TELEMETRI

Use-Case

Insider Threats

In most every enterprise, many activities occur daily that could damage or destroy the organization go undetected.

Software downloads, dark web related activities, and unauthorized file sharing are among the many activities that may go undetected with traditional security tools. Even if benign – when the insider isn't *trying* to harm the organization – the consequences of these activities can be devastating, particularly in an age of Bring Your Own Device (BYOD). Simultaneously, these users traverse different Wi-Fi and cell networks throughout the day, including those that may be unsecured and unsafe. This BYOD phenomenon, coupled with the blurring of the traditional line that existed between personal life and work, makes the insider threat problem a huge issue. Insider threat consequences include:

Data loss via exfiltration	What happens in the company network does NOT stay in the company network.
Intellectual property loss/trade secret loss	One wrong click and your organization can be rendered irrelevant or in a patent fight!
Malware	Trojan horses are tempting, invisible or brought in out of sheer carelessness.
Hidden liability	For the determined employee, a lot of damage can happen quickly.
Phishing and ransomware	The list is never-ending, when an employee visits external networks; and regardless of the circumstances, bad things DO happen.

Telemetri frequently and precisely maps the Internet's infrastructure, enabling users to determine where internal traffic is routed and to distinguish between what is necessary and productive from what is dangerous.

The **Telemetri** enriched data is a simple, yet comprehensive, addition to any existing suite of security related investments utilized to detect these types of activities. **Telemetri** provides swift and accurate identification employee activities such as software download, file sharing, and TOR (Public and Hidden Bridges). Social Networking activities are authenticated and mapped to isolate critical threat vectors. Guest Networks become "**Telemetri**", identifying hidden threats.

In short, **Telemetri** uniquely enables organizations to identify the "unknown/unknown" of strange non-work hour activities. Organizations can identify when employees are (1) connecting to TOR, including the hidden bridges, (2) accessing software download sites anywhere in the world, or (3) communicating file-sharing sites in the U.S. or overseas that may include transmission of protected, proprietary data. By immediately recognizing those interactions that shouldn't occur, organizations can protect themselves, their employees, and their customers from the negative consequences of intentional or unintended insider threats.