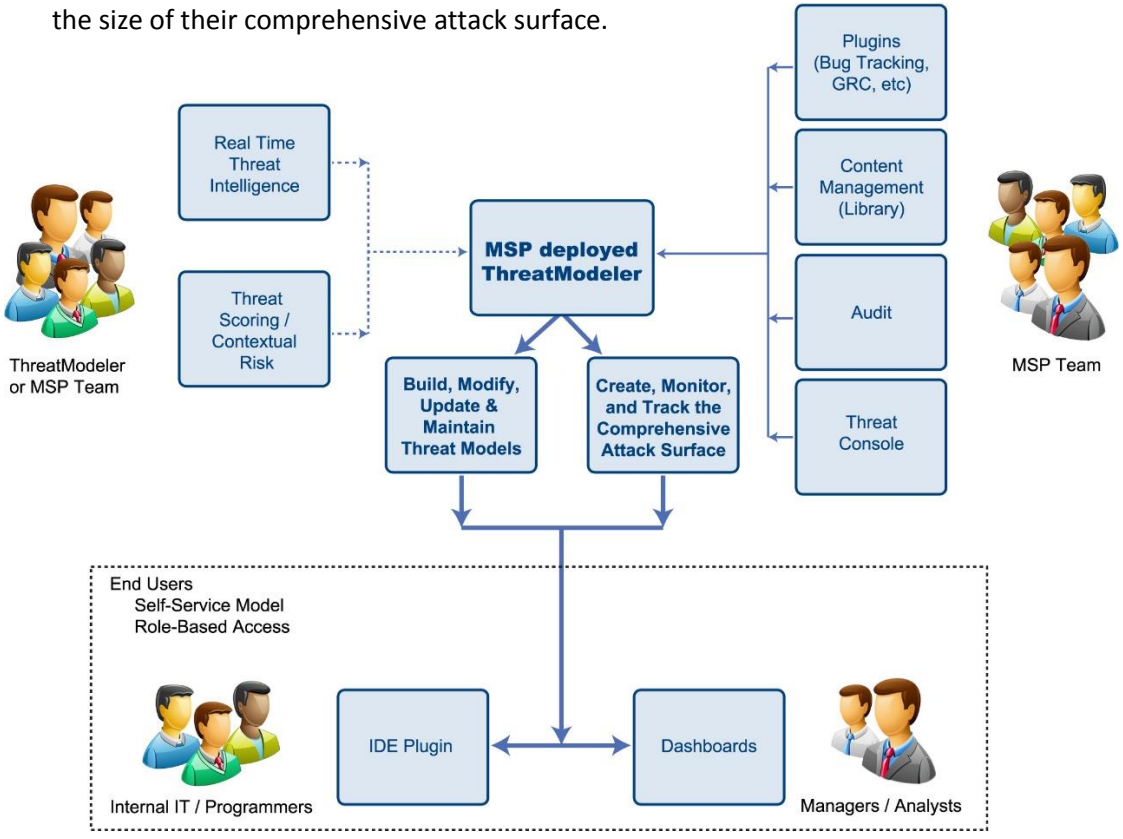
MSP End User Benefits Summary

ThreatModeler™ is the first enterprise-level threat modeling software that will enable MSPs to provide end-to-end, proactive management of their end user's comprehensive attack surface:

- **Application threat models** of end users' applications can be built in minutes based on the application architect's use case diagram or the documented business requirements;
- **Operational threat models** of end users' entire IT infrastructure – including their in-house system, cloud-based infrastructure, IoT components, Android or other mobile devices, managed services, shared components, and other 3rd party elements – can be created through chaining an unlimited number of individual threat models;
- **A repository of reusable templates** allows even non-security experts to quickly build end user threat models that will identify and contextually prioritize all the potential threats and provide the appropriate mitigating controls;
- **The comprehensive centralized threat library** is kept up to date with the latest real-world threat intelligence and appropriate mitigating controls; MSPs can update all end user threat models automatically;
- **High-level reporting and dashboards** allow MSPs to effectively communicate the end user's threat portfolio and risk profile; roll-based access allows end users self-service access to the reports and dashboards, to drill-down and understand the origin of individual threats, data exposure, and potential attacker profiles;
- **End users can collaborate with the MSP** to prioritize their risk mitigation strategy and reduce the size of their comprehensive attack surface.



ThreatModeler™

MSP End User Benefits Summary, continued

ThreatModeler™ will be installed on the MSP's secure, hardened network or over a hardened cloud-based infrastructure, or on a hybrid mix of cloud and on-site network. Regardless of the installation platform, all threat modeling data is encrypted and secured.

Software licensing include unlimited users and role-based access. Licensing fees are based on the number of threat models built rather than on the number of users or "seats." MSPs can increase their client offerings in three distinct ways:

- **End user product offering** allows MSPs to use ThreatModeler's SaaS platform to provide access to the threat modeling tool for end users who wish to create and maintain their own threat model portfolio;
- **Provide end-to-end threat modeling** as a value-add service to their end users that seek to off-load part of all of the threat modeling process to the MSP;
- **Utilize ThreatModeler's Amazon Web Services offering** to provide partial or complete threat modeling services for end users' cloud-based infrastructures.

ThreatModeler™ enables MSPs to provide a positive ROI for end users through:

- **Reducing the high cost of fixing vulnerabilities.** Case studies of Fortune 1000 companies demonstrate that testing and remediative development can require more than 225 resource hours and cost more than $17,500 per Agile sprint. Proactively mitigating potential threats costs approximately 30x less than mitigating deployed vulnerabilities.
- **Reducing the end user's risk exposure.** Static and dynamic testing do not catch all the critical and high-risk vulnerabilities. Deployed vulnerabilities create unnecessary risk and data exposure. ThreatModeler™ can identify 100% of the relevant critical and high-risk threats during the application design phase, and provide the appropriate mitigating controls to developers as they create write their initial code.
- **Proactively analyzing and discovering security vulnerabilities.** Traditional security tools can only detect attacks after malicious actors begin an attack. ThreatModeler™ allows security teams to proactively analyze applications and IT infrastructures from the attackers' perspective to find weaknesses and vulnerabilities before attackers find and exploit them. Preventing attacks before they happen reduces the risk of breaches and unauthorized activity that may go undetected by traditional security tools.
- **Allowing end users to focus their budgets and resources** on their prioritized strategic initiatives, while the MSP provides end-to-end proactive cyber security.