

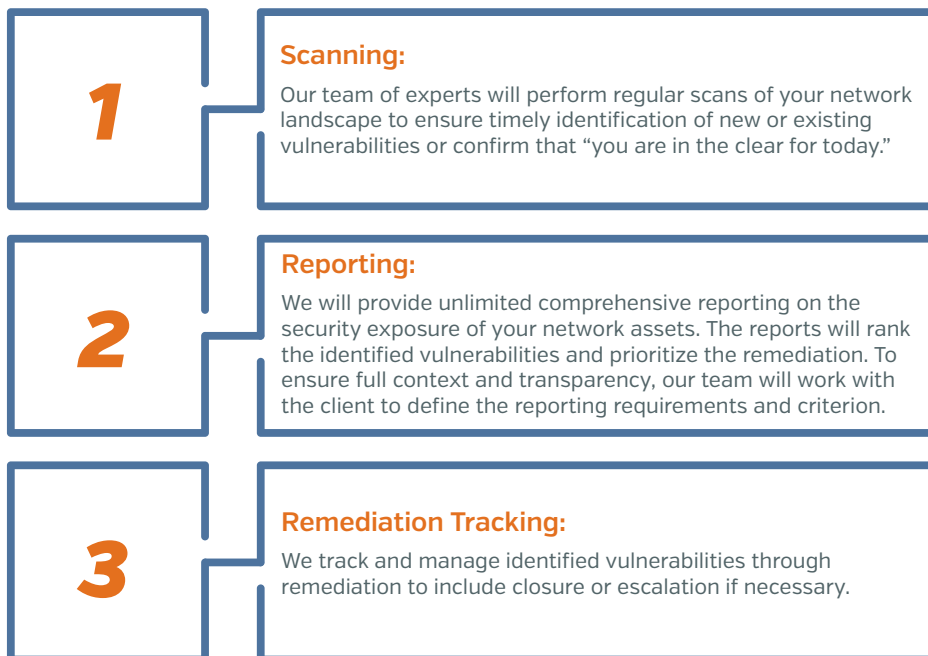
For almost every business cybersecurity and rapidly evolving threats from organized crime and foreign actors are a pervasive concern. Not only are cyber threats evolving, they are also increasing in volume and level of sophistication. The current threat vectors and landscape have changed and are significantly different from the past. Now, hundreds of thousands of new vulnerabilities are reported yearly, increasing the complexity of managing IT security and risk for an enterprise. Verizon's 2018 Data Breach Investigation Report shows 53,308 security incidents and 2,216 data breaches. These numbers are just those that are reported.

Improving the IT security and risk management posture for the enterprise is a top priority for the c-suite. A data breach, an unauthorized access to data, modification of data, or a data loss compromises the enterprise's confidentiality, integrity and availability which translates into RISK – reputational, market, regulatory and financial.

VULNERABILITY MANAGEMENT AS A SERVICE

Genesis10 provides comprehensive services from Vulnerability Identification to Vulnerability Remediation onsite or onshore at one of six Genesis10 operated Delivery Centers.

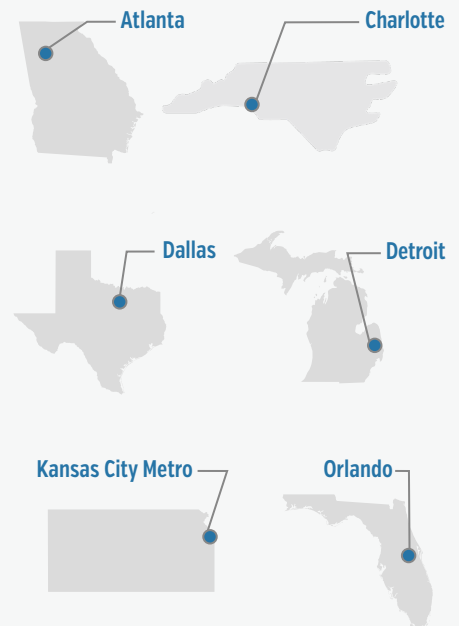
Vulnerability Identification



6 GENESIS10 OPERATED DELIVERY CENTERS



Our delivery centers operate as an extension of your delivery teams focused on your goals. Genesis10 effectively taps into markets across the U.S. to increase access to talent for our clients in a cost-effective, flexible delivery model.



Vulnerability Remediation

1

Patch Scheduling:

We take the guess work out of scheduling the vulnerability remediation to include communication and coordination with all relevant stakeholders and support the client-specific change control process. We manage the patching schedule and provide near real time visibility via reports and dashboards on patching efforts.

2

Patch Implementation Automation:

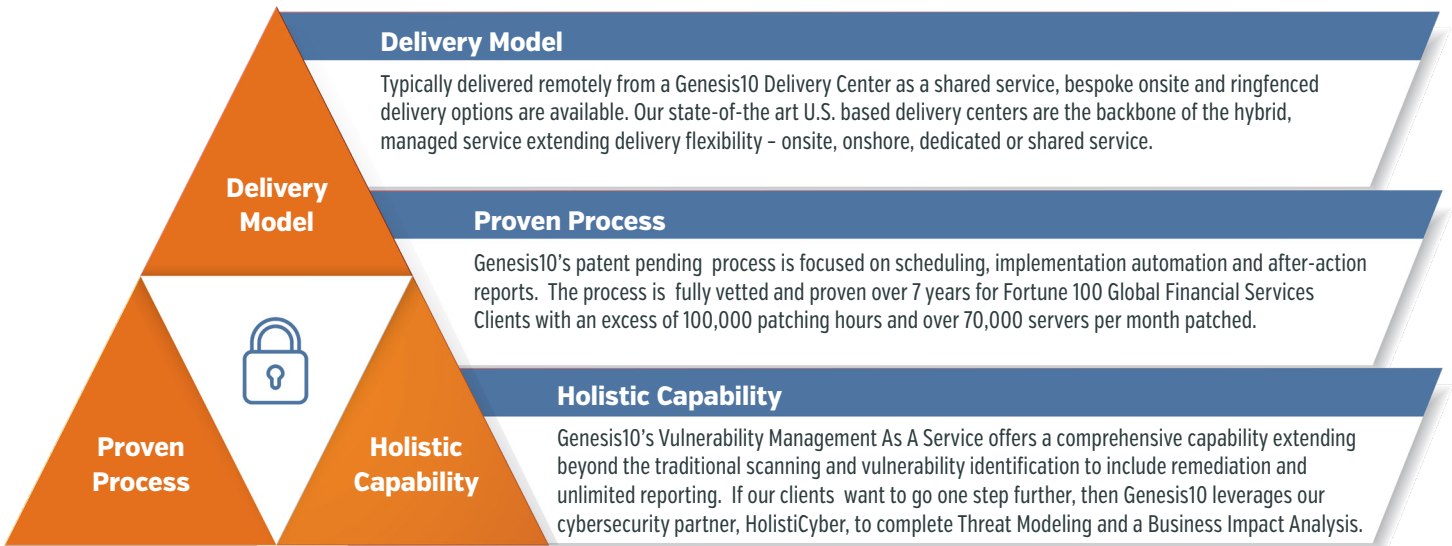
Our approach is to leverage the client's existing tools or, alternatively, Genesis10 can suggest industry standard patch implementation software and tools such as SSCM, Ivanti, Ansible, BladeLogic, Chef. The Genesis10 team will write the automation scripts to accurately address the right systems with the right patch and implement a structured, repeatable process.

3

Post-Patch Support:

We offer Day 1 support after patching to ensure full operational stability as well as track and fix any patch failures or incidents caused directly by the patching effort.

What Sets Us Apart



MEET TRUSTED ADVISOR SOAHAM JOSHI



As SVP of Digital Technology, Soaham Joshi brings more than 20 years of IT management and delivery experience in Enterprise IT Security and Risk, Infrastructure Operations, System Currency and Software Development. For our clients, he is focused on designing technical solutions and providing technical advisory services to drive cost out and improve operational efficiencies by identifying solutions that reduce risk and improve the operational construct, stability and resiliency. Soaham provides project delivery oversight and leads Genesis10's Vulnerability Management service and maintains a pulse on emerging technologies to provide guidance on the latest technology trends, technology stack and migration strategies.

CONTACT SOAHAM: sjoshi@genesis10.com | 312.254.6026