genesis10
Accelerate Innovation with Talent

CYBERSECURITY

PATCH MANAGEMENT PREVENTS CYBERATTACKS

For almost every business, cybersecurity and the constantly evolving threats from organized crime and foreign governments are a pervasive concern. **Cybersecurity Ventures projects that cybercrime will cost companies approximately $6 trillion annually worldwide by 2021, up from $3 trillion in 2015.** Insurance giant Lloyd's of London estimates that these attacks cost businesses $400 billion a year (including both direct damage and disruption to normal operations).

70% of successful cyberattacks exploit known vulnerabilities with available patches.

Patch Management Prevents Cyberattacks

Cybersecurity is a major vulnerability for most companies. The clear majority of cyberattacks take advantage of known software and hardware vulnerabilities.

Seventy percent of successful cyberattacks exploit known vulnerabilities. By implementing an effective patch management process, companies can prevent most cyberattacks and dramatically lower their reputational and operational risk.

What is a Patch?

A patch is a software update comprised of code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package, and include vendor application, network, and operating system updates.

Focused and Dedicated

Organizations with large complex server environments require highly focused and dedicated teams to plan, manage, deploy and monitor the application of patches. Since patch management often needs to be conducted during off-hours, scheduling of full-time employees can be inconvenient, burdensome, and divert them from their day-to-day priorities.

Genesis10's Patch Management capabilities provide dedicated teams and expertise to apply patches according to our clients' priorities resulting in:

SECURE SOLUTIONS. Onsite resources work in your facility, and remote resources work in a highly secure, controlled, and independently audited SSAE-16 certified U.S. based delivery center.

RISK REDUCTION. Companies are able to manage and mitigate threats and vulnerabilities with an effective patch management solution. This dramatically reduces the probability of a successful cyberattack, and the associated reputational, monetary, and system impacts.

PROACTIVE MANAGEMENT. Clients are able to proactively manage patching resources, and adjust both patching priorities and schedules dynamically.

INCREASED EFFECTIVENESS. Your staff is enabled to concentrate on high-priority tasks and projects knowing that systems are compliant with your patch policies.

COST SAVINGS. More cost effective than fixed-bid outsourcing.

Genesis10 provides Patch Management in a flexible engagement model that enables organizations to effectively adjust and align resources against business imperatives. Our onsite and onshore models enable delivery scalability capabilities, infusing contingent labor and freeing up critical-path capabilities while optimizing the cost of labor and managing delivery risk. Genesis10 is committed to helping our clients' achieve their operational goals.

Our consultants operate as an extension of our client's team which seamlessly positions them to enhance their patching capabilities. Genesis10's model provides our clients with speed-to-market, skilled resources and breadth of talent capabilities through leveraging our Delivery Center network model and diversifying access to talent.

Engagement Process

1. **Understand** our clients' patch management objectives.
2. **Tailor** a patch management solution to your needs.
3. **Deploy** onsite or onshore teams.
4. **Optimize** the patch management solution through measurement and progress reporting.
5. **Customized Reporting.** For each engagement, we partner with clients on customized reports to meet your unique compliance and vulnerability documentation needs.

Case Study: *Score Goes from Red to Green*

Client Situation

A multinational banking and financial services corporation faced significant regulatory findings regarding server patching.

Realizing that most cyberattacks take advantage of known hardware and software vulnerabilities, the client needed a regular server patching cadence.

Utilizing internal teams for patching was perceived as detrimental to competitive advantage.

Regulatory risk reduction with a tailored approach

Considerations

- Acquisitions created a variety of platforms and servers with inconsistent operating systems
- Access to production servers to apply patches was difficult. Off hours scheduling was required
- Internal personnel responsible for routine maintenance had higher priority issues
- The client utilized an offshore vendor to provide infrastructure support

Solution

Genesis10 built a dedicated team, housed in our Dallas Delivery Center that provided a consistent and repeatable process for maintaining software applications and operating systems with regular patches to fix security vulnerabilities and mitigate risk.

Team works in a 24x7 cadence across all technology stacks to identify, remediate, and maintain the health of the client's large server population. Patch schedules are developed weekly by the Genesis10 team, based upon customer priorities and inputs. The work is largely performed during non-business hours (nights & weekends).

Outcomes

As a result of dramatically lowered compliance risk and operational improvements delivered, the client's regulatory risk scorecard improved from red to green status.

Genesis10 team applies patches to tens of thousands of client servers in the U.S. and India. Primary operating systems are Microsoft, Unix and Linux. Multiple areas within the organization have adopted our solution, realizing similar benefits.