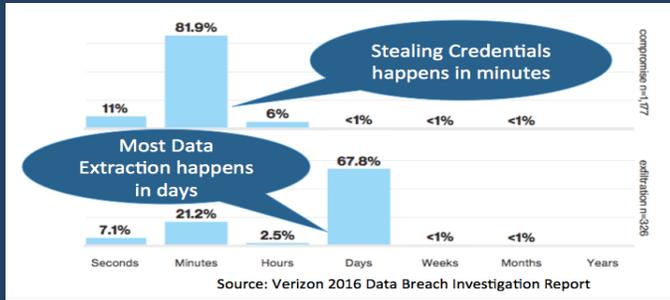**Seceon OTM, is a cyber security advanced threat management platform that visualizes, detects, and eliminates threats in real-time**. It provides a simple, comprehensive, fully automated approach to detecting and stopping the **threats that matter.**

Any solution to prevent cyber security threats must work in real time as most data breaches happen in minutes or days.

Compromised credentials and insider threats, account for more than 80% of these data breaches. Most traditional security solutions are blind to almost all forms of compromised credentials and insider threats.

Seceon OTM addresses the enterprise need for a Security Operations Center, **SOC, in a box to detect and stop threats in real time.** Seceon OTM leverages unmatched combination of behavioral analysis, machine learning and dynamic threat intelligence to detect and contain known as well as unknown cyber security threats. The solution is completely agent-less, can work in any hybrid cloud architecture, and can scale to any enterprise size.
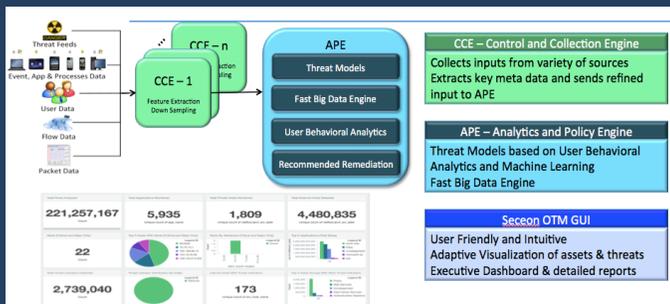

The solution works with both encrypted and unencrypted traffic. It pulls out key metadata from network flows and the logs generated by the devices, and applications running in your network, which also includes infrastructure such as Active Directories, DNS, as well as events from existing security infrastructure.

SOC in a box: Simple Setup and Automated Operation – Seceon OTM can install and be up and running within 4 hours, with minimal to no provisioning. There are no rules

to import and customize, no signatures to pull in, no complicated filters that need optimization. It just works – out of the box.

Immediate RIO - offered on a monthly fee per protected device. It allows for cost effective deployment on a pay as you go model for organizations of any size. It saves money by reducing the number of security tools required while dramatically reducing operational expenses.

Adaptive and Comprehensive Visualization - Solution builds a comprehensive view of how your users, devices, applications, and interact. The solution uses a combination of algorithms and machine learning techniques to generate behavior analytics that detect threat indictors. These threat indicators are correlated together and qualified to determine if they build up to actual threats. These threat alerts are displayed in clear concise jargon free language, that indicate the type of threat the sources and the targets. This makes it easy for untrained staff to understand at a glance as to what is happening and which actions to take to eliminate the threat.
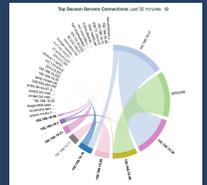
Surfacing only Threats that Matter and allows Remediation in Real-Time – Seceon OTM solution detects all forms of threats in minutes, not days and allow automated remediation within seconds. The platform provides comprehensive visualization of the threats and most importantly single line persistent alerts that are listed by criticality rather than generating thousands of threat indicators as many other products do.

Unlike traditional solutions built around static rules and signatures that are good at finding threats that have been seen before, Seceon's OTM Platform automatically surfaces all the threats within an organizations' environment, including those never seen before to deliver unparalleled visibility into internal and external threats.