NIMBUSSEC

NimbusSec Value Analysis

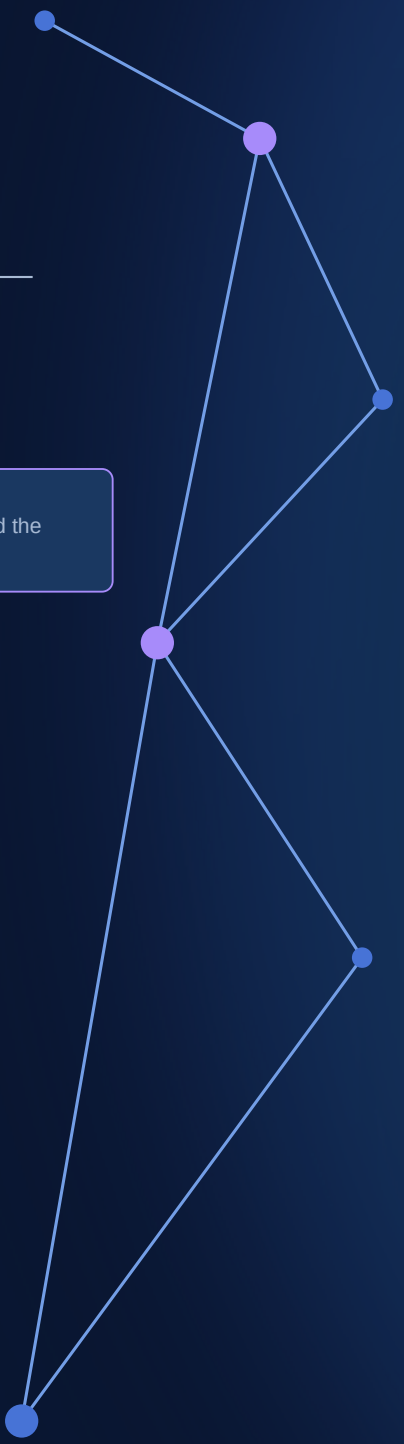
Prepared by CyberSecure

Modeled financial value, downside risk, and key operating assumptions assembled from client inputs, IRIS loss benchmarks, and cited NimbusSec evidence.

Report basis

Built from client scenario inputs [2], IRIS cyber-loss benchmarks [1], cited NimbusSec evidence [3], and the documented model methodology [4].

April 26, 2026 · Confidential



Decision summary and ROI evidence

This page translates the scenario into a decision-ready view: simulated NPV outcomes, downside frequency, and the organization profile used to size the business case.

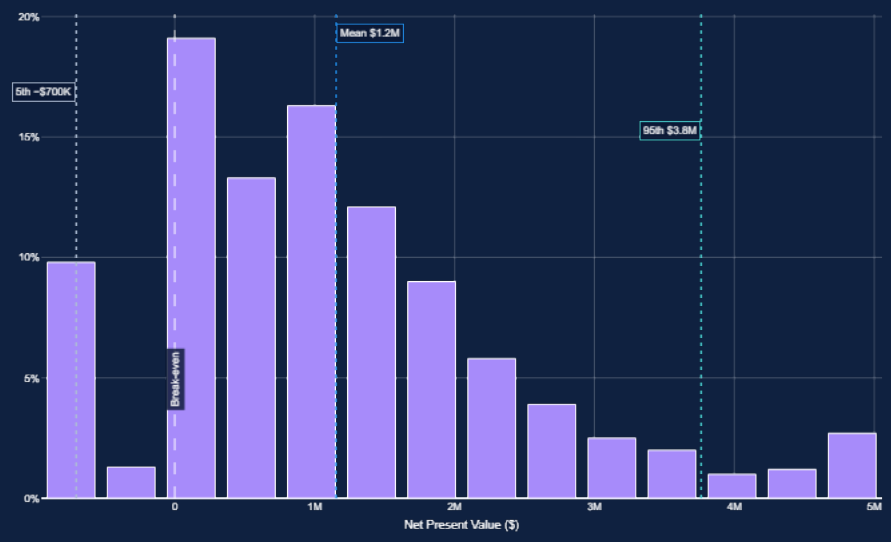
Modeled mean NPV is $1.2M after $830K of present-value cost, with a 6% chance of downside.

Reconciliation

KPI NPV is net of modeled subscription, deployment, support, timing, and discounting. Gross value drivers below show the largest benefit sources before those offsets.

Net value (NPV)	Chance of Downside	Loss reduction	ROI
$1.2M	6%	1.6%	140%

Modeled NPV distribution



NPV evidence summary

Metric	Value
Mean NPV	$1.2M
5th Percentile	–$700K
95th Percentile	$3.8M
Chance of Loss	6%

Modeled organization profile

Metric	Value
Employees	2.5K
Endpoints	2.5K
Revenue	$500M
Industry	Manufacturing
Industry factor	1.03x
Annual subscription	$110K
Years	3

Gross value drivers

Gross modeled benefits are $2.0M; the six drivers below explain $1.9M of that value, while the remaining $120K reflects timing, interaction effects, and discounting before modeled costs.

Incident Response

Faster investigation and remediation.

$960,744

Avoided Breach Loss

Lower expected loss from reduced incident frequency and severity.

$29,073

Posture Triage Efficiency

Faster CSPM finding triage and routing to owners.

$398,090

Audit Efficiency

Less compliance evidence gathering across cloud accounts.

$187,809

Misconfig Remediation

Automated drift remediation across cloud workloads.

$50,947

Penalty Avoidance

Expected regulatory or non-compliance exposure avoided.

$233,889

Risk evidence and value model

Cybersecurity risk assessment

Revenue calibrates breach frequency and severity from IRIS data [1], while efficacy assumptions determine how much of that inherent loss profile remains after deployment.

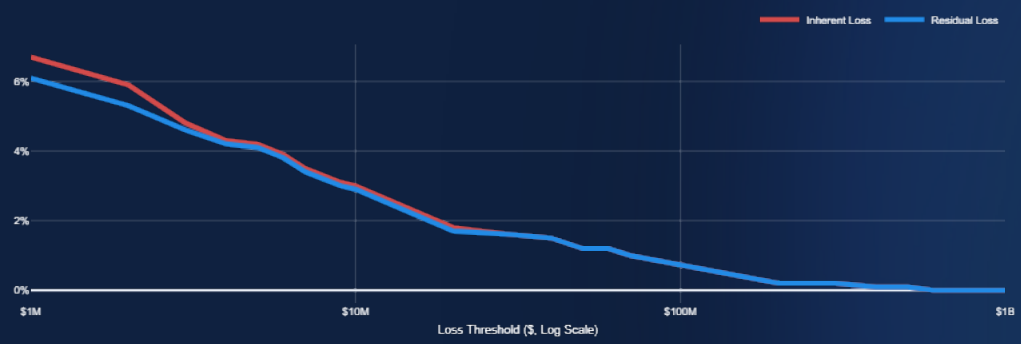
Evidence

The quantile table gives dollar loss thresholds at selected exceedance probabilities, while the curve shows the full inherent-versus-residual loss profile from the same simulation runs.

Loss exceedance statistics

Probability	Inherent	Residual
10%	$230K	$140K
5%	$2.7M	$2.6M
2%	$18M	$16M
1%	$65M	$65M

Modeled loss exceedance



Read the table and curve together: the table reports specific exceedance points, while the curve shows whether modeled loss reduction is broad-based or concentrated in the tail.

At the 2% loss-exceedance point, modeled downside declines from $18M to $16M.

At the 1% tail, residual loss converges with inherent loss, indicating the model assumes limited mitigation in the most extreme scenarios.

NimbusSec value framework and outputs

The value model links scenario inputs, realization timing, and a shared efficacy state to net financial outcomes that can be reconciled back to the evidence above.

Inputs

Firm parameters
Annual revenue, endpoint count, time horizon, and discount rate.

Baseline risk inputs
IRIS estimates incident frequency and loss severity from revenue tier.

Control inputs
NimbusSec changes prevention, containment, MTTR, and operating effort.

→

Model

Risk Reduction
NimbusSec lowers incident probability and reduces loss severity

Efficiency value
Labor savings from faster investigation, simpler operations,

Total

Total
Risk reduction plus operational efficiency.

→

Outputs

Financial metrics
NPV, ROI, and payback summarize investment performance.

Risk metrics
Outputs show inherent risk, residual risk, and expected loss avoided.

Distribution view
Monte Carlo results show downside, upside, and value by driver.

Attribution
The model separates value from prevention, containment, and efficiency.

Model inputs and source notes

The variables below define the modeled scenario across incident-response, breach-risk, operational, and commercial assumptions.

Use the type column to distinguish fixed values from modeled ranges; source IDs in brackets map to the citations below.

How to read this page

Type = Fixed when P5, P50, and P95 are the same value, regardless of whether the value comes from a client input, benchmark, or internal assumption.
Type = Range when uncertainty is modeled across the low / median / high columns. Source IDs in brackets map to the citations below.

A. Incident Response Drivers

Variable	Type	Low	Median	High
[2] Annual revenue ($)	Fixed	$500M	$500M	$500M
[2] Revenue per employee ($/employee)	Fixed	$200K	$200K	$200K
[2] Endpoints per employee	Fixed	1	1	1
[2][4] Investigations / endpoint / year	Range	0.20	0.30	0.40
[2][4] Investigation hours / incident	Range	9	12	15
[3][4] MTTR reduction if realized (%)	Range	68%	75%	82%
[2] SecOps hourly cost ($/hour)	Fixed	$78	$78	$78
[2] Worker hourly cost ($/hour)	Fixed	$52	$52	$52
[4] Operational efficacy realized (%)	Range	46%	49%	52%

B. Breach Frequency & Impact

Variable	Type	Low	Median	High
[1] Annual breach probability (%)	Range	2.7%	6.1%	14%
[4] Conditional breach reduction (%)	Range	60%	70%	80%
[4] Breach reduction if realized (%)	Range	30%	40%	50%
[1] Breach impact ($)	Range	$2.1K	$290K	$51M

Model inputs and source notes

Legend

Type = Fixed when P5, P50, and P95 are the same value, regardless of whether the value comes from a client input, benchmark, or internal assumption.
Type = Range when uncertainty is modeled across the low / median / high columns. Source IDs in brackets map to the citations below.

C. Operational Benefit Drivers

Variable	Type	Low	Median	High
[3][4] SecOps hours saved / endpoint / year	Range	0.84	0.94	0.99
[3][4] Audit efficiency realized (%)	Range	7.9%	9.8%	12%
[3][4] Audit hours saved / employee / year	Range	0.33	0.40	0.47
[2] Audit hourly cost ($/hour)	Fixed	$85	$85	$85
[2][4] Reimage rate per endpoint (%)	Range	3.7%	5.3%	7.1%
[2] Cost per reimage ($)	Range	$292	$391	$534
[4] Reimage reduction if realized (%)	Range	35%	46%	56%
[4] Conditional reimage reduction (%)	Range	71%	83%	92%
[4] Conditional penalty avoidance (%)	Range	30%	40%	50%
[4] Penalty as share of revenue (%)	Range	0.0013%	0.015%	0.039%

Model inputs and source notes

Legend

Type = Fixed when P5, P50, and P95 are the same value, regardless of whether the value comes from a client input, benchmark, or internal assumption.
Type = Range when uncertainty is modeled across the low / median / high columns. Source IDs in brackets map to the citations below.

D. Commercial Terms & Realization Timeline

Variable	Type	Low	Median	High
[2] Discount rate (%)	Fixed	10%	10%	10%
[2][3] Subscription / endpoint / year ($)	Range	$38	$44	$52
[2][3] Deployment / endpoint ($)	Range	$14	$21	$31
[2][3] Annual support ($/year)	Range	$100K	$130K	$160K
[3] Starting realization (%)	Range	65%	77%	86%
[3] Years to full realization	Range	2	3	4
Industry frequency multiplier	Fixed	1 x	1 x	1 x
[2] Manual subscription override ($)	Fixed	0	0	0
[2] Manual implementation override ($)	Fixed	0	0	0
[2] Manual other one-time override ($)	Fixed	0	0	0
[2] Useful life (years)	Fixed	3	3	3

Citations

[1] IRIS 2025 (Cyentia Institute): annualized incident probability and loss trends by firm size.

[2] User-supplied scenario inputs and TrialLevelValues table, 2025.

[3] Forrester Total Economic Impact of NimbusSec (December 2023): representative-firm benefits, costs, and survey evidence.

[4] Cyber value calculator methodology and scenario assumptions curated in 2025.

Legal disclaimer and use terms

At a glance

Illustrative only • Not advice • No warranty • Limited liability • User accepts terms and indemnification obligations

This report and the underlying cyber value calculator (the "Tool") are provided by the sponsoring parties to support evaluation of cybersecurity investments related to NimbusSec. By using this report or the Tool, you ("User") acknowledge and agree to the following legally binding terms and conditions:

1. No warranty — hypothetical results only

All figures, estimates, and projections produced by this Tool—including, but not limited to, Return on Security Investment (ROSI), cost savings, or quantified risk reduction—are hypothetical, non-binding, and based on generalized modeling assumptions or data inputs provided by the User.

The Tool does not, and cannot, account for all variables present in any actual business or cybersecurity environment. The outcomes are intended solely to demonstrate modeling concepts and should not be construed as predictive or factual representations.

2. Not professional advice

This Tool does not constitute legal, financial, investment, cybersecurity, or risk management advice, nor is it a substitute for professional judgment. Any decision made in reliance on the Tool is made solely at the User's discretion and risk.

The sponsoring parties are not providing legal or financial advisory services through this Tool. Users should consult their own qualified advisors before making any decisions based on the Tool's outputs.

3. Limitation of liability

To the fullest extent permitted by applicable law, the sponsoring parties and their respective directors, officers, employees, agents, affiliates, licensors, and partners disclaim all liability for any loss, claim, injury, or damage of any kind, including but not limited to economic loss, indirect or consequential damages, business interruption, or loss of data, arising from:

- The use of, or reliance upon, any output from this Tool;
- The inability to use the Tool; or
- Any errors or omissions in the Tool's methodology, code, or logic.

The Tool is provided "AS IS" and "AS AVAILABLE", without warranties of any kind, whether express, implied, or statutory, including but not limited to warranties of merchantability, fitness for a particular purpose, accuracy, or non-infringement.

4. Indemnification

User agrees to indemnify, defend, and hold harmless the sponsoring parties and their respective affiliates and representatives from and against any and all claims, liabilities, damages, losses, and expenses (including attorneys' fees) arising out of or related to:

- The User's use of the Tool or reliance on its results;
- Any data, content, or inputs submitted by the User; or
- Any breach by the User of these Terms.

5. User acknowledgment and acceptance

By using the information from this report, you confirm that you:

- Have read, understood, and accepted the above terms in full;
- Understand that any outputs are non-deterministic, hypothetical, and not a guarantee of any result;
- Acknowledge that use of this Tool is entirely at your own risk, and that you assume full responsibility for any decisions or actions taken based on the Tool's outputs;
- Agree that no liability shall attach to the sponsoring parties in connection with your use of this Tool.