# Inside Data Breaches

## How Long Does It Take to Discover a Breach?

Dwell time can span from hours to years.


**Breach Dwell Time**

**99 Days**

**Time to Contain It**

**66 Days**

Sources: *2019 Data Breach Investigations Report* (Verizon); *2017 Cost of Data Breach Study* (IBM Security and Ponemon Institute); *M-Trends 2017, A View From the Frontlines* (Mandiant)

## One Data Breach Costs $3.62 Million

And that's just the average. Below is a breakdown of how expensive a security incident can get.

Incident response and investigation
**$20K–10M**

Security audit
**$10K–120K**

Legal settlements
**$11.2M–115M**

Legal counsel
**$390–$1,200** /hour

Crisis management
**$200–$500** /hour

Customer notifications
**$5–$10** /customer

Employee turnover
**21%** of annual salary

New CISO
**$223K–$420K** salary

Recruiting new CISO
**20–50%** of salary

Regulatory Fines—% of annual income
Remediation/Extra Security
Discounts and Gift Cards

All numbers represent average costs. Sources: *2017 Cost of Data Breach Study* (IBM Security and Ponemon Institute); *Calculate the Business Impact and Cost of a Breach* (Forrester, 8/31/17); http://www.fairinstitute.org/blog/what-is-open-fair-and-who-is-the-open-group

### Equifax Lost $7 Billion


A pair of breaches caused its stock to plummet 65%—in a little over one week.

Stock figures as of 9/20/17. Source: Stock Chart and Quote (via Equifax.com)

## The Never-Ending SOC Cycle

Security teams can get thousands of SIEM system alerts each day. After deciding which are most pressing, they will spend hours investigating a threat. Here is one example of this often fruitless search.

- ☑ **Guess**
  - Choose an alert to pursue
- ☑ **Console**
  - Look at 8+ SOC dashboards for context
  - Check SIEM, and spot 2 IP addresses
- ☑ **Research**
  - Figure out which systems the IP address match
  - Determine if IP addresses are good or bad
  - Look at asset-inventory system for application owners
- ☑ **Setback**
  - Email owners, due to out-of-date asset inventory system
- ☑ **Research**
  - Find out when system was last scanned
  - Figure out if the system has been patched
- ☑ **Console**
  - See if the system has been backed up
- ☑ **Email**
  - Request a one-off vulnerability scan
- ☑ **Research**
  - Check if backend has been tested
- ☑ **Setback**
  - Discover disaster recovery is only annual
- ☑ **Console**
  - Find where log files are being sent
- ☑ **Setback**
  - Not all log files are available
- ☑ **Email**
  - Request missing logs
  - Receive missing logs within 2 hours
- ☑ **Setback**
  - 4+ hours later, realize that this is a false alarm
- ☑ **Guess**
  - Start this process again with next alert

Sources: "Cybersecurity: Why Context Matters and How Do We Find It" and "Cybersecurity: The End of Rules Is Nigh" (Hortonworks); "What Your Security Scientists Can Learn From Your Data Scientists to Improve Cybersecurity" (TechCrunch)

## How to Catch a Thief

Security analytics combined with AI and machine learning is transformative. Micro Focus Interset's big data processing swiftly pinpoints threats, while expanding visibility to get a contextual picture of enterprise risk.

The solution lies in distilling billions of events into hundreds of anomalies, then into a handful of actionable SOC leads.

## Learn More

Find and respond to unknown threats—before it's too late. Discover more at microfocus.com.