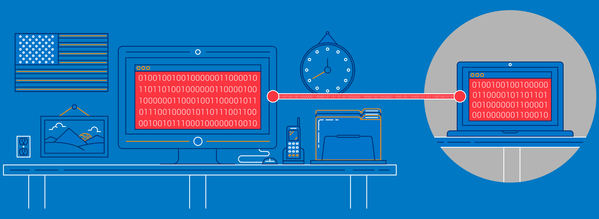
HOW HIDDEN ENCRYPTED THREATS IMPACT FEDERAL ORGANIZATIONS TODAY



Federal organizations are a frequent target of cyber-attacks — from antagonistic nation states and hacktivists to criminal organizations looking to steal sensitive data for personal gain. As the Internet moves toward 100 percent encryption to protect sensitive data, new threat vectors continue to emerge as attackers hide their activities behind SSL with increasing frequency. What dangers are pushing past your security infrastructure?

Discover the challenges you and your peers now face — including threats hiding in SSL traffic.

ARE FEDERAL ORGANIZATIONS EXPOSED TO CYBER THREATS?

55%
of federal organizations say that **less than half** of their Web traffic is inspected for attacks

77%
of federal organizations say they have definitely or likely been victim to a **cyber attack** or malicious insider activity in the past year

60%
of federal organizations agree or strongly agree that their infrastructure's inability to inspect encrypted traffic is a **barrier to compliance** now and in the future

Of those,

57%
either **didn't attempt encryption** to evade the attack—or aren't even sure if they did

ENCRYPTION IS INCREASING, BUT FEDERAL ORGANIZATIONS NEED DECRYPTION

Nearly **60%**
of federal organizations think network attackers will **increase encryption use** in the next year

Nearly **67%**
of federal organizations are concerned or very concerned that encrypted communications will leave their network **vulnerable to hidden threats** in SSL traffic

54%
of federal organizations don't currently decrypt Web traffic to **detect intrusions**

Only **50%** think they'll implement this in the next year

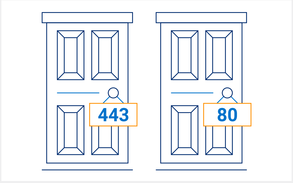
74%
of federal organizations agree or strongly agree that SSL traffic that is malicious could cause a **costly data breach**

But only **16%** strongly agree that their company is equipped to detect malicious SSL traffic

Despite all this, **29%**
of federal organizations say SSL is essential to their agency's overall **security infrastructure**

FEDERAL ORGANIZATIONS EXPECT ENCRYPTED THREATS BUT THEY AREN'T PREPARED*

Attackers use encryption to hide data exfiltration over standard ports, like 443 or 80



65% say this is extremely likely to happen

15% say they are properly equipped to resolve it

Attackers use SSL to make phishing sites look more legitimate and hide malware from IPS

58% say this is extremely likely to happen

9% say they are properly equipped to resolve it

*In this case, "extremely likely" and "properly equipped" are each defined by respondent ratings of 9-10 on a scale of up to 10.

TOP REASONS SSL HASN'T BEEN BROADLY IMPLEMENTED BY FEDERAL ORGANIZATIONS

57%
Lack of right tools

42%
Lack of resources

39%
Lack of performance

SSL DECRYPTION TOOLS: MUST-HAVES

89%
of federal organizations agree that **scaling** to meet current and future SSL performance demands is important, very important or essential

82%
of federal organizations agree that **maximizing** uptime, performance requirements and security infrastructure capacity is important, very important or essential

81%
of federal organizations agree that satisfying **compliance requirements** is important, very important or essential

Nearly **50%**
of federal organizations say their agency's security solutions are **collapsing** under growing SSL bandwidth demands and SSL key lengths

Learn how A10 Thunder SSLi delivers high-performance and cost-effective visibility into encrypted traffic, empowering your entire security infrastructure to defend your network against hidden threats.

Visit a10networks.com/ssli

Source:
Survey on Hidden Threats in Encrypted Traffic: Industry Verticals, Presented by Dr. Larry Ponemon. Ponemon Institute. March 27, 2016.

Part Number: A10-GR-70297-EN-01 July 2016