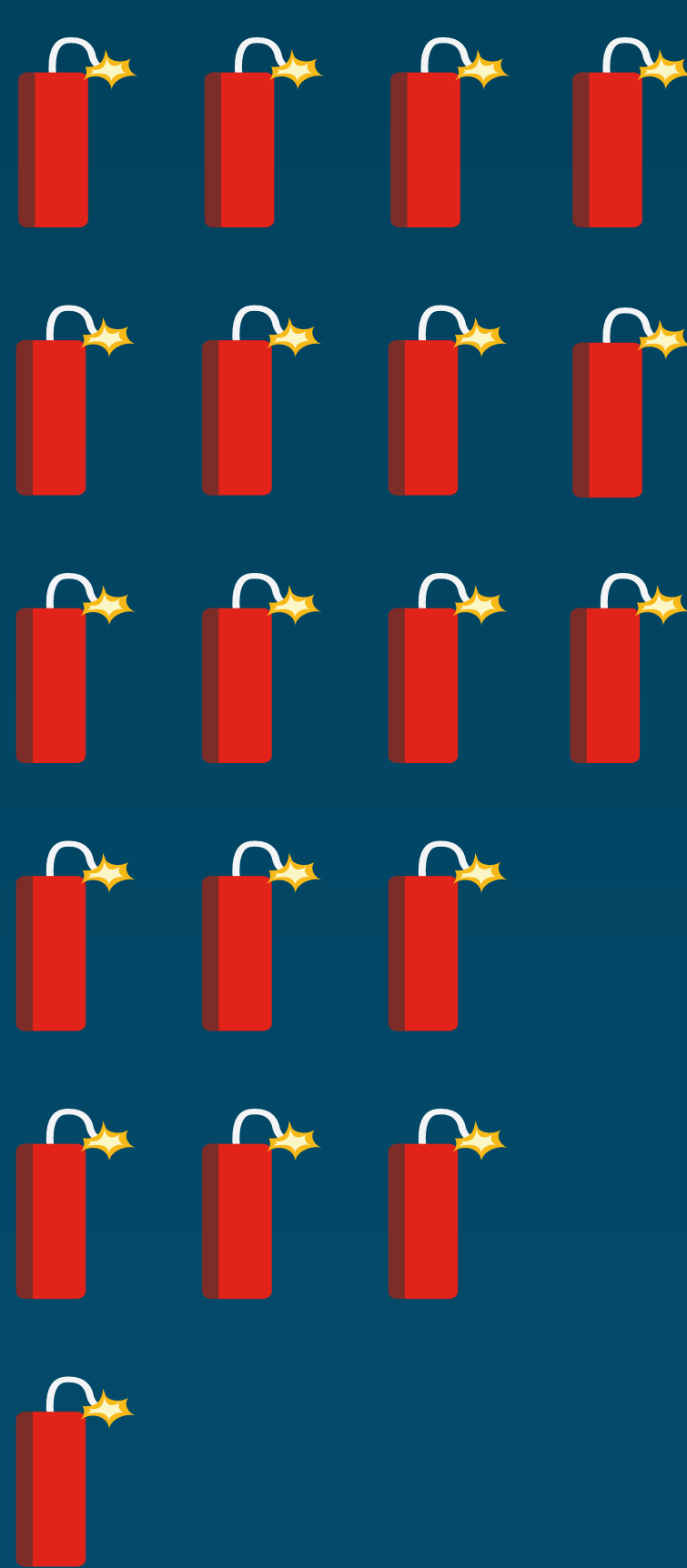


# Miners in the Shadows: Extracting Treasure with Stolen Resources



## What is Malicious Cryptomining?

Threat actors hijack an organization's computing power to create cryptocurrencies like Bitcoin and Monero. Your resources become their profits.



Cryptomining is booming.

**19X** increase in cryptomining-related traffic in the last 9 months of 2018<sup>1</sup>

## What's the cost?



Degraded performance



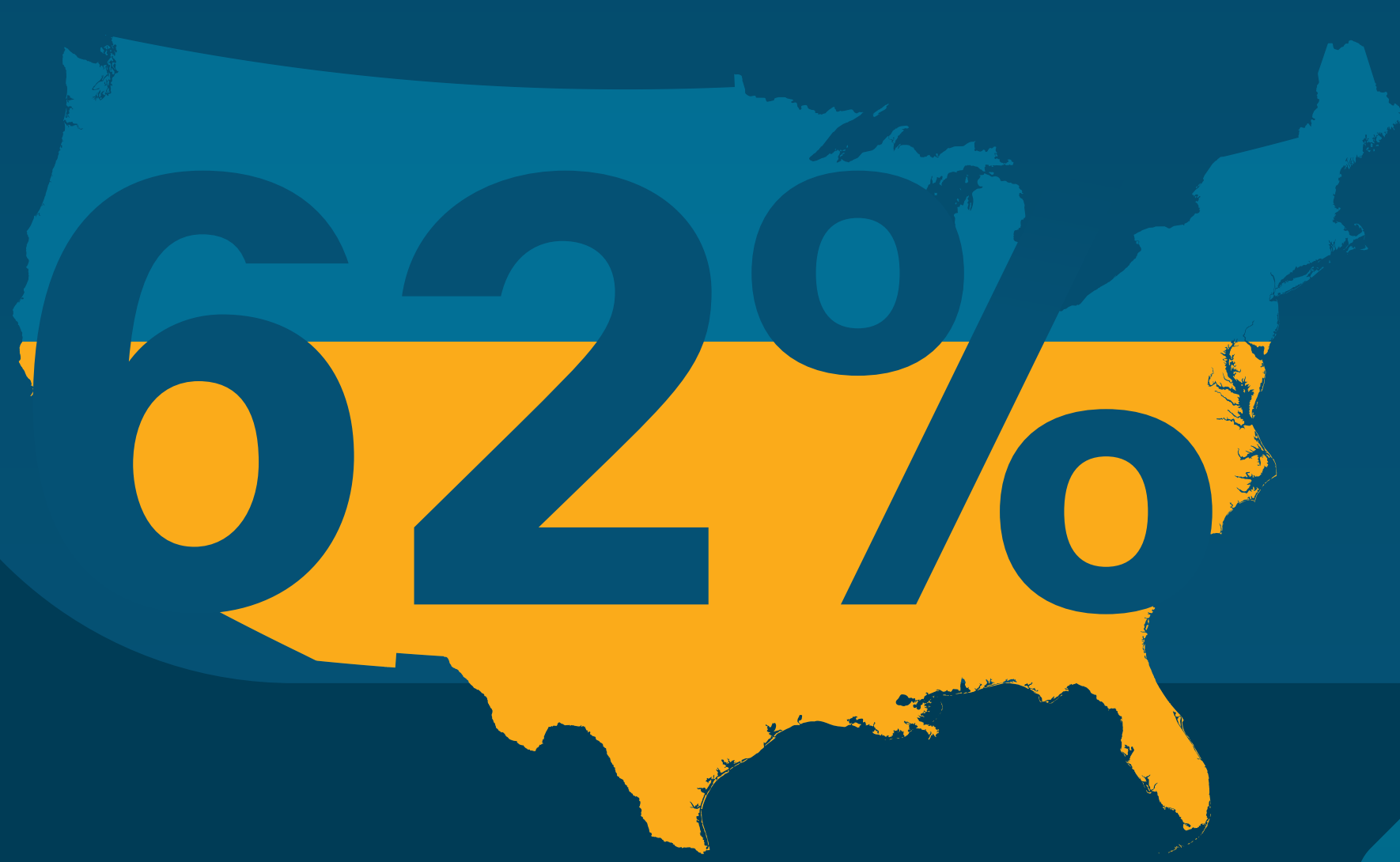
Securities regulation implications



Systems attacks



Soaring electricity usage



North America is a rich vein.

62% of total cryptomining traffic is seen in the U.S.

Small to mid-size businesses? **Biggest risk.**

**>80%** of cryptomining traffic happens in organizations with **<10,000** employees

## Is your business a potential gold mine?

No industry is safe from malicious cryptomining, but energy and utilities, and college education are hardest hit.



- 34%** Energy & Utilities
- 22%** College Education
- 8%** Other
- 7%** Healthcare
- 6%** Media
- 4%** K-12 Education
- 4%** State & Local Government
- 3%** MSPs
- Remaining 12%** Manufacturing, Financial Services, Technology, Retail, Education (Other), Hospitality, Not For Profit, Distributor/Wholesaler, Real Estate

## Your first line of defense against malicious cryptomining.

Cisco Umbrella automatically uncovers current and emerging threats by analyzing and learning from internet activity patterns.



## The Umbrella Advantage

**175B**  
DNS requests resolved daily

**30**  
data centers around the world

**90M**  
users

**160**  
countries

Detect, block, and protect against unwanted cryptomining with Cisco Umbrella.

[Read ebook](#)

[Start free trial](#)