Comparing How Two Financial Institutions Secure Customer Data With Red Canary

Learn how Red Canary helps two leading financial institutions secure sensitive customer data against advanced attacks.

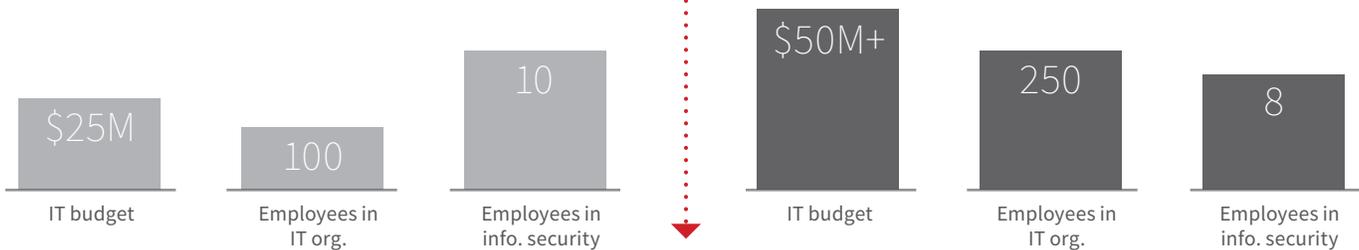| MULTI-STATE BANK	VS	GLOBAL FINANCIAL INSTITUTION

BUSINESS ENVIRONMENTS

MULTI-STATE BANK

AUM: **$15B+**

Revenue:	$1B
Employees:	2,000
Endpoints:	3,300
Locations:	125+

GLOBAL FINANCIAL INSTITUTION

AUM: **$252B+**

Revenue:	$300M
Employees:	2,000
Endpoints:	3,200
Locations:	Dozens across 30 countries

STAFFING RESOURCES

MULTI-STATE BANK

$25M	100	10
IT budget	Employees in IT org.	Employees in info. security

GLOBAL FINANCIAL INSTITUTION

$50M+	250	8
IT budget	Employees in IT org.	Employees in info. security

CHALLENGES

Security Gaps

The bank's IT team had already invested in application whitelisting to secure its endpoints. The solution succeeded in defending against the vast majority of attacks they were previously having to remediate, but gaps remained and endpoints were vulnerable.

Distributed Endpoints

With over 3,000 endpoints across 30 countries, the financial investment firm's network was large, distributed, and vulnerable. Their endpoint security solution was burdensome to the business and IT department, limited by operating systems, and threats continued to slip through.

NEEDS

- A second set of eyes
- Advanced threat detection especially those leveraging native OS tools
- Thorough investigation of all potential threats

- 24/7 monitoring and threat detection
- Outsourced event triage and investigation
- Extensive threat detection from commodity malware/ crimeware to advanced attacks
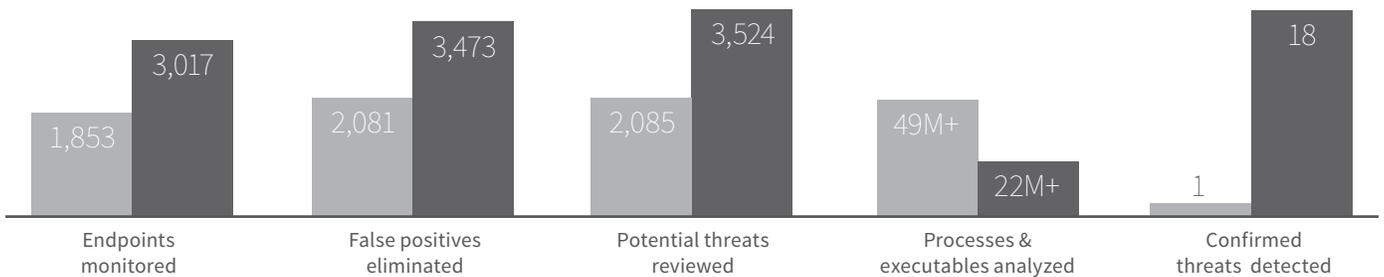
red canary

SOLUTION

Continuous 24/7 Monitoring and Hunting
Red Canary gives the bank the visibility and detection coverage they need to feel confident that advanced attacks are not being overlooked. The bank's red team expert tested Red Canary thoroughly and the solution detected each attack launched, the majority of which exploited PowerShell. Red Canary's detection and response solution was so effective the bank soon expanded coverage to its branches.

Red Canary's Cyber Incident Response Team
The CISO wanted to implement Carbon Black Response, but recognized his team didn't have the resources to manage it on their own. With Red Canary, the CISO got visibility across his endpoints, extensive threat detection, triage and investigation of every potential threat, and remote remediation tools. Threats are quickly detected and validated by Red Canary, and his team has the reporting and tooling they need to limit dwell time and eliminate each threat.

RED CANARY TYPICAL PERFORMANCE OVER 30 DAYS

Endpoints monitored	False positives eliminated	Potential threats reviewed	Processes & executables analyzed	Confirmed threats detected
1,853 / 3,017	2,081 / 3,473	2,085 / 3,524	49M+ / 22M+	1 / 18

IN THEIR OWN WORDS

"Red Canary is a true partner. They're in the fight with us, not just watching and sending alerts over the wall. If something happens, they are there to collect information and get us what we need to respond."

- Information Security Manager, Multi-State Bank

"Red Canary is extremely efficient at handling all of the endpoint data and accurately detecting threats. We haven't seen the same level of expertise with any other vendor."

- Director of Technology, Private Investment Firm

red canary

Every financial institution has its own unique challenges. Red Canary defends investment firms, banks, credit unions, capital management firms, foundations, and trust funds.

Learn more at **redcanary.com/demo**