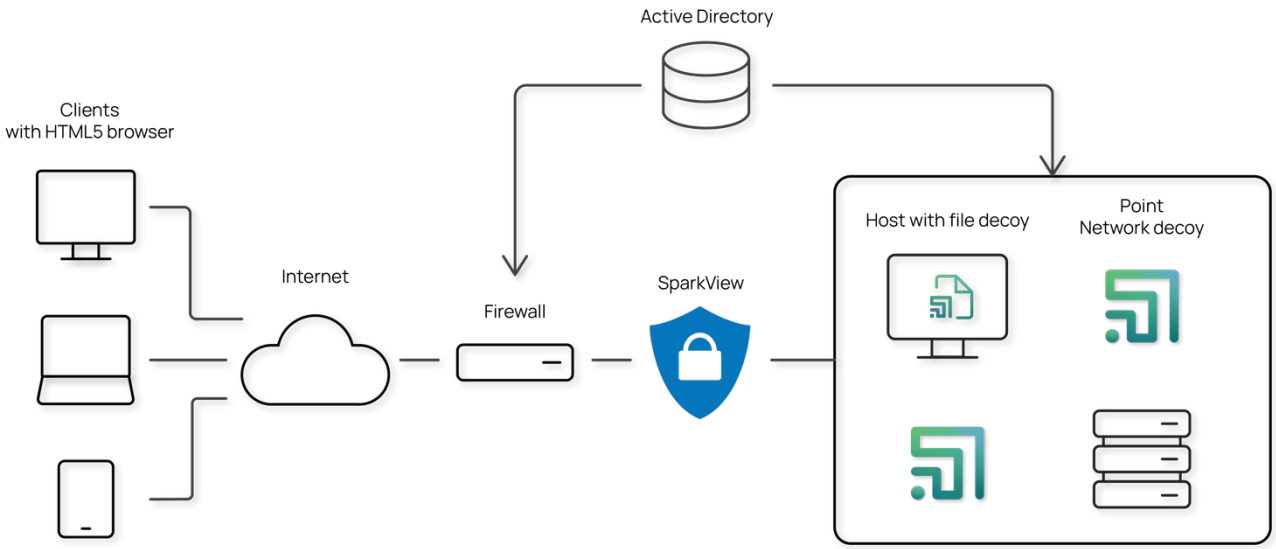
Labyrinth Deception Platform

Labyrinth is a deception-based threat detection technology designed to identify and block cyberattacks originating within a corporate network. Leveraging unique threat detection techniques, Labyrinth proactively defends against targeted attacks, advanced unknown threats, botnets, zero-day attacks, and malicious insider activities.

IMPLEMENTATION

The first step in implementing joint solution is placing the Labyrinth's network decoys, which imitate real hosts and services and may also be referred to as Points, in the corporate network alongside SparkView. The next step involves adding fake users to the Active Directory and/or local database and distributing file decoys across the real assets.

When Labyrinth detects anomalous activity on Points, it triggers a security alert with a detailed incident description handled by the security team or built into Labyrinth integrations.



USE CASES

Malicious Insider Detection

As beforehand placed network lures and fake credentials normally should remain untouched, when a malicious insider interacts with them, Labyrinth Deception Platform captures and analyzes attacker's behavior, providing real-time alerts and actionable insights for immediate response.

Enriching Security Alerts

SparkView integration with Labyrinth enriches security alerts by incorporating valuable information from SparkView sessions. This includes retrieving session data from SparkView API, allowing the Incident Response Team to enhance security alerts with usernames and real public IP addresses when attacks occur via compromised users accessing deceptive internal resources through SparkView.

BEYOND SSL
info@beyondssl.com
beyondssl.com
beyond SSL

LABYRINTH
info@labyrinth.tech
labyrinth.tech
Labyrinth Development