Device Security Maturity Model

	Level 1: Initial	Level 2: Repeatable	Level 3: Defined	Level 4: Managed	Level 5: Optimizing
Culture	**Vision**: Uncommunicated Device & Security Vision **Device Risk Identification**: Little to none **Communication**: Restricted **Innovation:** Sub-Innovating	**Vision**: Clear Device & Security Requirements **Device Risk Identification**: Immature Processes **Communication**: Rapid Intra-Team **Innovation:** by Necessity	**Vision**: Articulated Device & Security Business Goals **Device Risk Identification**: Process Defined & Known **Communication**: Rapid Inter-Team **Innovation:** by Design	**Vision**: Articulated Device and Security Business Vision **Device Risk Identification**: Clear & Proactive. Periodic Monitoring **Communication**: Frequent, Collaborative **Innovation:** Strategic	**Vision**: Articulated Device & Security Business Strategy **Device Risk Identification**: Continuous Monitoring **Communication**: Rapid Feedback **Innovation:** Ownership Mindset
Process	**Incident Recovery:** Reactive or Non-existent Processes **Management:** Inconsistent and Project **Product Rollout:** Ad Hoc for Development and Testing **Reporting:** Ad Hoc & Inconsistent	**Incident Recovery:** Resiliency and Recovery Capabilities Applied Consistently **Management:** Project & Requirements Based **Product Rollout:** Scheduled Testing and Deliveries **Reporting:** Tactical	**Incident Recovery: BC**/DR Plan Defines Steps to Continue Critical Function and Recover to Normal **Management:** Integrated Projects **Product Rollout:** Automated Deliveries and Testing **Reporting:** Consolidated	**Incident Recovery:** Complex Orchestrations **Management:** Quantitative Projects **Product Rollout:** Frequent Deliveries and Qualitative Testing **Reporting:** Strategic	**Incident Recovery:** Distributed Orchestrations **Management:** Organized and Performance Based **Product Rollout:** Continuous Deliveries and Testing **Reporting:** Predictive
People	**Incident Response Training:** Reactive or Non-existent process **Security Updates:** Forced on Constituents **Organization:** Ticket-centric, Skills-based Teams with Tribal Knowledge	**Incident Response Training:** Consistent Roles for Working **Security Updates:** Deadline Based **Organization:** Deliveries-based, In-Level Security Skills with Written Knowledge	**Incident Response Training:** Plan for Incident Preparation, Analysis, Containment, Eradication Orchestration Exists **Security Updates:** Collaboration based **Organization**: Projects-based with In-Level Skills, Automation	**Incident Response Training:** Response Times and Impacts Monitored and Minimized **Security Updates:** Community Based and Led **Organization**: Products-centric, In-Level Skills and Knowledge	**Incident Response Training:** Proactive, Regular Testing and Updating of Personnel, Procedures, and Tech **Security Updates**: Community Organized and Recommended **Organization**: KPI-goaled, Interdisciplinary Teams, Continuous Education
Technology	**Device Protection:** Minimal and Ad Hoc **Monitoring / Alerting**: Minimal with No Automation **Anomaly Detection:** Minimal or Non existent	**Device Protection:** Reactive and Ad Hoc **Monitoring / Alerting**: Core level - Build Automation **Anomaly Detection:** Functional Tooling	**Device Protection:** Formally Protected by Classifications **Monitoring / Alerting**: Integrated and Actionable **Anomaly Detection:** Continuous	**Device Protection:** All Environments Proactively Monitored via Protective Technologies **Monitoring / Alerting**: Self-healing **Anomaly Detection:** Continuous, Real-time Automation	**Device Protection:** Standards Operationalized and Automated Using Advanced Technologies **Monitoring / Alerting**: Self-learning, Self-managing **Anomaly Detection:** Automation Against Baselined Behavior
Standards	**Architecture**: Ad Hoc **Standards**: None in Place **Compliance**: Non Existent **Audit**: Third-party Imposed	**Architecture**: Stack Based **Standards**: Ad Hoc **Compliance**: Reactive Adherence **Audit**: Ad Hoc	**Architecture**: ZTNA and SASE Aspirations **Standards**: Reactive Adherence **Compliance**: Requirements Met **Audit**: Reactive Adherence	**Architecture**: ZTNA and SASE Vision in Progress **Standards**: NIST / CIS Aspirations **Compliance**: Requirements Baselined **Audit**: Frequent, Collaborative	**Architecture**: ZTNA and SASE Baselined and Measured **Standards**: NIST / CIS Baselined **Compliance**: Continuous Measurement and Testing **Audit**: Continuous and Organized

WootCloud HYPERCONTEXT