CODE42

42 42 42 42 42

Code42 + CrowdStrike: Threat Protection Inside & Out

You have CrowdStrike to protect against external threats. You need Code42 to detect and respond to insider threats.

CODE42 AS PART OF A LAYERED APPROACH TO SECURITY

Nearly 90 percent of insider threats go undetected for months. By the time organizations find that data was exfiltrated, the damage is done. Code42 speeds the time it takes to detect and respond to data risks so you can address insider threat without disrupting legitimate work.

Together, Code42 and CrowdStrike create a more complete picture of what's going on in your environment. Furthermore, using automation and orchestration platforms like Palo Alto Networks Cortex XSOAR creates time savings for security teams, allowing them to conduct investigations across their entire environment in seconds — and respond to risks quickly, whether that be through corrective conversation, legal action or anywhere in-between.

	Identify	Prevent	Detect	Respond	Recover
Data	Data Identification & Classification	DRM & Encrypt / Data Loss Prevention (DLP)	**CODE42**		
Network	Firewall	Next-Gen Firewall / Network DLP			
Identity	User Authentication	Identity & Access Management (IAM)			
Application	Cloud Gateways	Cloud Access Security Brokers (CASB) Integrated DLP (Gmail, O365, etc.)			
Device	"Legacy Antivirus" Endpoint AV	CROWDSTRIKE			

ELIMINATE DATA LOSS SURPRISES AND KEEP THREATS FROM SLIPPING THROUGH THE CRACKS

HISTORICAL BREADTH
- Monitor when files move to removable media devices, web browsers and cloud accounts, without the need for policies
- Maintain 90 days of historical user activity to identify abnormalities and speed investigations
- Configure alerts by user, activity type, and file size or count

FORENSIC DEPTH
- Review detailed information on files, devices, cloud destinations and exposure events
- Identify trends and abnormalities in data movement using dashboards for common exfiltration vectors
- Preserve copies of files for as long as needed to support your organization's legal hold and eDiscovery process

FILE ACCESS
- Access file contents to determine their sensitivity and value
- Restore files that have been deleted by employees
- Recover files from lost and stolen devices

> **If it wasn't for Code42's ability to see the files, we wouldn't really understand what the person is doing...It provides us both speed and thoroughness of investigations."**
>
> — **Tim Briggs,**
> Director, Incident Response, CrowdStrike

CODE42 QUICK FACTS

Founded 2001

Locations
Minneapolis (HQ)
Denver
Washington, D.C.

Customers include:

50,000+
organizations worldwide

7 of the world's **10** largest tech companies

13 of the world's **20** most valuable brands

7 of the **8** Ivy League schools

OUR CUSTOMERS

SAMSUNG · Ping Identity · CROWDSTRIKE · Schneider Electric

BOSTON UNIVERSITY · PEGA · MIT · okta

MacDonald-Miller FACILITY SOLUTIONS · Adobe · MACOM · BAYADA Home Health Care

OUR INTEGRATIONS

CORTEX XSOAR BY PALO ALTO NETWORKS · IBM Security

splunk> · splunk> phantom · okta · Ping Identity

Code42 has an open API

AWARDS

2019 Info Security Products Guide Global Excellence Award
Gold Winner Security Products and Solutions for Enterprise (Medium)

2019 Cyber Defense Awards
Black Unicorn Award Winner

2019 Globee Awards
Gold Winner for IT or Cybersecurity – Security Software

2019 Cyber Defense Magazine InfoSec Award
Next-Gen Data Loss Prevention

2019 Cyber Defense Magazine InfoSec Award
Next-Gen Insider Threat Detection

2019 Cybersecurity Excellence Awards
Gold Winner: Data Leakage Prevention

2019 Cybersecurity Excellence Awards
Silver Winner: Best Cybersecurity Company

FOR MORE INFORMATION: VISIT CODE42.COM

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM

OV0919161