YOUR PATH TO COMBAT

CYBERSECURITY THREATS

CHALLENGES IN CYBERSECURITY

Government has entered a new era of cybersecurity threats.

1,121%
increase in federal agency security incidents from 2006 to 2014.

50,315
reported public sector security incidents in 2015.

Attackers are highly successful, attacks are application focused and governments are subject to new, unknown attack methods.

71%
of organizations in the public and private sector were affected by a successful cyberattack in 2014.

86%
of attacks are application specific.

24
zero-day vulnerability attacks discovered in 2014 - an all-time high.

Security breaches lead to data loss, negative publicity and the financial costs are record breaking.

$6,500,000
is the average total cost of a data breach.

11%
increase in total cost of data breach.

Using Citrix solutions, government agencies can transform their IT infrastructures into solutions that are simple, secure, and cost-effective.

CITRIX NETSCALER

An enterprise class application delivery controller that combats cybersecurity threats.

Network Security
Establish a self-defending perimeter defense.

Connection Security
Decrypt and inspect Secure Sockets Layer used to encrypt links between a web server and browser.

End-point Security
Permit or deny access by evaluating client security posture.

Application Security
Protect the application from logic attacks and data loss by controlling input and output.

Threat Intelligence
Utilize evidence-based knowledge to combat cyberthreats.

Cloud, Identity & Remote Access
Add two factor authentication and use Security Assertion Markup Language to ensure secure exchanges between inside identities to outside identities.

OVERCOMING CYBERSECURITY THREATS

Government agencies can tackle the challenges of the new era of cybersecurity threats through secure and cost-effective solutions like NetScaler.

1. Reduce costly downtime and negative press by mitigating distributed denial of service attacks.
2. Stop malicious attacks by removing direct application layer access.
3. Prevent vulnerable or unauthorized devices from accessing data center resources.
4. Prevent unauthorized user access and secure cloud authentication.
5. Ensure privacy and eliminate web application data loss.
6. Block high-risk intellectual property threats using reputation based protection.
7. Block known application threats using signature based protection.
8. Permit only the correct application behavior and deliver zero day attack prevention.
9. Enhance security decision-making priorities.
10. Ensure compliance with government regulations.

For more information, visit citrix.com/government or email us at citrixpublicsector@citrix.com

CITRIX® | govloop

Sources
GAO | Data Breach Investigations Report | 2015 Cyberthreat Defense Report | Ponemon State of Application Security Report
Symantec Internet Security Threat Report | Ponemon Institute 2015