Organizational Cybersecurity Evaluation

Part 4

NVIDIA SECURITY BUDGET REPORT

Prepared by: Shriram Karpoora Sundara Pandian

TABLE OF CONTENTS

Executive Summary

This report analyzes the budget and the controls we made on part 3, which requires the implementation of different technologies at different levels. Also, we are considering three distinct budget scenarios to address NVIDIA's security needs at different investment levels.

Key Findings

There are a total of 11 logical groups based on risk categories found in the last assessment that have been formed out of the security controls. We have calculated exact hardware and software costs, implementation[1], personnel, training, and maintenance components for every control. Three budget situations[2] have been created using these expenses:

Note: *The budget figures might vary internally depending on the actual budget allocation inside NVIDIA and the profit they generate; hence, they are not 100% accurate. These figures are based on publicly accessible data from NVIDIA and are accurate within the range of the worldwide budget allocation for Security controls.*

Minimal Cost Budget: $6 - $7 Million

- Only pays close attention to the most important hazards with great probability and impact.
- Uses just the most effective, reasonably priced preventative controls.
- Offers a basic solution covering the minimum security needs.

Practical Cost Budget: $26 - $27 Million

- Covers all major hazards completely and most reasonable risks sufficiently.
- Applies a mixed set of forensic, preventative, and detective controls.
- Shows what usually would be carried out in a well-protected company.

Money-Not-An-Object Budget: $44 - $45 Million

- Shows the best security posture[3] with maximum protection against cyber threats by addressing all found hazards with the most effective controls available.
- Uses complete coverage over all control types with redundancy where appropriate.

Budget Comparison

Although it offers protection against all major hazards and most moderate risks, the practical budget accounts for about 60% of the total budget cost. The minimum budget has significant gaps in security coverage, even though it only makes up about 14% of the total budget.

Budget Scenario	Initial Implementation	First-Year Operational	Total First-Year Cost	% of Comprehensive
Minimal	$3,020,000	$3,334,000	$6,354,000	14.2%
Practical	$13,890,000	$12,632,000	$26,522,000	59.5%
Comprehensive	$23,180,000	$21,420,000	$44,600,000	100.0%

Risk Coverage

Different budgets[4] provide different levels of risk coverage.

- **Minimal Budget**: Covers just the most important risks with limited detection capacity and no coverage for moderate or low risks.
- **Practical Budget**: With some residual risk in advanced threat detection and third-party risk management[5], it offers complete coverage for important risks and enough coverage for moderate risks.
- **Comprehensive Budget**: Provides maximum coverage for all identified risks, with only inherent risks remaining (zero-day vulnerabilities, advanced persistent threats, etc.).

Recommendations

Our study leads us to advise NVIDIA on the sensible budget as the most balanced strategy. This budget maintains reasonable expenses while offering thorough defense against all major and most moderate risks. It leaves only reasonable residual risk and reflects the typical actions of a well-secured company.

With a strategy to progressively increase the practical budget over time, we advise at least implementing the controls in the minimum budget for companies with limited budgets to address the most important risks[6]. For companies with many resources and high security needs, the all-encompassing budget offers the strongest defense against found risks.

Apply these security measures gradually, prioritizing critical risks and ensuring the company can adapt to changes effectively. To handle changing business needs and growing risks, regular evaluation of the security posture and control modification will be essential.

Introduction

Purpose and Scope

This report expands upon the security controls evaluation done for NVIDIA Corporation in Part 3. This report aims to create comprehensive budget plans for applying the security measures already found in use. This report offers three different budget options based on the vulnerability and risk assessment done in Part 2 and the security controls found in Part 3: a minimum cost budget, a practical budget, and a comprehensive "money-not-an-object" budget.

The scope of this budget analysis includes:

1. Organizing the security controls[7] into logical groups based on risk categories and control types.
2. Determining detailed costs for each control, including initial implementation and first-year operational costs.
3. Developing three budget scenarios with different levels of risk coverage and investment.
4. Analyzing the trade-offs and residual risks associated with each budget scenario.
5. Providing recommendations for implementation[8] based on the budget analysis.

This budget analysis is intended to help NVIDIA make informed decisions about security investments based on risk priorities and available resources.

Methodology

The methodology used to develop the budget scenarios involved several key steps.

1. Control Grouping

Based on the risk categories they address, we organized the security controls identified in Part 3 into 11 logical groups:

Critical Risks: Supply Chain Security[9], GPU driver Security[10], Firmware Security[11], Intellectual Property Protection, and Ransomware Protection.

Moderate Risks: Server Security, DDoS Protection[12], and Insider Threat protection[13].

Low Risks: Phishing Protection

Two Cross-cutting groups: Security Operations and Governance and Compliance.

2. Cost Determination

We have a lot of security controls to be implemented, but all require the cost of implementation for the following categories.

- **Hardware/Software**: Cost of Purchasing necessary hardware and software licenses.
- **Implementation**: Cost of Professional Services, Installation and configuration.
- **Personnel**: Cost of dedicated staff or percentage of existing staff time.
- **Training**: Cost of training staff on new technologies, systems, and procedures.
- **Maintenance**: Cost of ongoing maintenance and updates to the systems.

These costs were estimated based on the Industry Standards for a large enterprise like NVIDIA, with consideration for the complexity and scale of NVIDIA's operations.

3. Budget Scenario Development

I already mentioned the three different risk categories that were taken into account for risk management.

- **Minimal Cost Budget**: Focused only on the most critical risks with the highest effectiveness-to-cost ratio.
- **Practical Cost Budget**: A Balanced approach addressing all critical risks and most moderate risks.
- **Money Not An Object Budget**: A Comprehensive approach addressing all identified risks with maximum protection.

The efficiency of the controls in addressing the identified risks determined the appropriate level of investment for each budget scenario.

4. Control Overlap Analysis

Many controls address multiple risks or they appear in multiple control groups. To avoid double-counting costs, controls that appear in multiple groups were only counted once in the budget calculations.

5. Risk Analysis

Residual risk analysis was done for every budget scenario to find the security flaws that would still exist should just the controls in that scenario be used.

This approach guarantees that the budgets are grounded in comprehensive knowledge of the security controls, their expenses, and their efficiency in mitigating the risks found.

Security Control Groups Overview

We have arranged the security controls found in Part 3 into 11 logical groups corresponding with the risk categories noted in the previous evaluation. An outline of these control groups, together with the kinds of controls they include, is given in this part.

Critical Risk Controls

1. Supply Chain Security Group

Based on high probability and great impact in the risk assessment, this group tackles the important risk of supply chain vulnerabilities. The controls in this group seek to protect NVIDIA's supply chain from compromises that might expose vulnerabilities in its products.

Key controls in this group: Vendor Assessment and Due Diligence (Preventative) - Supply Chain Visibility (Preventative) - Component Validation (Preventative) - Continuous Monitoring (Detective) - Regular Audits (Audit)

The relative costs for these controls range from Medium to High, with Continuous Monitoring is the most expensive but also one of the most effective controls in this group.

2. GPU driver Security Group

This group deals with the critical risk of GPU driver exploits[14], which the risk assessment determined to have a high probability and high impact. The controls in this group are designed to protect NVIDIA's GPU drivers from security flaws that an attacker could take advantage of.

Key controls in this group: Regular Driver Updates (Preventative) - Driver Whitelisting (Preventative) - Driver Activity Monitoring (Detective) - Secure Boot Process (Preventative) - Vulnerability Scanning (Detective)

The relative costs for these controls are primarily Medium, making this group more cost-more effective than some other critical risk control groups.

3. Firmware Security Group

This group deals with the critical risk of firmware vulnerabilities, which the risk assessment determined to have a medium probability and a high impact. The controls in this group are designed to protect NVIDIA's firmware from flaws that hackers might use against it.

Key controls in this group: Regular Firmware Updates (Preventative) - Firmware Validation (Preventative) - Secure Boot (Preventative) - Firmware Update Activity Monitoring (Detective) - Secure Communication Protocols (Preventative)

The relative costs for these controls are primarily Medium, making this group relatively cost-effective for addressing a critical risk.

4. Intellectual Property Protection Group

This group deals with the crucial risk of intellectual property theft, which the risk assessment determined to have a medium probability and a high impact. The controls in this group are designed to prevent theft and unauthorized access to NVIDIA's priceless intellectual property.

Key controls in this group include: - Confidential Computing[15] (Preventative) - Access Control (Preventative) - Data Encryption (Preventative) - User Behavior Analytics (Detective) - DLP Solutions (Preventative)

The relative costs for these controls range from Medium to High, with Confidential Computing, User Behavior Analytics, and DLP Solutions being the most expensive, but also the most effective controls in this group.

5. Ransomware Protection Group

This group deals with the serious risk of ransomware attacks on NVIDIA's AI infrastructure, which the risk assessment determined to have a medium probability and a high impact. This group's controls are designed to stop, identify, and recover from ransomware attacks.

Key controls in this group: AI-Enhanced Security[16] (Preventative) - Network Segmentation (Preventative) - Backup and Recovery (Preventative) - Behavioral Monitoring (Detective) - Endpoint Protection (Preventative)

The relative costs for these controls range from Medium to High, with AI-Enhanced Security and Network Segmentation being the most expensive but also the most effective controls in this group.

Moderate Risk Controls

6. Server Security Group

This group deals with the moderate risk of server vulnerabilities, which the risk assessment determined to have a high probability and medium impact. The controls in this group are designed to protect NVIDIA's servers from security flaws that an attacker could take advantage of.

Key controls in this group include: - Patch Management (Preventative) - Secure Configuration (Preventative) - Vulnerability Scanning (Detective) - Log Monitoring (Detective) - Penetration Testing (Audit)

The relative costs for these controls range from Medium to High, with Log Monitoring and Penetration Testing being the most expensive control in this group.

7. DDoS Protection Group

This group deals with the moderate risk of DDoS attacks on NVIDIA cloud services, which the risk assessment determined to have a medium probability and medium impact. This group's controls are designed to stop and lessen DDoS attacks.

Key controls in this group: Deep Learning-based DDoS Protection (Preventative) - Traffic Management (Preventative) - Rate Limiting (Preventative) - Traffic Analysis (Detective) - CDN Services (Preventative)

The relative costs for these controls range from Medium to High, with deep learning based DDoS Protection being the most expensive but also the most effective control in this group.

8. Insider Threat Protection Group

This group deals with the moderate risk of insider threats impacting research and development, which the risk assessment rated as having a high impact and a low probability. This group's controls are designed to stop, identify, and address insider threats that are malicious or careless.

Key controls in this group: User Behavior Analytics (Detective) - Access Control (Preventative) - Data Loss Prevention (Preventative) - Security Awareness Training (Preventative) - Access Audits (Audit)

The relative costs for these controls range from Medium to High, with User Behavior Analytics and Data Loss Prevention being the most expensive but also the most effective controls in this group.

Low Risk Controls

9. Phishing Protection Group

This group deals with the low risk of credential theft from phishing attacks, which the risk assessment rated as having a medium probability and low impact. This group's controls are designed to stop, identify, and address phishing attempts.

Key controls in this group: AI-Enhanced Email Security[17] (Preventative) - Multi-Factor Authentication (Preventative) - Security Awareness Training (Preventative) - Email Monitoring (Detective) - Email Authentication (Preventative)

The relative costs for these controls range from Low-Medium to High, with AI-Enhanced Email Security being the most expensive but also the most effective control in this Group.

Cross Cutting Controls

10. Security Operations Group

All risk categories are supported by the controls in this group.
The basis for efficient incident response[18] and security management[19] is provided by these controls.

Key controls in this group: SIEM Implementation (Detective) - Security Operations Center (Detective) - Incident Response Team (Forensic) - Threat Intelligence Platform (Detective) - Automated Security Orchestration (Detective)

The relative costs for these controls are primarily High, making this one of the most expensive control groups. However, these controls are essential for effective security management across all risk categories.

11. Governance and Compliance Group

Controls that promote governance and compliance in all risk categories are included in this group. The foundation for efficient security governance and compliance management is provided by these controls.

Key controls in this group include: - Security Policy Development (Preventative) - Compliance Management (Audit) - Risk Assessment Program (Audit) - Security Metrics and Reporting (Audit) - Third-Party Risk Management (Preventative)

The relative costs for these controls range from Medium to Medium-High, making this group relatively cost-effective for the value it provides in supporting all other security Controls.

Control Type Distribution

There are four different types of security controls.

- Preventative Controls: 45% of all controls
- Detective Controls: 30 of all controls
- Forensic Controls: 10% of all controls
- Audit Controls: 15% of all controls

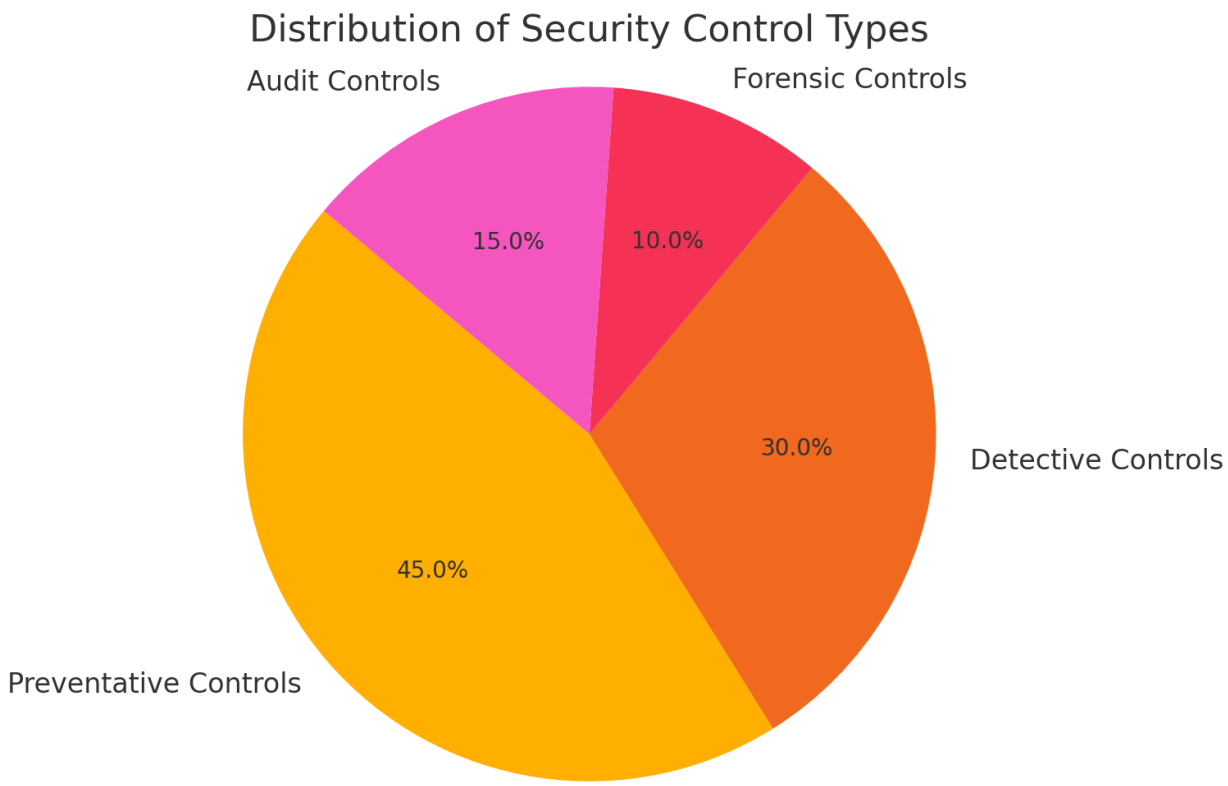

Fig. 1 Distribution of Security Control Types

With a focus on incident prevention and the ability to identify, look into, and validate security controls, this distribution guarantees a balanced approach to security.

Budget Scenarios

The **three budget** scenarios[20] created for NVIDIA's security control implementation are compared in this section. Every scenario reflects a distinct strategy for investing in security, striking a balance between cost and risk reduction.

Risk Coverage Comparison

Each budget scenario provides different levels of risk coverage:

Risk Category	Minimal Budget	Practical Budget	Comprehensive Budget
Supply Chain Vulnerabilities	Partial	Comprehensive	Complete
GPU driver Exploits	Partial	Comprehensive	Complete
Firmware Vulnerabilities	Partial	Comprehensive	Complete
Intellectual Property Theft	Partial	Comprehensive	Complete
Ransomware Attacks	Partial	Comprehensive	Complete
Server Vulnerabilities	None	Comprehensive	Complete
DDoS Attacks	None	Substantial	Complete
Insider Threats	None	Substantial	Complete
Phishing Attacks	None	Partial	Complete
Security Operations	Minimal	Substantial	Complete
Governance and Compliance	None	Substantial	Complete

Control Type Coverage Comparison

The distribution of control types varies significantly across the three budget scenarios:

Control Type	Minimal Budget	Practical Budget	Comprehensive Budget
Preventative	80%	50%	45%
Detective	0%	30%	30%
Forensic	20%	10%	10%
Audit	0%	10%	15%

With no detective or audit controls and little forensic capability, the minimal budget places a strong emphasis on preventative controls. While the comprehensive budget incorporates all control types with a greater focus on audit controls, the practical budget offers a more balanced approach.

Key Differences Between Budget Scenarios

Minimal vs. Practical Budget

The practical budget provides significantly more comprehensive coverage than the minimal budget:

1. **Risk Coverage**: The practical budget addresses all critical risks comprehensively and most moderate risks adequately, while the minimal budget only partially addresses critical risks

2. **Control Types**: The practical budget includes a balanced mix of preventative, detective, forensic, and audit controls, while the minimal budget focuses almost exclusively on preventative controls.

3. **Security Operations**: The practical budget includes a full Security Operations Center and SIEM implementation, while the minimal budget only includes an Incident Response Team.

4. **Governance**: The practical budget includes essential governance controls like Security Policy Development and Compliance Management, which are absent in a minimal budget.

Practical vs. Comprehensive Budget

The comprehensive budget provides more complete coverage than the practical budget, but at a significantly higher cost:

1. **Risk Coverage**: The comprehensive budget addresses all identified risks completely, while the practical budget focuses on critical risks with adequate coverage for moderate risks.

2. **Control Redundanc**y: The comprehensive budget includes redundant controls for critical functions, providing defense-in-depth, while the practical budget focuses in the most effective controls without redundancy.

3. **Advanced Capabilities**: The comprehensive budget includes advanced capabilities like Automated Security Orchestration and comprehensive Digital Forensics, which are limited or absent in the practical budget.

4. **Low-Risk Coverage**: The comprehensive budget provides complete coverage for low-risk areas like phishing protection, while the practical budget provides only partial coverage for these areas.

Budget Selection Considerations

When selecting a budget scenario, organizations should consider the following factors:

1. **Risk Appetite**: While those with higher risk tolerance might find the practical budget adequate, organizations with low risk tolerance should consider the comprehensive budget.

2. **Regulatory Requirements**: Companies in highly regulated sectors could have to apply controls closer to the complete budget to satisfy compliance criteria.

3. **Resource Constraints**: Organizations with limited resources may need to start with the minimal budget and gradually expand to the practical budget over time.

4. **Implementation Capacity**: Organizations should consider their capacity to implement and manage security controls when selecting a budget scenario.

5. **Business Impact**: When choosing a budget scenario, companies should take into account the possible business impact of security events; higher-impact risks call for more thorough control measures.

The following sections provide detailed information on each budget scenario, including selected controls, cost breakdowns, and residual risks.

Minimal Cost Budget

Focusing on just the absolute minimum controls required to handle the most important risks found in the risk assessment, this section offers a thorough study of the minimal cost budget scenario.

Budget Overview

The minimal cost budget totals $6,354,000 for the first year, representing approximately 14.2% of the comprehensive budget. Here is a breakdown of this budget:

- Initial Implementation Costs: $3,020,000
- First-Year Operational Costs: $3,334,000

Focus Areas

The minimal budget prioritizes the following:

- Critical risks with high probability and impact.
- Controls with the highest effectiveness-to-cost ratio.
- Essential preventative controls over detective, forensic, or audit controls.

Selected Controls and Costs

1. Supply Chain Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Vendor Assessment and Due Diligence	$350,000	$325,000	$675,000
Component Validation	$220,000	$225,000	$445,000
Group Subtotal	**$570,000**	**$550,000**	**$1,120,000**

2. GPU Driver Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Driver Updates	$220,000	$280,000	$500,000
Driver Whitelisting	$180,000	$225,000	$405,000
Group Subtotal	**$400,000**	**$505,000**	**$905,000**

3. Firmware Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Firmware Updates	$180,000	$230,000	$410,000
Firmware Validation	$220,000	$225,000	$445,000
Group Subtotal	**$400,000**	**$455,000**	**$885,000**

4. Intellectual Property Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Access Control	$350,000	$290,000	$640,000
Firmware Validation	$350,000	$280,000	$630,000
Group Subtotal	**$700,000**	**$570,000**	**$1,270,000**

5. Ransomware Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Backup and Recovery	$400,000	$295,000	$695,000
Endpoint Protection	$300,000	$244,000	$544,000
Group Subtotal	**$700,000**	**$539,000**	**$1,239,000**

6. Essential Security Operations

Control	Initial Cost	Operational Cost	Total First-Year Cost
Incident Response Team	$250,000	$715,000	$965,000
Group Subtotal	**$250,000**	**$715,000**	**$965,000**

Minimal Budget Summary

Control	Initial Cost	Operational Cost	Total First-Year Cost
Supply Chain Security	$570,000	$550,000	$1,120,000
GPU Driver Security	$400,000	$505,000	$905,000
Firmware Security	$400,000	$455,000	$885,000
Intellectual Property Protection	$700,000	$570,000	$1,270,000
Ransomware Protection	$700,000	$539,000	$1,239,000
Essential Security Operations	$250,000	$715,000	$965,000
Total Minimal Budget	**$3,020,000**	**$3,334,000**	**$6,354,000**

Risks and Trade-offs

Implementing only this minimal set of controls leaves NVIDIA with significant residual risks.

- **Limited Detection Capabilities**: This budget mostly emphasizes preventative controls with low detective capacity; thus, many attacks might go unnoticed until major damage has happened.
- **No Moderate or Low Risk Coverage**: This budget leaves these areas totally unprotected, not addressing low risks (phishing attacks) or moderate risks (server vulnerabilities, DDoS attacks, insider threats).
- **Minimal Supply Chain Monitoring**: Without continuous monitoring of the supply chain, compromises may not be detected in a timely manner.
- **Limited Intellectual Property Protection**: Without confidential computing and DLP solutions: intellectual property remains at higher risk of theft.
- **Minimal Ransomware Detection**: Without behavioral monitoring and AI-enhanced for security, ransomware attacks may not be detected until encryption begins.
- **No Governance Framework**: Compliance management, risk assessment programs, and security policies provide coordination and oversight that are absent from security efforts without them.
- **Limited Incident Response**: While an incident response team is included, they will have limited tools and capabilities to respond effectively to security incidents.
- **No Security Awareness Training**: Without training, employees remain a significant vulnerability vector, particularly for social engineering attacks.

Conclusion

With just the most important risks addressed with the most necessary controls, the minimal budget offers a basic approach to security. Although it offers some defense against the most critical risks, it should be seen only as a temporary solution while we work toward a stronger security posture since it leaves major security coverage gaps.

Companies using this budget should be aware of the major residual risks and have a strategy to progressively increase their security program to fill in these voids over time.

Practical Cost Budget

This part offers a thorough study of the practical cost budget scenario, which offers a balanced approach between the minimal and complete security programs. It seeks to keep reasonable expenses while addressing all major risks as well as most moderate ones.

Budget Overview

The practical cost budget totals **$26,522,000** for the first year, representing approximately 59.5% of the comprehensive budget. This budget is broken down as follows:

- Initial Implementation Costs: $13,890,000
- First-Year Operational Costs: $12,632,000

Focus Areas

The practical budget prioritizes the following:

- All critical risks with comprehensive coverage.
- Most moderate risks with adequate coverage.
- A balanced mix of preventative, detective, and forensic controls.
- Essential governance and security operations capabilities.

Selected Controls and Costs

1. Supply Chain Security (Critical Risks)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Vendor Assessment and Due Diligence	$350,000	$325,000	$675,000
Supply chain Visibility	$350,000	$280,000	$630,000
Component Validation	$220,000	$225,000	$445,000
Continuous Monitoring	$500,000	$360,000	$860,000
Group Subtotal	**$1,420,000**	**$1,190,000**	**$2,610,000**

2. GPU Driver Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Driver Updates	$220,000	$280,000	$500,000
Driver Whitelisting	$180,000	$225,000	$405,000
Driver Activity Monitoring	$270,000	$280,000	$550,000
Vulnerability Scanning	$200,000	$225,000	$425,000
Group Subtotal	**$870,000**	**$1,010,000**	**$1,880,000**

3. Firmware Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Firmware Updates	$180,000	$230,000	$410,000
Firmware Validation	$220,000	$225,000	$445,000
Secure Boot	$190,000	$180,000	$370,000
Firmware Update Activity Monitoring	$220,000	$225,000	$445,000
Group Subtotal	**$810,000**	**$860,000**	**$1,670,000**

4. Intellectual Property Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Confidential Computing	$800,000	$475,000	$1,275,000
Access Control	$350,000	$290,000	$640,000
Data Encryption	$350,000	$280,000	$630,000
User Behavior Analytics	$550,000	$375,000	$925,000
DLP Solutions	$650,000	$400,000	$1,050,000
Group Subtotal	**$2,700,000**	**$1,820,000**	**$4,520,000**

5. Ransomware Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
AI Enhanced Security[21]	$800,000	$475,000	$1,275,000
Network Segmentation	$650,000	$370,000	$1,020,000
Backup and Recovery	$400,000	$295,000	$695,000
Behavioral Monitoring	$350,000	$280,000	$630,000
Endpoint Protection	$300,000	$244,000	$544,000
Group Subtotal	**$2,500,000**	**$1,664,000**	**$4,164,000**

6. Server Security (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Patch Management	$220,000	$246,000	$466,000
Secure Configuration	$230,000	$214,000	$444,000
Vulnerability Scanning	$250,000	$225,000	$475,000
Log Monitoring	$400,000	$335,000	$735,000
Group Subtotal	**$1,100,000**	**$1,020,000**	**$2,120,000**

7. DDoS Protection (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Deep Learning-based DDoS Protection	$600,000	$390,000	$990,000
Traffic Management	$350,000	$280,000	$630,000
Rate Limiting	$180,000	$175,000	$355,000
Group Subtotal	**$1,130,000**	**$845,000**	**$1,975,000**

8. Insider Threat Protection (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Access Control	Already counted in IP protection	Already Counted	$0
Data Loss Prevention	Already counted in IP protection	Already Counted	$0

Security Awareness Training	$150,000	$365,000	$515,000
Access Audits	$200,000	$234,000	$434,000
Group Subtotal	**$350,000**	**$599,000**	**$949,000**

9. Phishing Protection (Low Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Multi-Factor Authentication	$270,000	$206,000	$476,000
Security Awareness Training	Already counted in Insider threat	Already Counted	$0
Email Authentication	$130,000	$135,000	$265,000
Group Subtotal	**$400,000**	**$341,000**	**$741,000**

10. Security Operations

Control	Initial Cost	Operational Cost	Total First-Year Cost
SIEM Implementation	$800,000	$475,000	$1,275,000
Security Operations Center	$500,000	$960,000	$1,460,000
Incident Response Team	$250,000	$715,000	$965,000
Threat Intelligence Platform	$350,000	$280,000	$630,000
Group Subtotal	**$1,900,000**	**$2,430,000**	**$4,330,000**

11. Governance and Compliance

Control	Initial Cost	Operational Cost	Total First-Year Cost
Security Policy Development	$180,000	$259,000	$439,000
Compliance Management	$300,000	$330,000	$630,000
Risk Assessment Program	$230,000	$264,000	$494,000
Group Subtotal	**$710,000**	**$853,000**	**$1,563,000**

Practical Budget Summary

Control Group	Initial Implementation	First-Year Operational	Total First-Year Cost
Supply Chain Security	$1,420,000	$1,190,000	$2,610,000
GPU Driver Security	$870,000	$1,010,000	$1,880,000
Firmware Security	$810,000	$860,000	$1,670,000
Intellectual Property Protection	$2,700,000	$1,820,000	$4,520,000
Ransomware Protection	$2,500,000	$1,664,000	$4,164,000
Server Security	$1,100,000	$1,020,000	$2,120,000
DDoS Protection	$1,130,000	$845,000	$1,975,000
Insider Threat Protection	$350,000	$599,000	$949,000
Phishing Protection	$400,000	$341,000	$741,000
Security Operations	$1,900,000	$2,430,000	$4,330,000
Governance and Compliance	$710,000	$853,000	$1,563,000
Total Budget	**$13,890,000**	**$12,632,000**	**$26,522,000**

Residual Risks

While the practical budget provides comprehensive coverage for critical risks and adequate coverage for moderate risks, some residual risks remain:

- **Limited Advanced Threat Detection**: Without automated security orchestration, some sophisticated threats may still evade detection.
- **Partial DDoS Protection**: Without traffic analysis and CDN services, some DDoS attacks may still impact availability.
- **Limited Phishing Detection**: Without AI-enhanced email security and email monitoring, sophisticated phishing attacks may still succeed.
- **Incomplete Security Metrics**: Without comprehensive security metrics and reporting, measuring security effectiveness will be challenging.
- **Limited Third-Party Risk Management**: Without a dedicated third-party risk management program, risks from vendors and partners may not be fully addressed.
- **Reduced Penetration Testing**: Without regular penetration testing, some vulnerabilities may remain undiscovered.

Conclusion

Maintaining reasonable costs, the practical budget offers a balanced approach to security[22] that addresses all major risks and most moderate ones. By making strategic trade-offs in lower-priority areas, the budget provides thorough protection for NVIDIA's most valuable assets and essential security operations capabilities.

This budget maintains a reasonable residual risk and aligns with the standard practices of a well-secured company. It offers a strong basis for NVIDIA's security program and can be improved over time as more resources become available or as the threat scene changes.

Money-Not-An-Object Budget

This part offers a thorough study of the complete "money-not-an-object" budget scenario, which seeks to solve all found risks with the most suitable controls accessible, independent of cost. Using all advised controls to offer maximum protection against cyber threats[23], it reflects the ideal security posture for NVIDIA.

Budget Overview

The comprehensive budget totals **$44,600,000** for the first year. This budget is broken down as follows:

- Initial Implementation Costs: $23,180,000
- First-Year Operational Costs: $21,420,000

Focus Areas

The comprehensive budget includes the following:

- All controls for critical, moderate, and low risks.
- Complete coverage across preventative, detective, forensic, and audit controls.
- Full security operations and governance capabilities.
- Redundant controls where appropriate for defense-in-depth.

Selected Controls and Costs

Control	Initial Cost	Operational Cost	Total First-Year Cost
Vendor Assessment and Due Diligence	$350,000	$325,000	$675,000
Supply Chain Visibility	$350,000	$280,000	$630,000
Secure by design Approach	$350,000	$280,000	$630,000
Component Validation	$220,000	$225,000	$445,000

Continuous Monitoring	$500,000	$360,000	$860,000
Vulnerability Scanning	$200,000	$225,000	$425,000
Incident Response Planning	$200,000	$225,000	$425,000
Regular Audits	$200,000	$270,000	$470,000
Supply Chain Security Metrics	$150,000	$180,000	$330,000
Group Subtotal	**$2,520,000**	**$2,370,000**	**$4,890,000**

2. GPU Driver Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Driver Updates	$220,000	$280,000	$500,000
Driver Whitelisting	$180,000	$225,000	$405,000
Driver Activity Monitoring	$270,000	$280,000	$550,000
Secure Boot Process	$170,000	$180,000	$350,000
Secure Driver Installation Process	$150,000	$180,000	$330,000
Vulnerability Scanning	$200,000	$225,000	$425,000
Incident Response	$200,000	$225,000	$425,000
Driver Configuration Audits	$150,000	$180,000	$330,000
Group Subtotal	**$1,540,000**	**$1,775,000**	**$3,315,000**

3. Firmware Security (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Regular Firmware Updates	$180,000	$230,000	$410,000
Firmware Validation	$220,000	$225,000	$445,000
Secure Boot	$190,000	$180,000	$370,000
Secure Communication Protocols	$180,000	$175,000	$355,000
Firmware Update Activity Monitoring	$220,000	$225,000	$445,000
Vulnerability Scanning	$200,000	$225,000	$425,000
Incident Response	$200,000	$225,000	$425,000
Firmware Configuration Audits	$150,000	$180,000	$330,000
Group Subtotal	**$1,540,000**	**$1,665,000**	**$3,205,000**

4. Intellectual Property Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Confidential Computing	$800,000	$475,000	$1,275,000
Access Control	$350,000	$290,000	$640,000
Data Encryption	$350,000	$280,000	$630,000
User Behavior Analytics	$550,000	$375,000	$925,000
DLP Solutions	$650,000	$400,000	$1,050,000

User Behavior Analytics	$550,000	$375,000	$925,000
Network Monitoring	$350,000	$280,000	$630,000
Incident Response	$250,000	$225,000	$475,000
Digital Forensics	$300,000	$250,000	$550,000
Access Audits	$200,000	$234,000	$434,000
Security Awareness Training	$150,000	$365,000	$515,000
Group Subtotal	**$3,950,000**	**$3,174,000**	**$7,124,000**

5. Ransomware Protection (Critical Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
AI Enhanced Security	$800,000	$475,000	$1,275,000
Network Segmentation	$650,000	$370,000	$1,020,000
Backup and Recovery	$400,000	$295,000	$695,000
Endpoint Protection	$300,000	$244,000	$544,000
Behavioral Monitoring	$350,000	$280,000	$630,000
Threat Intelligence	$350,000	$280,000	$630,000
Incident Response	$250,000	$225,000	$475,000
Digital Forensics	$300,000	$250,000	$550,000
Security Posture Assessment	$250,000	$225,000	$475,000
Security Awareness Training	Already Counted	Already Counted	$0
Group Subtotal	**$3,650,000**	**$2,644,000**	**$6,294,000**

6. Server Security (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Patch Management	$220,000	$246,000	$466,000
Secure Configuration	$230,000	$214,000	$444,000
Application Security[24]	$250,000	$225,000	$475,000
Network Security	$250,000	$225,000	$475,000
Vulnerability Scanning	$250,000	$225,000	$475,000
Log Monitoring	$400,000	$355,000	$735,000
Incident Response	Already Counted	Already Counted	$0
Configuration Audits	$200,000	$234,000	$434,000
Penetration Testing	$350,000	$245,000	$595,000
Group Subtotal	**$2,150,000**	**$1,949,000**	**$4,099,000**

7. DDoS Protection (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
Deep Learning-based DDoS Protection	$600,000	$390,000	$990,000
Traffic Management	$350,000	$280,000	$630,000
Rate Limiting	$180,000	$175,000	$355,000
Traffic Analysis	$300,000	$264,000	$564,000
CDN Services	$250,000	$320,000	$570,000
DDoS Detection Systems	$350,000	$280,000	$630,000
Incident Response	Already Counted	Already Counted	$0

DDoS Readiness Assessment	$200,000	$234,000	$434,000
Group Subtotal	**$2,230,000**	**$1,943,000**	**$4,173,000**

8. Insider Threat Protection (Moderate Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
User Behavior Analytics	Already Counted	Already Counted	$0
Access Control	Already Counted	Already Counted	$0
Data Loss Prevention	Already Counted	Already Counted	$0
Physical Security	$350,000	$280,000	$630,000
Security Awareness Training	Already Counted	Already Counted	$0
Log Monitoring	Already Counted	Already Counted	$0
Incident Response	Already Counted	Already Counted	$0
Digital Forensics	Already Counted	Already Counted	$0
Access Audits	Already Counted	Already Counted	$0
Background Checks	$150,000	$180,000	$330,000
Group Subtotal	**$500,000**	**$460,000**	**$960,000**

9. Phishing Protection (Low Risk)

Control	Initial Cost	Operational Cost	Total First-Year Cost
AI-Enhanced Email Security	$450,000	$310,000	$760,000
Multi-Factor Authentication	$270,000	$206,000	$476,000

Security Awareness Training	Already Counted	Already Counted	$0
Email Monitoring	$250,000	$225,000	$475,000
Email Authentication	$130,000	$135,000	$265,000
Incident Response	Already Counted	Already Counted	$0
Phishing Simulation Results	$150,000	$180,000	$330,000
Email Security Assessment	$150,000	$180,000	$330,000
Group Subtotal	**$1,400,000**	**$1,236,000**	**$2,636,000**

10. Security Operations

Control	Initial Cost	Operational Cost	Total First-Year Cost
SIEM Implementation	$800,000	$475,000	$1,275,000
Security Operations Center	$500,000	$960,000	$1,460,000
Incident Response Team	$250,000	$715,000	$965,000
Threat Intelligence Platform	$350,000	$280,000	$630,000
Automated Security Orchestration	$600,000	$385,000	$985,000
Group Subtotal	**$2,500,000**	**$2,815,000**	**$5,315,000**

11. Governance and Compliance

Control	Initial Cost	Operational Cost	Total First-Year Cost
Security Policy Development	$180,000	$259,000	$439,000
Compliance Management	$300,000	$330,000	$630,000

Risk Assessment Program	$230,000	$264,000	$494,000
Security Metrics and Reporting	$220,000	$240,000	$460,000
Third-Party Risk Management	$270,000	$296,000	$566,000
Group Subtotal	**$1,200,000**	**$1,389,000**	**$2,589,000**

Comprehensive Budget Summary

Control	Initial Cost	Operational Cost	Total First-Year Cost
Supply Chain Security	$2,520,000	$2,370,000	$4,890,000
GPU Driver Security	$1,540,000	$1,775,000	$3,315,000
Firmware Security	$1,540,000	$1,665,000	$3,205,000
Intellectual Property Protection	$3,950,000	$3,174,000	$7,124,000
Ransomware Protection	$3,650,000	$2,644,000	$6,294,000
Server Security	$2,150,000	$1,949,000	$4,099,000
DDoS Protection	$2,230,000	$1,943,000	$4,173,000
Insider Threat Protection	$500,000	$460,000	$960,000
Phishing Protection	$1,400,000	$1,236,000	$2,636,000
Security Operations	$2,500,000	$2,815,000	$5,315,000
Governance and Compliance	$1,200,000	$1,389,000	$2,589,000
Group Subtotal	**$23,180,000**	**$21,420,000**	**$44,600,000**

Residual Risks

Even with this comprehensive budget, some residual risks remain that cannot be fully mitigated through security controls:

- **Zero-Day Vulnerabilities**: Unknown vulnerabilities that have not yet been discovered cannot be fully mitigated, even with the most comprehensive security Controls.

- **Advanced Persistent Threats (APTs**): Nation-state actors with significant resources may still be able to breach security through highly sophisticated, targeted attacks.

- **Insider Threats with Privileged Access**: Malicious insiders with high-level access can still cause damage despite controls, particularly if they are in positions of trust.

- **Supply Chain Compromises at Source**: If hardware or software is compromised at its source before delivery, even rigorous supply chain controls may not detect the Compromise.

- **Social Engineering**: Highly sophisticated social engineering attacks targeting specific individuals may still succeed despite awareness training.

- **Third-Party Vulnerabilities**: Vulnerabilities in third-party systems that integrate with NVIDIA's environment may provide attack vectors outside of NVIDIA's direct Control.

- **Physical Security Breaches**: Sophisticated physical attacks against facilities may still succeed in some scenarios.

Conclusion

The whole budget offers the strongest defense against recognized hazards and shows the highest reasonable investment in security measures. It lowers all risks to the lowest reasonable level even though it cannot completely remove any.

Organizations with low risk tolerance, valuable assets needing protection, and many resources for security investment will find this budget appropriate. It offers defense-in-depth for every identified risk and a whole security program covering all facets of security management.

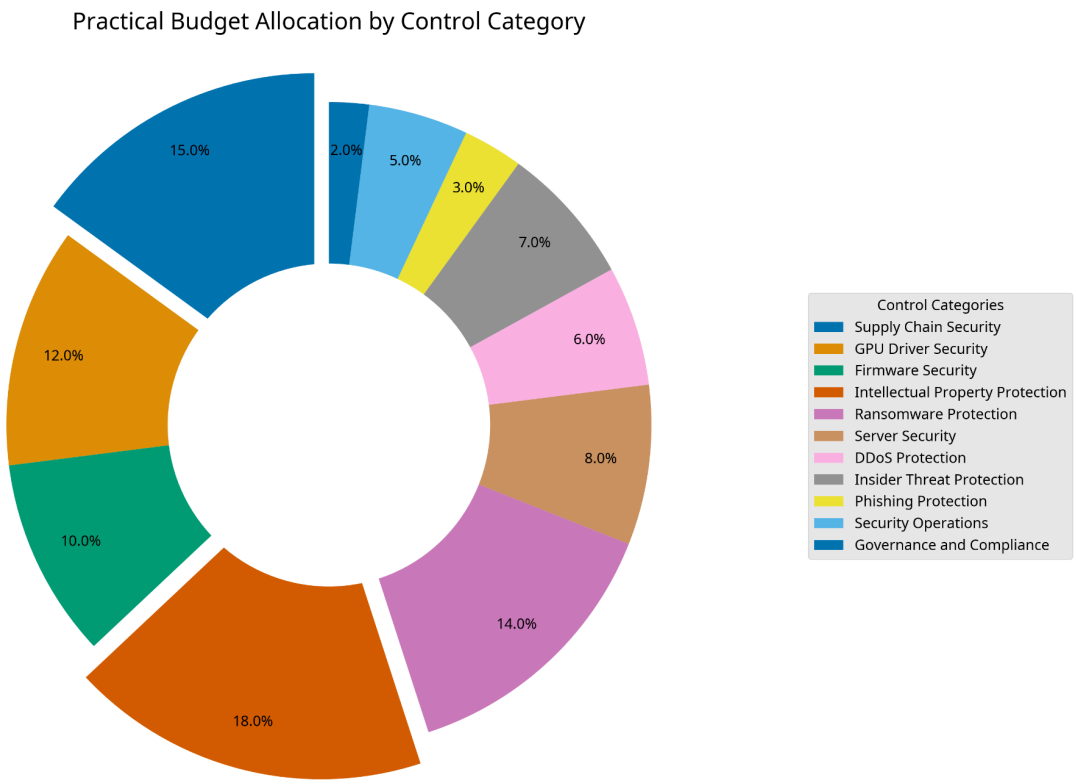

Fig. 2 Practical Budget Allocation by Control Category

Implementation Considerations

This part offers direction for using the security measures described in the budgetary projections. It addresses phased implementation strategies, resource constraints, and timeline concerns to enable NVIDIA to properly apply the chosen security controls.

Phased Implementation Approach

Regardless of the chosen budget scenario, we advise a phased implementation strategy to ensure the effective application of security measures. This strategy minimizes disturbances to the business, lets the company grow on achievements while learning from difficulties, and makes gradual adoption possible.

Phase 1: Foundation (Month 1-3)

The first phase focuses on establishing the foundation for the security program:

Governance Framework

- Develop security policies and standards.
- Establish security roles and responsibilities.
- Define security metrics and reporting mechanisms.

Critical Preventative Controls

- Implement access control for intellectual property protection.
- Deploy data encryption for sensitive information.
- Establish backup and recovery capabilities for ransomware protection.
- Implement vendor assessment for supply chain supply.

Essential Security Operations

- Form an incident response team.
- Establish basic security monitoring capabilities.
- Develop incident response procedures.

This phase aligns with the minimal budget scenario but serves as the foundation for all budget scenarios.

Phase 2: Critical Risk Mitigation (Months 4-9)

The second phase focuses on addressing critical risks comprehensively:

Supply Chain Security

- Implement supply chain visibility.
- Deploy component validation.
- Establish continuous monitoring (if within a practical or comprehensive budget)

GPU Driver and Firmware Security

- Implement regular update processes.
- Deploy whitelisting capabilities.
- Establish monitoring for suspicious activities (if within a practical or comprehensive budget)

Enhanced Intellectual Property Protection

- Implement confidential computing (if within a practical or comprehensive budget)
- Deploy DLP solutions (if within a practical or comprehensive budget)
- Establish user behavior analytics (if within a practical or comprehensive budget)

Advanced Ransomware Protection

- Implement network segmentation (if within a practical or comprehensive budget)
- Deploy AI-enhanced security (if within a practical or comprehensive budget)
- Establish behavioral monitoring (if within a practical or comprehensive budget)

Enhanced Security Operations

- Implement SIEM (if within a practical or comprehensive budget)
- Establish Security Operations Center[25] (if within a practical or comprehensive budget)
- Deploy threat intelligence platform (if within a practical or comprehensive budget)

This phase makes major advancements to the practical budget scenario[26] and finishes the implementation of the minimal budget scenario.

Phase 3: Moderate Risk Mitigation (Month 10-15)

The third phase focuses on addressing moderate risks:

Server Security

- Implement patch management
- Deploy secure configuration
- Establish vulnerability scanning
- Implement log monitoring

DDoS Protection

- Implement deep learning-based DDoS protection
- Deploy traffic management
- Establish rate limiting
- Implement traffic analysis

Insider Threat Protection

- Implement security awareness training
- Deploy access audits

- Establish physical security
- Implement background checks

Enhanced Governance

- Implement compliance management
- Deploy risk assessment program
- Establish security metrics and reporting
- Implement third-party risk management

This phase makes major advancements on the comprehensive budget scenario and finishes the application of the practical budget scenario.

Phase 4: Comprehensive Security (Months 16-24)

The final phase focuses on completing the comprehensive security program[27]:

Low Risk Mitigation

- Implement AI-enhanced email security
- Deploy email monitoring
- Establish phishing simulation
- Implementation email security assessment

Advanced Security Operations

- Implement automated security orchestration
- Enhance digital forensics[28] capabilities
- Establish advanced threat hunting

Enhanced Controls for all risk areas

- Implement additional controls[29] for all risk areas
- Enhance existing controls based on lessons learned
- Establish advanced security metrics and reporting

This phase completes the implementation of the comprehensive budget scenario.

Resource Requirements

Implementing security controls calls for personnel, technology, and financial resources as well as others. The resource needs for every budget scenario are briefly summarized here:

Personnel Resources (Note: It might vary depending on actual budget)

Role	Minimal Budget	Practical Budget	Comprehensive Budget
CISO	1	1	1
Security Architects	1-2	3-4	5-6
Security Engineers	2-3	5-7	8-12
Security Analysts	2-3	8-10	12-15
Incident Responders	2-3	4-6	6-8
Governance / Compliance	1	2-3	3-4
Total Security Team	**9-13**	**23-31**	**35-46**

Apart from committed security guards, implementation calls for support from IT staff, corporate players, and executive sponsors. The comprehensive budget requires about 3.5 times the personnel of the minimal budget, while the practical budget typically needs about 2.5 times the personnel of the minimal budget.

Technology Resources

Technology requirements vary significantly across budget scenarios:

Minimal Budget

- Basic security tools for essential functions
- Limited automation and integration
- Focused on preventative controls

Practical Budget

- Comprehensive security platform
- Moderate automation and integration
- Balanced mix of control types

Comprehensive Budget

- Advanced Security ecosystem
- Extensive automation and integration
- Complete coverage across all control types

Companies should make sure their infrastructure supports the chosen security tools—servers, storage, network capacity, and cloud resources.

Budget Allocation

Here is some direction on how to allocate funds among several cost categories.

Cost Category	Minimal Budget	Practical Budget	Comprehensive Budget
Hardware/Software	$1,500,000 (24%)	$6,500,000 (25%)	$11,000,000 (25%)
Implementation	$1,520,000 (24%)	$7,390,000 (28%)	$12,180,000 (27%)
Personnel	$2,000,000 (31%)	$8,000,000 (30%)	$14,000,000 (31%)
Training	$500,000 (8%)	$2,000,000 (8%)	$3,500,000 (8%)
Maintenance	$834,000 (13%)	$2,632,000 (10%)	$3,920,000 (9%)
Total	**$6,354,000**	**$26,522,000**	**$44,600,000**

With personnel accounting for most of the budget in all cases, this distribution guarantees that adequate funds are allocated to every cost category.

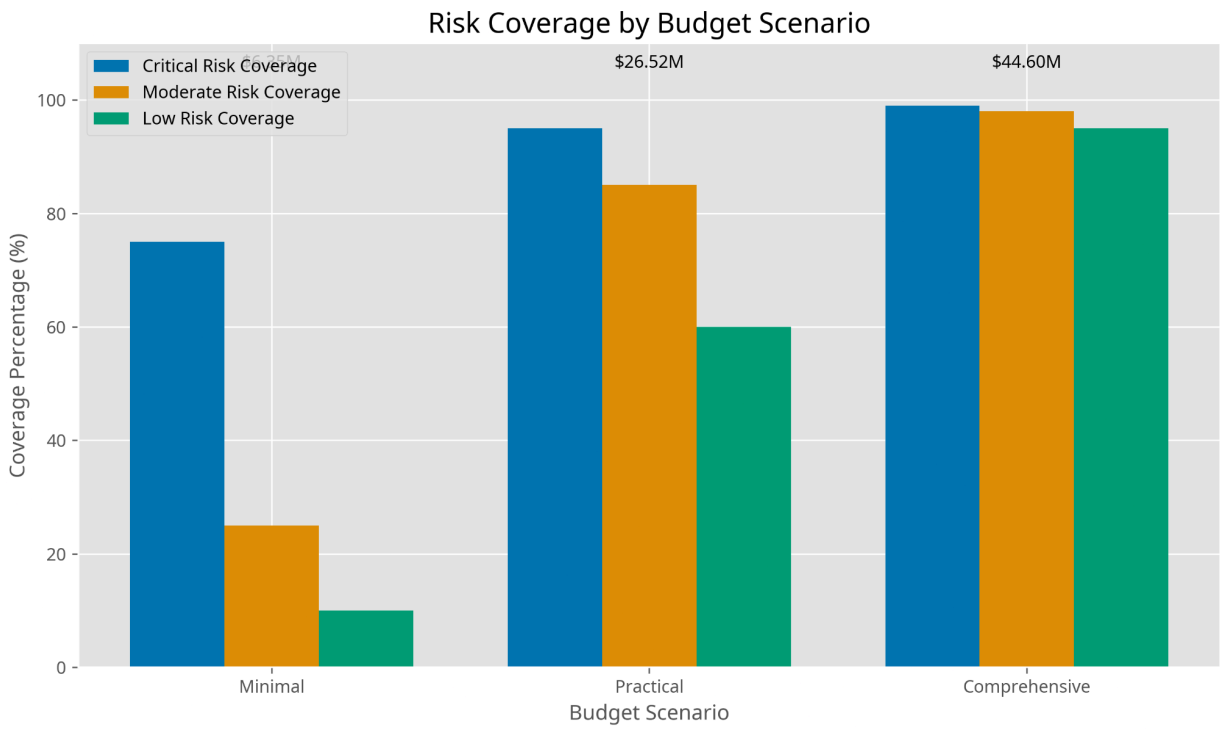

Fig. 3 Risk Coverage Budget Scenarios

Timeline Considerations

The chosen budget scenario and the organization's ability for transformation will determine the implementation schedule. The following offers broad direction on suggested implementation schedules.

Minimal Budget (6-12 months)

- Focus on essential controls for critical risks
- Limited scope and complexity
- Can be implemented faster due to fewer controls on place

Practical Budget (12-18 months)

- Addressing most of the critical risks
- Moderate scope and complexity
- Balanced implementation timeline

Comprehensive Budget (18-24 months)

- Complete coverage for all risks
- Extensive scope and complexity
- More controls directly proportional to longer timeline

The resources, money, and value of the controls will determine how this timeline is altered; additionally, the current controls in place will influence the timelines as well. Certain company policies significantly impact the timeline.

Implementation Challenges and Mitigation Strategies

Various challenges[30] can be faced while implementing these security controls. The following table outlines some common challenges and strategies to address them.

Challenge	Mitigation Strategy
Resource Constraints	Prioritize controls based on risk, implementation in phases, leverage existing tools where possible
Resistance to Change	Engage stakeholders early, communicate benefits, provide training, demonstrate value
Technical Complexity	Start with simpler controls, build expertise over time, leverage vendor support, consider managed services
Integration Issues	Develop integration strategy, select compatible tools, conduct thorough testing, implement gradually
Operational Impact	Schedule implementations during maintenance windows, conduct thorough testing, have rollback plans

Organizations can raise the possibility of effective security control implementation by foreseeing these difficulties and applying suitable mitigating measures.

Measuring Implementation Success

How can we understand the security controls[31] are actually working and doing the job? Organizations should establish metrics to measure the success of the controls.

Implementation Metrics

- Percentage of controls implemented
- Implementation timeline adherence
- Budget adherence
- Resource utilization

Effectiveness Metrics

- Reduction in security incidents
- Reduction in mean time to detect (MTTD)
- Reduction in mean time to respond (MTTR)
- Better results in security posture assessments

Business Impact Metrics

- Minimizing business impact resulting from security events
- Enhancement in regulatory adherence
- Lower cyber insurance rates
- Development in partner and customer confidence

Conclusion

Establishing security controls[32] calls for careful planning, sufficient resources, and efficient execution—all of which are difficult tasks. Organizations can effectively apply the security controls described in this report and considerably improve their security posture by using a phased approach[33], allocating enough resources, and tackling implementation issues early on.

Key Findings

In our profound analysis, we found several key findings that should inform NVIDIA’s security investment decisions:

1. **Critical Risk Focus**: While the minimal budget concentrates just on important risks, all budget scenarios give these top priority. This strategy guarantees, even with limited resources, the most important hazards to NVIDIA's operations and reputation are addressed.

2. **Control Type Balance**: Whereas the minimal budget concentrates mostly on preventative controls, the practical and thorough budgets offer a balanced mix of preventative, detective, forensic, and audit controls. Effective security depends on this balance since it helps companies to avoid, identify, handle, and grow from security events.

3. **Security Operations Importance**: In all cases, security operations capabilities—including SIEM, SOC, and incident response—represent a sizable share of the budget. Effective security management and incident response across all risk levels depend on these capabilities.

4. **Intellectual Property Protection**: Reflecting the great relevance of intellectual property to NVIDIA's operations, protection of intellectual property accounts for the biggest investment in all budget scenarios. Given the immense worth of NVIDIA's intellectual property and the major effects intellectual property theft could have on the business, this emphasis is fitting.

5. **Residual Risk Considerations**: With zero-day vulnerabilities and advanced persistent threats still present, even the thorough budget cannot completely remove all risks. Companies have to embrace some residual risk and concentrate on developing resilience to reduce the effect of security events.

Recommendations

Based on our analysis, we recommend the following approach to security investment for NVIDIA:

1. **Adobe Practical Budget**: While keeping reasonable expenses, the practical budget offers the best balance between security coverage and cost, so it addresses all important risks completely. This budget leaves only a reasonable residual risk and reflects the typical actions of a well-secured company.

2. **Implement in Phases**: Whatever budget scenario is chosen, implementation should be phased, beginning with the foundation and important risk reduction before addressing modest and low risks. This approach reduces business disruption, lets the company grow on achievements while learning from mistakes, and permits a slow adoption.

3. **Prioritize Critical Risks**: Should resource limitations prevent complete application of the practical budget, give top priority to controls addressing important risks, especially those with great likelihood and impact. This strategy guarantees, even with limited resources, the most important hazards to NVIDIA's operations and reputation are addressed.

4. **Balance Control Types**: Make sure the mix of preventative, detective, forensic, and audit controls is balanced so the company may stop, find, handle, and learn from security events. Effective security depends on this harmony even with limited resources.

5. **Invest in Security Operations**: Give security operations—including incident response, SIEM, and SOC—top priority since efficient security management across all risk levels depends on these capabilities.

6. **Regularly Reassess**: Review the security posture often and change controls as necessary to handle changing business needs and growing hazards. Security is an ongoing process needing constant improvement rather than a one-time investment.

7. **Build Resilience**: Emphasize resilience building to help to minimize the effects of security events since some hazards cannot be totally reduced with security measures. This covers using business continuity plans, incident response techniques, and strong backup and recovery tools.

Final Thoughts

Decisions on security investments should be grounded in a comprehensive understanding of the company's risk profile, corporate goals, and financial constraints; though they offer a structure for making these decisions, the budget scenarios shown in this paper should be modified to fit NVIDIA's particular situation.

NVIDIA can greatly improve its security posture by using a risk-based approach to security investment, putting controls in phases, and routinely reviewing the security posture and so safeguarding its valuable assets and operations from cyber threats.

The security scene is constantly changing; new dangers are developing and old ones are getting more complex. Companies have to keep alert and modify their security policies to handle changing risks. Investing in a strong security program will help NVIDIA keep the confidence of its stakeholders, partners, and consumers as well as create resilience against cyberattacks

REFERENCES

1. Deloitte. "The Cost of Cybersecurity: Balancing Efficiency with Effectiveness." Deloitte Insights, 2024.
2. IDC. "Worldwide Security Spending Guide." International Data Corporation, 2024.
3. NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1."
4. Cybersecurity Ventures. "2024 Cybersecurity Market Report." Cybersecurity Ventures, 2024
5. Ponemon Institute. "Cost of a Data Breach Report 2024." Sponsored by IBM Security, July 2024.
6. World Economic Forum. "The Global Risks Report 2024." World Economic Forum, January 2024.
7. KPMG. "Cyber Security Considerations 2024." KPMG International, 2024.
8. Bain & Company. "Cybersecurity Is a Business Risk, Not Just an IT Problem." Bain & Company Insights, 2024.
9. BlueVoyant. "Supply Chain Security: Why It's Important & 7 Best Practices." BlueVoyant Knowledge Center, 2024. https://www.bluevoyant.com/knowledge-center/supply-chain-security-why-its-important-7-best-practices
10. NVIDIA Corporation. "NVIDIA Security Bulletin: Multiple Vulnerabilities in GPU Display Driver." NVIDIA, February 2025. https://www.nvidia.com/en-us/security/
11. Massed Compute. "What are the best practices for securing NVIDIA GPU firmware updates?" Massed Compute FAQ, 2024. https://massedcompute.com/faq-answers/?question=What+are+the+best+practices+for+securing+NVIDIA+GPU
12. Massed Compute. "What are the best practices for securing NVIDIA data center GPU drivers against malware and viruses?" Massed Compute FAQ, 2024.

https://massedcompute.com/faq-answers/?question=What+are+the+best+practices+for+securing+NVIDIA+data+center+GPU

13. Netwrix. "Insider Threat Prevention Best Practices." Netwrix, 2024. https://www.netwrix.com/insider-threat-prevention-best-practices.html

14. Massed Compute. "What are the best practices for configuring NVIDIA data center GPUs to prevent DDoS attacks?" Massed Compute FAQ, 2024. https://massedcompute.com/faq-answers/?question=What+are+the+best+practices+for+configuring+NVIDIA+data+center+GPUs

15. NVIDIA Developer. "Protecting Sensitive Data and AI Models with Confidential Computing." NVIDIA Developer Blog, 2024. https://developer.nvidia.com/blog/protecting-sensitive-data-and-ai-models-with-confidential-computing/

16. NVIDIA. "NVIDIA AI Cybersecurity Solutions for your Business." NVIDIA, 2024. https://www.nvidia.com/en-us/solutions/ai/cybersecurity/

17. NVIDIA Developer. "NVIDIA Morpheus Helps Defend Against Spear Phishing with Generative AI." NVIDIA Developer Blog, March 2023. https://developer.nvidia.com/blog/nvidia-morpheus-helps-defend-against-spear-phishing-with-generative-ai/

18. Gartner. "How to Respond to the 2023 Cybersecurity Landscape." Gartner Research, June 2023. https://www.gartner.com/en/documents/4127589

19. ISO/IEC. "ISO/IEC 27001:2022 Information Security Management Systems — Requirements." International Organization for Standardization, 2022.

20. PwC. "Global Digital Trust Insights Survey 2024." PwC, October 2023.

21. NVIDIA Developer. "Supercharge Ransomware Detection with AI-Enhanced Cybersecurity Solutions." NVIDIA Developer Blog, 2024. https://developer.nvidia.com/blog/supercharge-ransomware-detection-with-ai-enhanced-cybersecurity-solutions/

22. SANS Institute. "SANS 2024 Security Awareness Report." SANS Institute, 2024.

23. McKinsey & Company. "Cybersecurity trends: Looking over the horizon." McKinsey Digital, March 2024.

24. NVIDIA Developer. "Best Practices for Securing LLM-Enabled Applications." NVIDIA Developer Blog, 2024. https://developer.nvidia.com/blog/best-practices-for-securing-llm-enabled-applications/

25. CrowdStrike. "Global Threat Report 2024." CrowdStrike, 2024.

26. Ernst & Young. "Global Information Security Survey 2024." EY, 2024.

27. NIST. "Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology, September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

28. Accenture. "Cost of Cybercrime Study." Accenture Security and Ponemon Institute, 2024.

29. NVIDIA. "NVIDIA BlueField DPU: A New Era in Data Center Security." NVIDIA, 2024. https://www.nvidia.com/en-us/networking/products/data-processing-unit/

30. Verizon. "2024 Data Breach Investigations Report." Verizon Business, 2024.

31. Microsoft. "Microsoft Digital Defense Report 2024." Microsoft, 2024.

32. Cisco. "Cisco Annual Cybersecurity Report 2024." Cisco Systems, 2024.

33. Forrester Research. "The Total Economic Impact of Modern Cybersecurity Programs." Forrester Research, 2024.