

## PRIME 100

# Product Overview

Admitted, standalone cyber insurance for businesses with up to \$100M in revenue

Prime 100 is designed for small and medium-sized enterprises (SMEs) with up to \$100M in revenue. It's the ideal solution for businesses buying cyber insurance for the first time or moving beyond bundled coverage in a BOP or packaged policy.

### Clarity that cuts through complexity

Policies address today's most common cyber incidents, from ransomware and phishing to business interruption and data compromise, explained in terms brokers can share with clients.

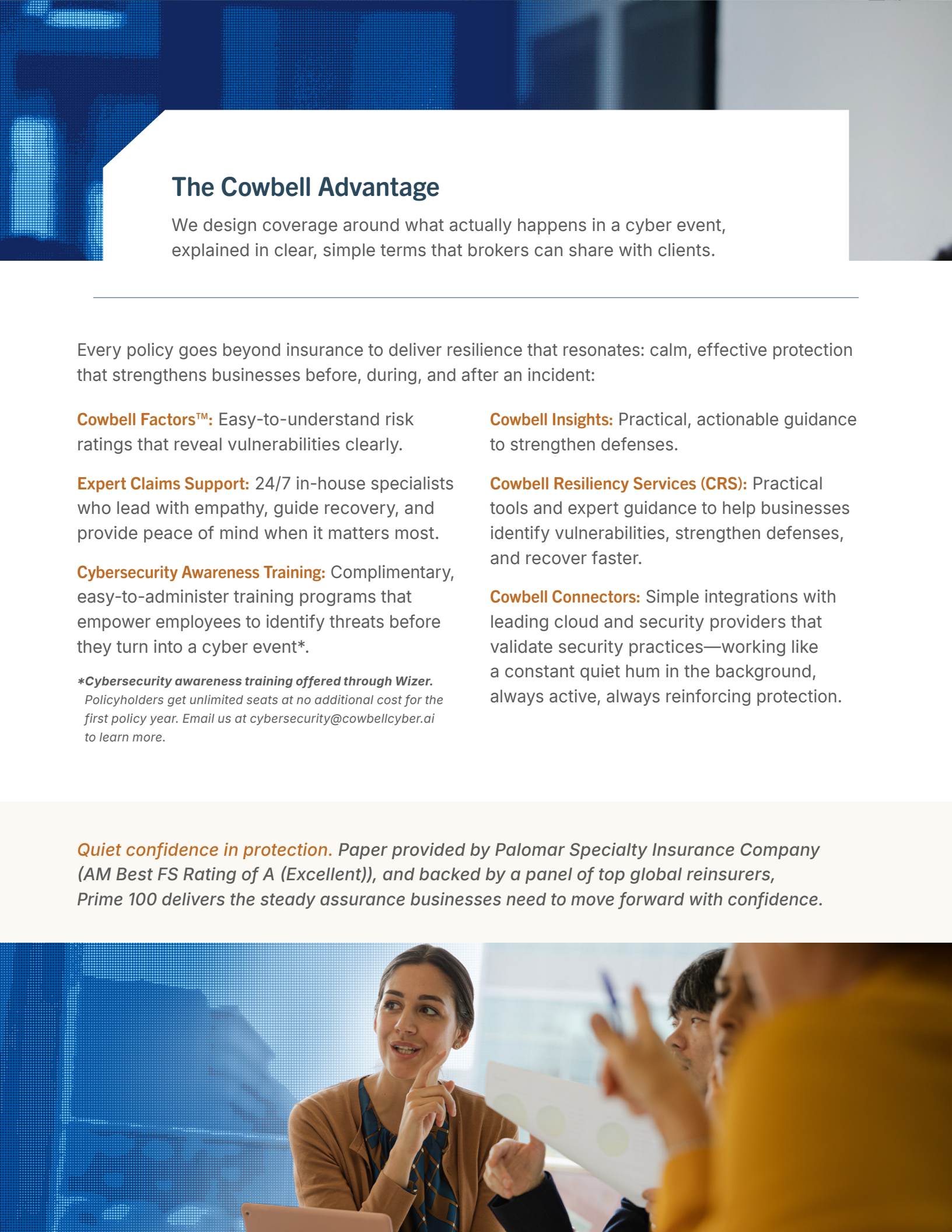
### Fast, flexible protection

Agents can quote, bind, and issue customizable policies in less than five minutes, giving clients fast access to tailored protection.



### Risk Appetite:

- 
- |                      |                   |
|----------------------|-------------------|
| • Accounting Firms   | • Law Firms       |
| • Contractors        | • Manufacturing   |
| • Dental Offices     | • Medical Offices |
| • Financial Services | • Nonprofits      |
| • Healthcare         | • Retailers       |
| • Hospitality        | • Truckers        |
| • Insurance Agencies | • Wholesale       |
| • Prof. Services     | • and more!       |



## The Cowbell Advantage

We design coverage around what actually happens in a cyber event, explained in clear, simple terms that brokers can share with clients.

---

Every policy goes beyond insurance to deliver resilience that resonates: calm, effective protection that strengthens businesses before, during, and after an incident:

**Cowbell Factors™:** Easy-to-understand risk ratings that reveal vulnerabilities clearly.

**Expert Claims Support:** 24/7 in-house specialists who lead with empathy, guide recovery, and provide peace of mind when it matters most.

**Cybersecurity Awareness Training:** Complimentary, easy-to-administer training programs that empower employees to identify threats before they turn into a cyber event\*.

**\*Cybersecurity awareness training offered through Wizer.**  
Policyholders get unlimited seats at no additional cost for the first policy year. Email us at [cybersecurity@cowbellcyber.ai](mailto:cybersecurity@cowbellcyber.ai) to learn more.

**Cowbell Insights:** Practical, actionable guidance to strengthen defenses.

**Cowbell Resiliency Services (CRS):** Practical tools and expert guidance to help businesses identify vulnerabilities, strengthen defenses, and recover faster.

**Cowbell Connectors:** Simple integrations with leading cloud and security providers that validate security practices—working like a constant quiet hum in the background, always active, always reinforcing protection.

**Quiet confidence in protection.** Paper provided by Palomar Specialty Insurance Company (AM Best FS Rating of A (Excellent)), and backed by a panel of top global reinsurers, Prime 100 delivers the steady assurance businesses need to move forward with confidence.

## Prime 100 Coverages

The portfolio of coverages in Cowbell Prime 100 is designed to address the diversity of cyber incidents and resulting damages that can impact businesses.



### Security Breach Expense

Coverage for losses and expenses directly associated with recovery activities in the aftermath of a cyber incident. This can include investigation and forensic services, notification to customers, call center services, overtime salaries, post-event monitoring services such as credit monitoring for impacted customers, and more.



### Security Breach Liability

Coverage for third-party liability directly due to a cyber incident, and the insured becomes legally obligated to pay. This includes defense expenses, compensatory damages, settlement amounts, and fines or penalties assessed against the insured by a regulatory agency or government entity, or for non-compliance with the Payment Card Industry Data Security Standards.



### Hardware Replacement Costs

Coverage for the cost to replace computers or any associated devices or equipment operated by the insured that are unable to function as intended due to corruption or destruction of software or firmware, resulting from a cyber incident.



### Extortion Threats

Coverage for loss resulting from an extortion threat that is discovered during the policy period. This can include approved firms and resources that determine the validity and severity of the threat, interest costs associated with borrowing for the ransom demand, reward payment that leads to conviction and arrest of the party responsible, the ransom payment, and other reasonable expenses.



### Business Income & Extra Expense

Coverage for the losses and costs associated with the inability to conduct business due to a cyber incident or an extortion threat. Business income includes net income that would have been earned or incurred. Note that business interruptions due to system failure or voluntary shutdown are not covered.



### Social Engineering

Coverage for a loss resulting from a social engineering incident where the insured is intentionally misled to transfer money to a person, place, or account directly from good faith reliance upon an instruction transmitted via mail by an imposter. A documented verification procedure requirement needs to have been completed in order to be provided coverage.



### Public Relations Expense

Coverage for the fees and costs to restore reputation in response to negative publicity following a cyber incident or a security breach. This includes, for example, the fees associated with the hiring of a public relations firm that handles external communications related to the breach.



### Computer & Funds Transfer Fraud

Coverage for the losses due to a fraudulent computer operation that causes money (or other property) to be transferred from an insured's account. This also covers losses incurred by a fraudulent instruction directing a financial institution to debit money from the insured's transfer account.



### Telecommunications Fraud

Coverage for the cost of unauthorized calls or unauthorized use of the insured's telephone system's bandwidth, including but not limited to phone bills.



### Website Media Liability

Coverage for the income loss and extra expense due to a system failure (see policy wording) which causes the actual and measurable interruption, suspension, failure, degradation, or delay in performance of a service provider's computer system.



### Ransom Payments

Coverage for the reimbursement of the monetary value of any ransom payment made by the insured to a third party in response to a ransom demand to resolve an extortion threat.



### Restoration of Electronic Data

Coverage for the costs to replace or restore electronic data or computer programs in the aftermath of an incident. This can also include the cost of data entry, reprogramming, and computer consultation services to restore lost assets.

## Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.



The scenario, examples, and descriptions provided above are for general informational purposes only and are illustrative in nature. They do not set forth all possible situations or outcomes and should not be relied upon as any guarantee of coverage or resolution. Each incident is unique and actual experiences may differ. This document does not amend, extend, or form part of any insurance policy. Coverage is determined solely by the specific terms, conditions, limitations, and exclusions of the issued policy. Please refer to your policy for complete details. ©2024 Cowbell Cyber, Inc. All Rights Reserved. Cowbell Insurance Agency LLC, State Licenses: <https://cowbell.insure/state-licenses/>.