Featured image: https://www.shutterstock.com/image-photo/person-holds-out-their-hand-digital-2694021153?trackingId=89ec0bb5-ee60-4f64-aa37-89144bc9f2a1&listId=searchResults

How Much Should You Budget for Cybersecurity in 2027?

Budget season tends to land on the IT leader's desk with very little instruction attached. Finance wants a number for security, sales wants SOC 2 wrapped up before the next enterprise deal closes, and you're still the person keeping email, infrastructure, and uptime running.

You don't need to guess. Current benchmarks can give you a defensible starting range, and the factors that move your number up or down are predictable. Below, we explain:

- How much to budget for cybersecurity in 2027
- What drives your budget
- Which line items belong in the plan
- How to phase spending across the year
- How to present your budget to the executive team

Key Takeaways

- Plan for 10-15% of your IT budget, or roughly 0.7% to 1.1% of revenue, based on IANS Research's 2026 benchmarks.
- Compliance frameworks and contract requirements say more about your budget than industry averages do.
- Optimize the tools you own before buying new ones.
- In 2026, IANS found compliance-driven budget requests won increases about 5x the average.

How Much Should a Mid-Market Company Budget for Cybersecurity in 2027?

Most mid-market companies should plan to spend 10-15% of their IT budget on cybersecurity in 2027, or roughly 0.7% to 1.1% of annual revenue. IANS Research's 2026 benchmarks put the all-company average at 9.9% of IT spend, and companies under

$1 billion at a 0.78% median of revenue. Compliance mandates and enterprise contracts push that number higher.

The 2026 IANS Research and Artico Search's 2026 Security Budget Benchmark Report found that security's share of IT spending fell back to 9.9%, the same level as 2021, because AI-driven IT budgets grew faster than security budgets did. On the revenue side, IANS and Artico Search's report on small and mid-market company CISOs puts security at 0.78% median and 1.08% mean of revenue for companies under $1 billion.

Security Budget As a Percentage of IT Spend vs. Revenue

- The **IT percentage** measures how much of your technology budget goes to protecting it.
- The **revenue percentage** measures security investment against the size of the business.

Use the IT percentage for planning and the revenue percentage for board conversations.

The market as a whole keeps growing. In July 2025, Gartner's worldwide information security spending forecast projected end-user spending would rise 12.5% in 2026 to $240 billion. Individual budgets are moving more slowly. The same 2026 IANS report found average security budget growth of 5%, with a median of 0%, and only 45% of security leaders received an increase.

In dollar terms, IANS and Artico Search's 2025 Compensation and Budget Report for CISOs in the Small and Middle Market found an average security budget of $600,000 for companies under $50 million in revenue, scaling to $5 million for companies between $600 million and $1 billion.

Our Take
Don't panic if your IT percentage looks high. Smaller companies carry a baseline of leadership, testing, audit, and core tooling that doesn't shrink with headcount. A $30 million SaaS company preparing for SOC 2 can land well above 15% of IT spend, and that's normal. The revenue percentage usually tells a more accurate story.

— Reviewed by Zach Fuller, Managing Partner and Head of Business Operations & Strategy at Silent Sector

What Moves a Cybersecurity Budget Up or Down?

Four factors decide where your cybersecurity budget lands: the compliance frameworks you must meet, the contracts you're pursuing, your industry, and whether you have internal security staff.

What Moves Your Cybersecurity Budget		
Factor	**Pushes Budget Up When...**	**Keeps It Steady When...**
Compliance frameworks	You're facing a first audit or adding a framework	You're maintaining an existing certification
Contracts	Enterprise or DoD deals require proof of security	Customers don't request security documentation
Industry	Regulators or customers set specific controls	Data sensitivity and oversight are low
Internal staff	No one owns security today	A trained team already runs the program

Which Compliance Frameworks Do You Need to Meet?

Your required frameworks set the floor for your budget. SOC 2 means readiness work, an annual audit, and the controls to stay audit-ready all year. CMMC Level 2 asks defense contractors to implement the NIST SP 800-171 requirements and pass a third-party assessment. HIPAA requires a documented risk analysis and ongoing safeguards across every location that touches patient data.

If you need more than one framework, budget for mapping controls once and reusing the evidence. Overlapping requirements are one of the easiest places to save money.

Which Contracts Are You Pursuing?

The contracts in your 2027 pipeline should shape your budget more than last year's spend. An enterprise prospect's security questionnaire, an RFP that requires SOC 2 Type II, or a DoD contract with CMMC clauses can each justify readiness work on its own. Plan around the deals you intend to win.

How Does Cybersecurity Spend Differ by Industry?

Cybersecurity spend by industry varies widely, and the gap is only growing. IANS's October 2026 guide, 2027 Security Budgets: Where Does Your Industry Stand?, notes that the 5% average growth figure hides a widening split between industries.

What matters most is what your customers and regulators expect:

- **B2B SaaS and tech:** Enterprise buyers drive SOC 2 and ISO 27001 requirements, so spend clusters around audits, testing, and questionnaire readiness.
- **Healthcare and insurance:** HIPAA and payer requirements, spread across multiple locations, push spending toward centralized controls and staff training.
- **Manufacturing and defense:** CMMC drives the budget. IT budgets tend to be lean, so security can look high as a share of IT while staying modest against revenue.

Do You Have Internal Security Staff?

Your staffing model shapes how the budget is split. In 2026, IANS found that staff and compensation took 37% of the average security budget, two points ahead of software and AI at 35%. Companies without a security team reallocate that staffing share to fractional leadership and expert partners, which often costs less than a full-time hire.

What Should a 2027 Cybersecurity Budget Include?

A complete 2027 cybersecurity budget should cover six line items: security leadership, compliance readiness, testing, tooling, training, and incident response reserve.

Here's how that might look for a $60 million B2B SaaS company with an IT team but no dedicated security staff, budgeting about 0.9% of revenue ($540,000) while preparing for its first SOC 2 Type II audit.

Sample 2027 Security Budget Allocation			
Line Item	**% of Security Budget**	**Sample Amount**	**What It Covers**
Tooling	33%	$178,000	Endpoint protection, identity and access management, email security, logging and monitoring
Security Leadership (vCISO)	25%	$135,000	Strategy, roadmap, policy, executive reporting, and hands-on program execution
Compliance Readiness & Audit	20%	$108,000	Compliance alignment analysis, control implementation, evidence collection, auditor fees

Security Testing	12%	$65,000	Annual penetration test, vulnerability scanning, remediation validation
Incident Response Reserve	6%	$32,000	IR retainer, tabletop exercise, contingency
Training & Awareness	4%	$22,000	Security awareness program, phishing simulations, role-based training for IT

Building your 2027 plan? Talk with our team about a cybersecurity budget built around your compliance deadlines and the contracts you want to win.

How to Phase 2027 Cybersecurity Spending Across the Full Year

Phase cybersecurity spending in four stages: assess in Q1, build in Q2, validate in Q3, and prove readiness in Q4. Sequencing the work this way means each dollar builds on the last, and your heaviest spending lands before your audit or contract deadlines instead of after them.

Quarter-by-Quarter Cybersecurity Spending Plan			
Quarter	**Focus**	**What Happens**	**Share of Annual Spend**
Q1	Assess and align	Compliance alignment analysis, priorities set against the 2027 contract pipeline, tool inventory	~20%
Q2	Build and implement	Policies written, controls implemented, existing tools configured, new tools added (only where needed)	~35%
Q3	Validate	Penetration testing, audit readiness review, training push	~25%
Q4	Prove and plan	Audit, questionnaire response library, 2028 planning	~20%

Leadership and tooling subscriptions usually run evenly across the year. The phases above shape everything else.

Phasing also helps with approvals. A request framed as four funded stages with visible progress is easier for leadership to approve than a single number with no milestones attached.

What if your biggest deal closes in June?
Shift the calendar to match. The point is to work backward from the dates that matter to revenue.

Buying New Security Tools vs. Optimizing What You Already Have

Optimize what you already own before you buy anything new. Most mid-market environments already pay for security capabilities that were never fully configured, and tightening those settings often closes priority gaps faster and for less money than a new platform.

At Silent Sector, we're vendor- and technology-neutral, so our recommendations aren't shaped by reseller margins. When a new tool is the right answer, we help you evaluate options objectively. When it isn't, we help you get full value from the stack you already pay for.

The pull toward new tools is especially strong right now. In 2026, IANS found that 69% of CISOs named AI for security as their top priority for net-new budget dollars. Some of those investments will pay off, but others may add another console your team doesn't have time to manage.

Before approving a tool purchase in 2027, ask three questions:

1. Which existing tool covers part of this need today?
2. What would it take to configure that tool fully?
3. Who on our team will own the new tool after it's deployed?

Our Enterprise Cyber Risk Assessment shows what your current environment can already do and where new investment would deliver measurable value. Check it out →

How to Tie Cybersecurity Spend to Revenue Outcomes

Tie cybersecurity spend to revenue by connecting each line item to a business result leadership tracks: deals closed, security questionnaires passed, contracts renewed,

and audits completed on schedule. When the budget reads as a plan for growth, it's more likely to be evaluated as one.

In 2026, IANS's 2026 Security Budget Benchmark Report found that only 3% of CISOs with growing budgets cited a major breach as the reason. New regulations or compliance requirements produced a 22% average budget increase when cited, roughly 5x the overall average, and stronger board or executive focus produced 23%.

Expert Insight
Fear is the weakest budget argument available. Leadership responds to business conditions it already cares about. "We need SOC 2 Type II to close the three enterprise deals in our Q3 pipeline" will win more support than any headline about the latest attack.

— Zach Fuller, Managing Partner at Silent Sector

What does that look like in practice? Pair each major line item with a metric leadership already reviews regularly:

- **Compliance readiness:** Audit dates met, certifications earned or renewed
- **Testing and tooling:** Security questionnaires completed without findings, time to respond
- **Leadership:** Contracts won that required proof of security maturity
- **Training:** Few incidents tied to user error, faster reporting of suspicious activity

Framing the budget this way also prepares you for the conversation that comes next: getting leadership aligned behind the plan.

Build a Cybersecurity Budget That Drives Growth

A defensible 2027 cybersecurity budget starts with a benchmark of 10% to 15% of IT spend, or about 0.7% to 1.1% of revenue. From there, adjust for your frameworks, contracts, industry, and staffing. Build the plan around six line items, phase spending across the year, and optimize what you own before buying more. Then tie every dollar to a revenue outcome. Done that way, the budget stops reading as a cost center and starts reading as a growth plan.

Book a conversation with our team to map your 2027 cybersecurity budget to your compliance deadlines and contract goals.

Frequently Asked Questions About Cybersecurity Budgets

Will cybersecurity budgets increase in 2027?

Many security leaders expect they will. In 2026, IANS and Artico Search found that 64% of CISOs expect a budget increase in 2027, while only 45% received one in 2026. Requests tied to compliance requirements and board priorities have won the largest increases, so frame your request around those drivers.

What percentage of the IT budget should go to cybersecurity?

Most mid-market companies should allocate 10% to 15% of their IT budget to cybersecurity. In 2026, IANS Research and Artico Search's Security Budget Benchmark Report found the average across all company sizes was 9.9%. Companies facing SOC 2, CMMC, or HIPAA requirements, or running lean IT budgets, often land higher.

What percentage of revenue should a company spend on cybersecurity?

A practical range for mid-market companies is about 0.7% to 1.1% of annual revenue. IANS and Artico Search's 2026 research on companies under $1 billion reports a 0.78% median and a 1.08% mean. The right number depends on your compliance requirements, the contracts you pursue, and your industry.

How much does compliance add to a cybersecurity budget?

Compliance is often one of the largest line items in a mid-market security budget, especially in a first audit year. Costs include readiness work, control implementation, evidence collection, and auditor or assessor fees. Companies pursuing multiple frameworks save by mapping controls once and reusing evidence across SOC 2, ISO 27001, CMMC, or HIPAA.

Is a vCISO more cost-effective than a full-time CISO?

For most mid-market companies without a security team, yes. A vCISO provides executive-level strategy and program leadership without a full-time executive salary. In 2026, IANS found staff and compensation took 37% of the average security budget. A NextGen vCISO also handles hands-on execution, so plans get implemented.

How often should you budget for penetration testing?

Budget for at least one third-party penetration test per year, plus retesting after remediation. Many enterprise buyers and auditors expect a recent annual test, and

PCI DSS requires one. Add testing after major changes, such as launching new applications, migrating to the cloud, or completing an acquisition.

URL slug: cybersecurity-budget-2027

SEO title: How Much to Budget for Cybersecurity in 2027

Meta description: Plan your 2027 cybersecurity budget with current benchmarks, a sample allocation, and a quarterly plan that ties security spend to revenue growth.