LACEWORK

How to protect your cloud environment from ransomware

Ransomware is big business

A company, on average, faces 21 days[1] of downtime and a recovery cost of $1.85 million[2] because of ransomware.

Ransomware-as-a-service model payment demands range from

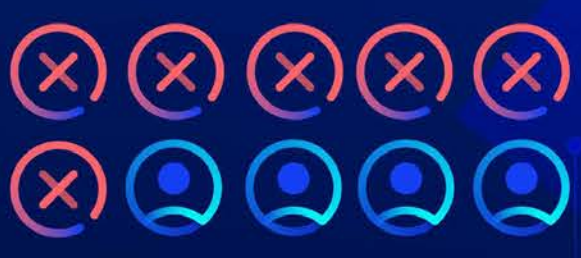
$200,000 to $2,000,000[3]

83%[4]

of successful attacks now feature double or triple extortion.

The true costs of an attack

9 in 10[5] consider trustworthiness prior to purchasing.



6 in 10[6] said they would avoid business with a company that experienced a cyberattack.

Savings start with a better defense

Get better visibility, insights, and action to respond and investigate attacks faster.

Speed cuts costs.

Save with less downtime, less to remediate, and less damage to your brand.

Lacework gives you the visibility and insights needed to take action before, during, and after an attack

Before an attack	During an attack	After an attack
Prevention	**Detection**	**Investigation**
✓ Cloud Security Posture Management (CSPM)	✓ Behavioral anomaly detection	✓ 180-day data retention
✓ Vulnerability management	✓ File integrity monitoring	✓ Contextual event cards
✓ Multicloud visibility	✓ Host intrusion detection	✓ Command line visibility
	✓ Runtime detection	✓ Third-party remediation/ orchestration
Visibility	**Insights**	**Action**
Extensive visibility across your entire cloud environment Understand sprawl and assess risk	Comprehensible, accurate detection of what matters most Make sense of the chaos and monitor for trouble	Automated understanding of your cloud to make investigations faster Turn insights into action from build to runtime
83%[7] of organizations report using 2+ public cloud providers.	The average Lacework customer has **14.2 billion** signals monthly.	**90%**[8] of organizations say data silos create significant business challenges.

Lacework can help you answer these critical questions about your cloud environment to spot risks sooner

- What is my environment?
- What are my assets?
- Where are my assets?
- What's happening in my environment?
- How do I identify and quickly shut down threats?
- Are the right things talking to the right things?
- Is anything happening that shouldn't be?
- Are there measures I can take to reduce risks proactively during build time?
- What can I automate to quickly remediate issues in production?

A new approach to combat ransomware

With an abundance of tools, technologies, and processes available to combat ransomware, why do attacks continue to rise? We're relying on old tools to detect new attack methods.

Change the game and fight ransomware attacks with behavioral analysis. Let Lacework shine a light on anomalous activities across your cloud environment.

Learn more about our anomaly detection

Sources:
(1) Coveware Quarterly Report
(2) Sophos State of Ransomware
(3) Zdnet
(4) TechHQ
(5) Intelligent CISO
(6) Intelligent CISO
(7) Business Technographics Infrastructure
(8) MuleSoft Connectivity Benchmark Report, Data Silos

LACEWORK

04/22