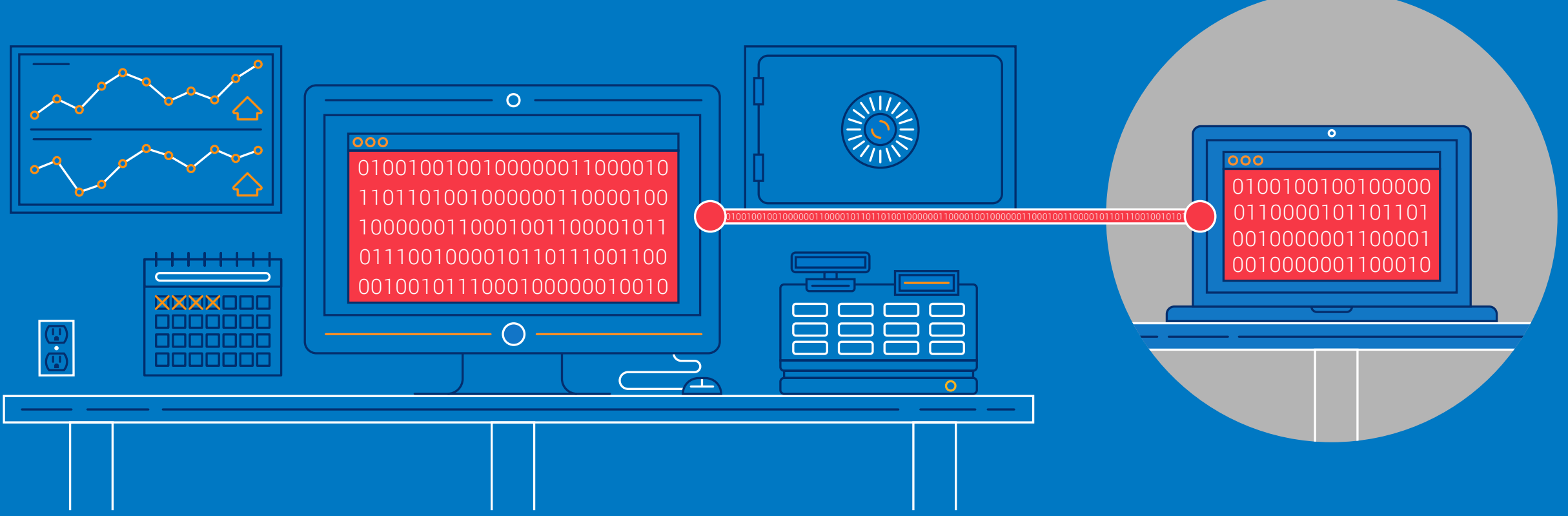


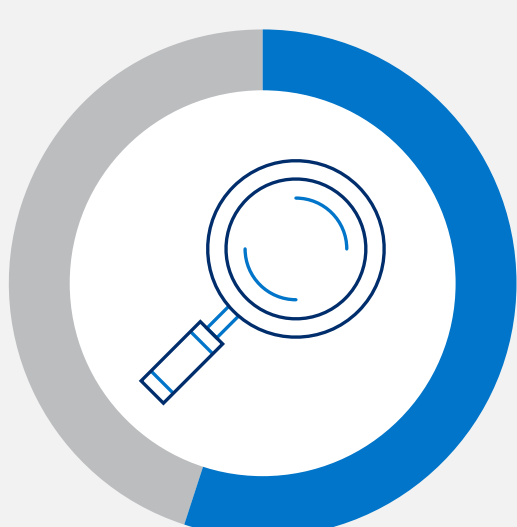
HOW HIDDEN ENCRYPTED THREATS IMPACT FINANCIAL ORGANIZATIONS TODAY



Financial organizations are being increasingly targeted by cyber criminals seeking to steal customers' personally identifiable information (PII) and other confidential data. 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 FINANCIAL ORGANIZATIONS EXPOSED TO CYBER THREATS?



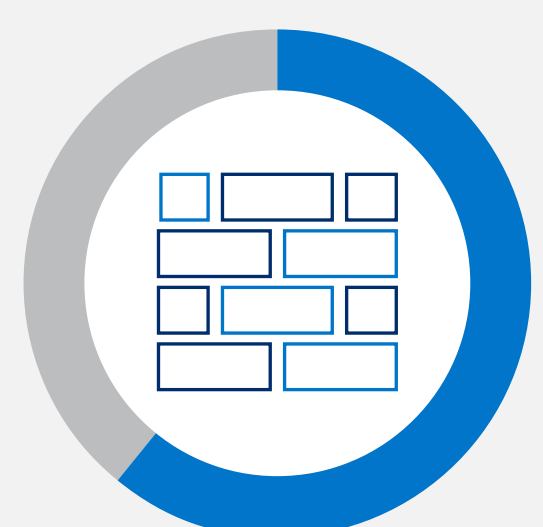
55%

of financial organizations say that **less than half** of their Web traffic is inspected for attacks



81%

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



61%

of financial 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,

60%

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

ENCRYPTION IS INCREASING, BUT FINANCIAL ORGANIZATIONS NEED DECRYPTION



Nearly

60%

of financial organizations think network attackers will **increase encryption use** in the next year



Nearly

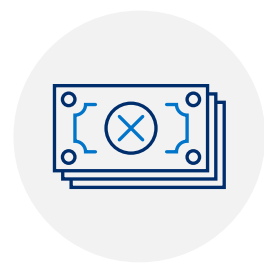
70%

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



51%

of financial organizations don't currently decrypt web traffic to **detect intrusions**



71%

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

Only

57%

think they'll implement this in the next year

But only

14%

strongly agree that their company is equipped to detect malicious SSL traffic



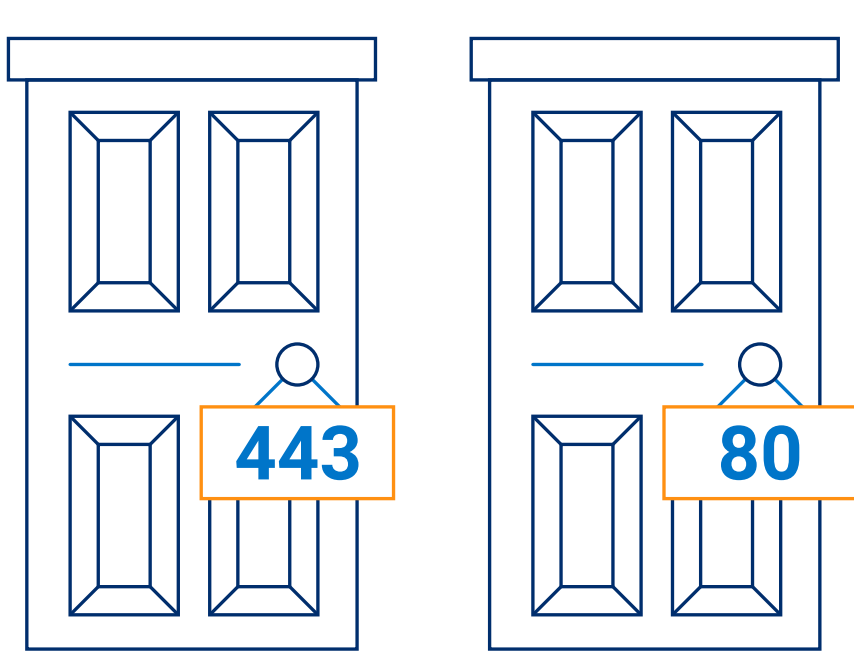
Despite all this,

27%

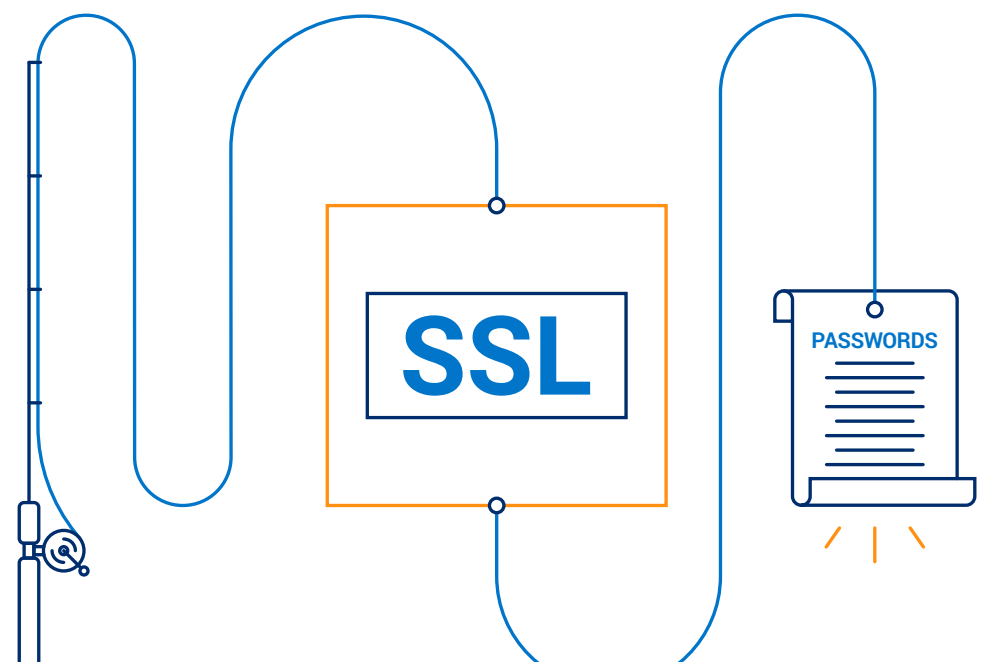
of financial organizations say SSL is essential to their agency's overall **security infrastructure**

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

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



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



62%

say this is extremely likely to happen

15%

say they are properly equipped to resolve it

60%

say this is extremely likely to happen

6%

say they are properly equipped to resolve it

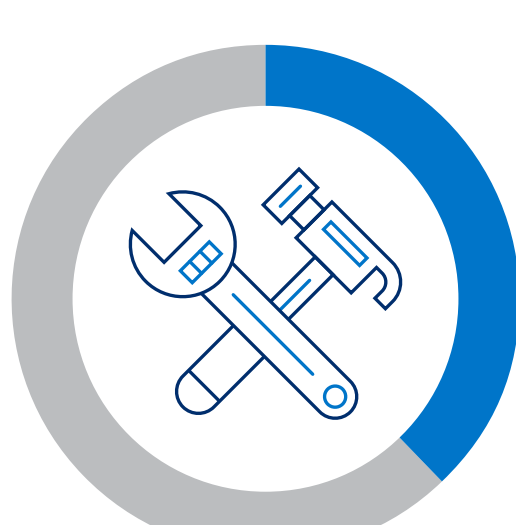
*In this case, "extremely likely" and "extremely equipped" are each defined by respondent ratings of 9-10 on a scale of up to 10.

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



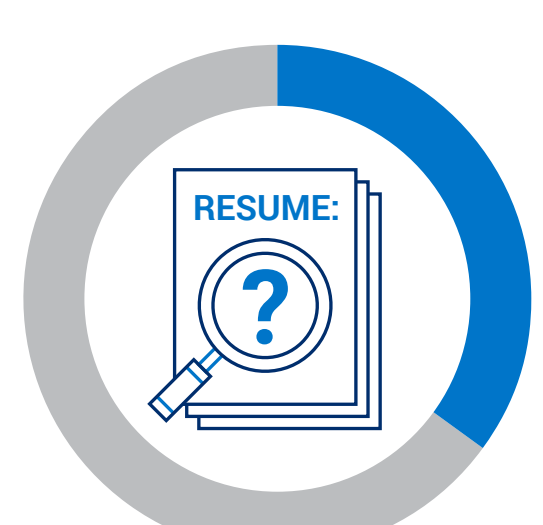
62%

Lack of performance



38%

Lack of right tools



35%

Lack of in-house expertise

SSL DECRYPTION TOOLS: MUST-HAVES



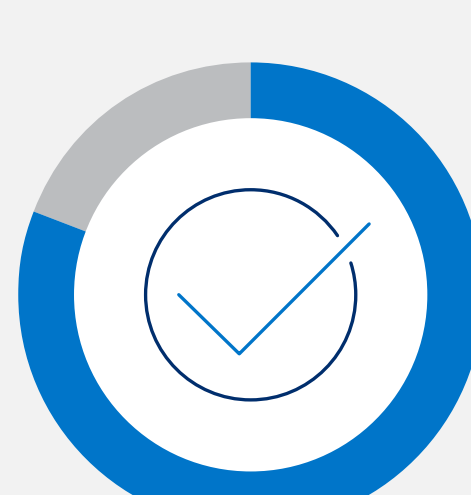
87%

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



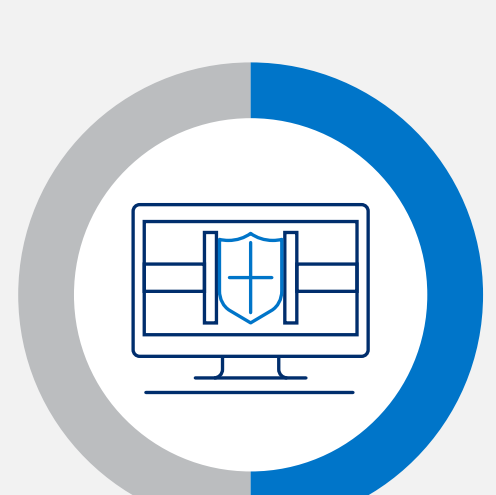
84%

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



81%

of financial organizations agree that satisfying **compliance requirements** is important, very important or essential



50%

of financial 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.

©2016 A10 Networks, Inc. All rights reserved. The A10 Logo, and A10 Networks are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners.

Part Number: A10-GR-70298-EN-01 July 2016

