ivanti

SOLUTION BRIEF

Helping Protect Agencies from Denial of Service Cyberattacks

Public Sector agencies from Federal to local levels are facing distributed denial of service (DDoS) cyberattacks more regularly. You must protect your agency and constituents from these threats to keep services and communication flowing.

Avoid Disruptions to Agency Services

A distributed denial-of-service (DDoS) cyberattack floods a website or other online service with more traffic than the hosting platform can handle. Typically, hacked computers become agents or “bots” that carry out the attack, enlisting other unprotected endpoints to become bots themselves, and they all attack the same target—be it a website, server, or network. Cybercriminals use this type of attack to slow or completely crash access to a site, making it nearly impossible for the online venue’s intended audience to access its services. This kind of attack can start from vulnerabilities in a device you didn’t even know you had, or from an employee launching an unauthorized app they didn’t know was malicious.

For government agencies, the impact of a DDoS attack ranges from disruptive to devastating. Bringing down an online public service system could delay fiscal and economic support, impede utility services, or even disrupt emergency and public safety response or other constituent services. No matter the degree of risk, agencies must protect against these kinds of cyberattacks to maximize their security posture and public safety.

Patching Strengthens Agency Defenses

Recent attacks have hit government entities and contractors at federal and local levels. Among the first steps toward protecting your agency and constituents is to assess risk from potential vulnerabilities and develop plans to mitigate. Having clear visibility into all devices and software used in your environment is foundational. Performing an audit to ensure software patches are up to date is a great place to start, and should cover your entire estate—from the data center to the endpoint devices and third-party applications. Safeguarding endpoints reduces the risk that they could succumb to a DDoS attack and be turned into bots used against your agency. Patching third-party applications prevents these apps from being the point of entry for malicious actors, whether they reside on the endpoint or in the data center.

Making sure patches are up to date in the data center stabilizes the core of your systems. Many DDoS attacks target a known vulnerability in a server architecture, or a specific application installed on networked servers. Applying the latest patches eliminates these vulnerabilities, fortifying your agency’s defenses against these kinds of cyberattacks.

Turn Discovery into Action

Your agency’s security and IT operations teams need visibility into all the servers and endpoints across your environment so they can see what’s protected and which systems require action. With Ivanti, systems administrators can discover and inventory devices, verify they are properly configured, and that they’re running the latest agency-approved versions of applications and operating systems. This applies to both authorized and unauthorized software. Analysts can also gain insights on inventoried hardware—ranging from device type to operational status, and take control of the device when necessary.

IT teams can also patch physical and virtual servers, in addition to third-party applications such as Adobe, Java, and browsers. With agentless patching, you can address vulnerabilities on connected endpoints and servers while minimizing the bandwidth required by both staff and the network. With Ivanti, systems administrators also gain the control to enforce your agency's security policies and prevent unauthorized executables from launching unknown apps that could contain malware and other threats.

Agency Security through Innovation

Choosing Ivanti means you're partnering with a leader in innovation. In fact, Ivanti was awarded *Cyber Defense Magazine's* InfoSec Award for "Most Innovative: Patch and Configuration Management" at the RSA Conference 2020.

"Ivanti embodies three major features the judges look for to become winners: understanding tomorrow's threats, today; providing a cost-effective solution; and innovating in unexpected ways that can help stop the next breach."

— Gary S. Milliefsky
Publisher, Cyber Defense Magazine

Ivanti Helps Protect Against DDoS

- Discover and inventory hardware and software assets
- Patch across operating systems and third-party apps
- Patch virtual servers and apps
- Device and application control
- Enforce whitelisting and privilege management
- Agentless deployment of patches
- Create unified reports for real-time insights

Protect your agency, employees, and the public you serve. Make sure the systems you depend on are secure, available, and accessible. Ask Ivanti to show you how.

Learn More

ivanti.com
☎ **1 800 982 2130**
✉ **sales@ivanti.com**

IVI-2391 03/20 RD/BB/DH