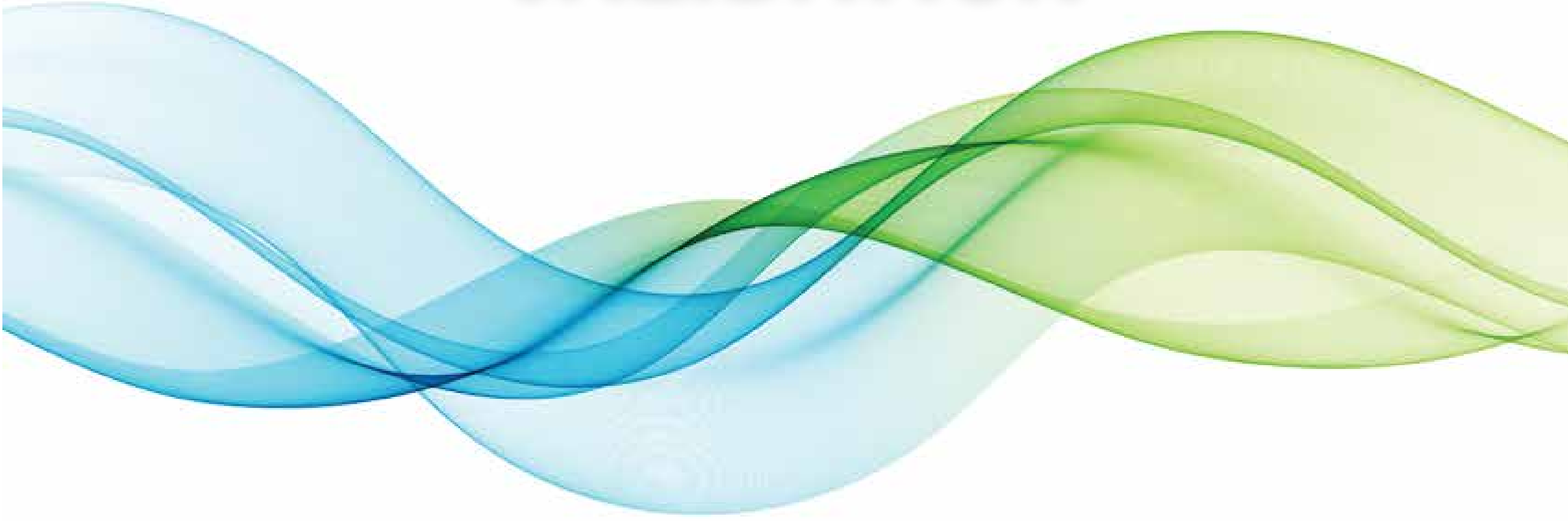
TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

PENTERA AUTOMATED SECURITY VALIDATION



DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG INFOSPHERE, INC.

PENTERA

RETURN ON INVESTMENT (ROI) ANALYSIS:

PENTERA AUTOMATED SECURITY VALIDATION

DR. EDWARD AMOROSO
FOUNDER & CEO, TAG INFOSPHERE, INC.

EXECUTIVE SUMMARY

This TAG[1] analyst report provides a high-level summary of the qualitative and quantitative return on investment (ROI) for the commercial Pentera[2] platform to achieve continuous automated security validation. The assessment shows that organizations should expect excellent qualitative benefits from use of Pentera[3] as well as significant quantitative ROI in the range of 525% to 600% for midsized and larger organizations under reasonable assumptions.

INTRODUCTION

Enterprise security teams must work each day to strengthen their cyber posture in order to reduce their threat exposure and support compliance. Recognition that the enterprise security goal involves *risk reduction* rather than *risk removal* implies that the cybersecurity process will always be on-going. Such continuity, in turn, prompts the need for so-called *continuous threat exposure management* (CTEM) based on the use of an automated platform.

Various types of commercial platforms address continuous cybersecurity since this is such a multidimensional challenge. For instance, identity and access management (IAM), endpoint detection and response (EDR), and secure access service edge (SASE) solutions must now be continuous in their provision of controls. The need thus emerges to validate that these controls are operating as expected and that vulnerabilities are identified and addressed.

This requirement for continuous validation is driven by both the complex nature of modern cybersecurity controls as well as the automation that underlies such technology. Modern IT infrastructure and adversary threats are also evolving constantly, growing ever more sophisticated. Security teams must therefore take steps to ensure that their controls consistently provide the desired level of protection for their fast-changing environment.

Traditional options exist for validation including assessments, penetration testing, scanning, and breach and attack simulation (BAS). One new strategy, however, involves the *continuous validation* of controls *using real-life attack methods* with the goal of identifying exposures. This approach, referred to as *automated penetration testing*, is gaining traction, especially since commercial support for smart automation has improved so much during recent years.

In this report, we focus on the *automated security validation* solution from cybersecurity vendor *Pentera* with specific focus on the cost effectiveness of their approach. Our goal is to explore the qualitative and quantitative returns on investment (ROI) that come from use of this commercial platform. We do so in the context of case study scenarios that are derived from our extensive experience at TAG supporting modern security teams.

The estimated return on investment (ROI) for Pentera was measured in the 525% to 600% range. Such ROI values should make the selection of Pentera's solution a high-priority choice for most enterprise security teams. Use of the Pentera platform will also align with the objective established in many enterprise environments to replace resource-heavy and error-prone manual tasks with streamlined automated support.

BRIEF DESCRIPTION OF PENTERA PLATFORM

Founded in 2015, Pentera is a private cybersecurity company that has been backed by a range of leading investors including Insight Partners, Blackstone, Evolution Equity Partners, K1 Investment Management, and AWZ.[4] The company's most recent round of Series C funding raised an impressive $150M. Pentera now supports over 1,000 enterprise customers located across 60 different countries around the globe.[5]

As suggested above, the company focuses on automated security validation for internal, external, and cloud environments. The platform leverages the expertise of an in-house cyber research team that ensures up-to-date attack surface coverage, control assessment, attack emulation techniques, and support for mitigation. As one would expect, this approach to continuous validation scales well across a range of different industries, verticals, and segments. It is also an effective solution for organizations of varying sizes and security maturity levels.

The Pentera platform is designed to validate cybersecurity across an attack surface including the enterprise network, public and private cloud services, and deployed systems such as for CI/CD and web applications. The platform is comprised of three main products – Core, Cloud, and Surface. These products in turn support two add-on modules testing specific cybersecurity threats – namely, Credential Exposure and RansomwareReady. Security Validation Advisory is a service offering delivered by Pentera technical experts to help organizations accelerate their time-to-value with the platform.[6]

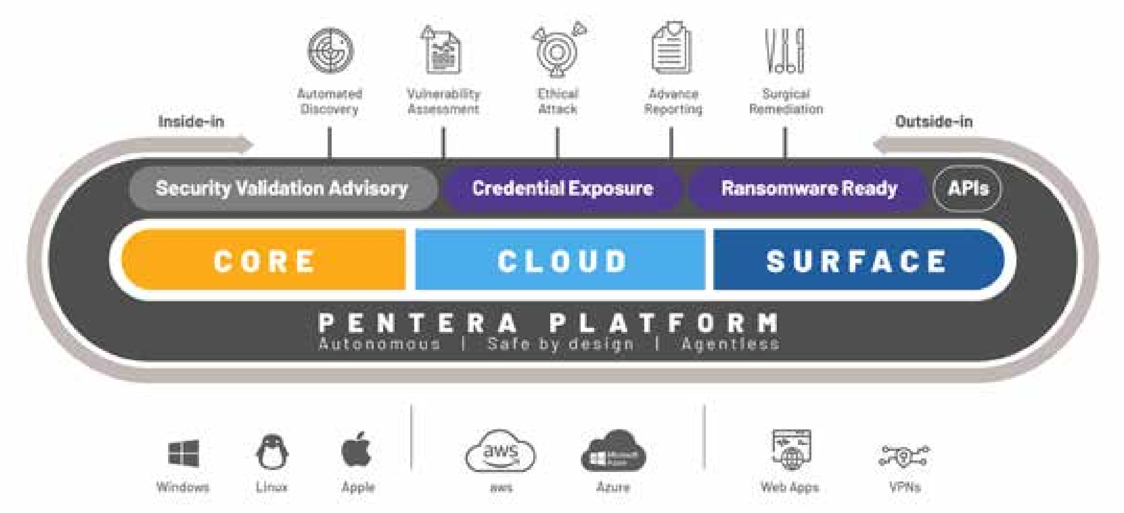


Figure 1. Pentera Platform Schema

In short, the Pentera platform supports validation of security posture. Starting with digital asset discovery and vulnerability assessment, the platform runs ethical attacks in the live production environment to identify kill-chains and provide advanced reporting and surgical remediation guidance. These capabilities allow security teams to offload repetitive testing activities and proactively fix the security gaps that cause the most significant cyber risk exposure.

TAG ROI METHODOLOGY

The approach taken for this Pentera ROI assessment involves identification of two categories of benefit that come from deployment and use of the platform. The first involves *qualitative ROI* which includes benefits that are clearly valuable to a given security or executive team, but that do not result in any direct line-item reductions in budget expenditure. Qualitative ROI is certainly tangible but is sometimes considered non-financial.

In contrast, *quantitative ROI* includes those benefits that have a direct impact on the security, information technology (IT), or related budgets. Such direct impacts include costs for staff, consultants, contractors, services, platforms, or tools. They are usually classified as operating expenses, but in some cases, these costs can be part of a capital budget. In either case, quantitative ROI can be viewed as line-item changes in budgets.

Our ROI analysis is performed in the context of sample use-cases derived from our experience at TAG working with CISOs, as well as running security programs.[7] We have sufficient access to live CISO budgets and expenditures to understand the issues relevant to ROIs. We also spoke with Pentera users directly to validate our assumptions and collaborated closely with the Pentera team who shared experiences with customers, as resources for developing this ROI report.

QUALITATIVE ROI ASSESSMENT

Measuring the qualitative ROI for any platform requires establishment of a reasonable comparison base. For example, if a company is currently doing little or no security validation, which might be found in a smaller or mid-sized company, then the benefits of deploying Pentera will be significant – albeit perhaps requiring the security team to train on how best to use the new capability.

For larger enterprise teams, our experience at TAG is that few are doing no security validation tasks today. This makes qualitative assessment of ROI more nuanced and dependent on the local environment. Qualitative ROI – which, as explained above, implies benefits that are not directly realized in a budget, would likely have a positive impact on business by improving how the organization deals with cyber threats and the quality of work experience for security team members.

We can thus make general comments about qualitative benefits that come from deployment and use of the Pentera solution in most environments. We make these in the context of reasonable assumptions that a given organization is engaged in various on-going security validation tasks, such as performing periodic penetration tests or engaging a security assessment from an external consulting team. We list these benefits below.

Qualitative Benefit: Cybersecurity Employee Retention

The challenge of keeping cyber experts on board and engaged has been a consistent pain-point that emerges often in discussions with customers considering use of Pentera. Specifically, in a market where skilled security professionals are notoriously difficult to find, retaining existing talent becomes paramount. By automating tasks that would otherwise require intensive manual effort, Pentera frees up security teams to focus on deep analysis and creative exploration of non-standard use cases. The exposure findings collected by Pentera serve as input for security teams to build upon. This shift not only enhances job satisfaction but also fosters a more engaged and motivated workforce, ultimately leading to reduced turnover and a more stable, experienced security team.

Qualitative Benefit: Improved Day-to-Day Security Operations

Pentera drives higher levels of day-to-day productivity in security operations. It does this by improving how technology, people, and processes ensure that deployed controls are tuned and validated on an on-going basis and that coordination exists between red teams, blue teams, and the SOC. Pentera performs repetitive testing at a speed and scale not possible using manual methods. Security teams can thus multiply the frequency and scope of their validation tasks, while focusing efforts on advanced use cases and cross-team collaboration.

Qualitative Benefit: Support for Compliance

The Pentera platform helps security teams provide evidence for compliance by continually testing the effectiveness of prevention, detection and response capabilities. The platform helps organizations provide evidence of compliance and address gaps that might detract from compliance. Pentera is especially useful in cases where regulators, auditors, and other assessors demand hard evidence of continuous and on-going security testing.

Qualitative Benefit: Reduced Cyber Insurance Premiums

Engaging with a cyber insurance broker or company will generally demand the provision of detailed information about deployed cyber controls, involving completion of in-depth questionnaires. Pentera will ease this process, helping an organization to establish proof of a strong security regimen and continuous cyber hygiene. Evidence of healthy security behavior and on-going cyber-posture vigilance may result in improvements in cyber insurance terms or rates.[8]

Additional Qualitative Benefits

There are many additional benefits that will emerge in local environments choosing to deploy Pentera, and while a comprehensive list is beyond our scope, we should point out that streamlined mergers and acquisitions (M&A) security assessment and improved communication with leadership regarding security posture and incidents are benefits that accrue from deployment of the automated platform.

QUANTITATIVE ROI ASSESSMENT

The approach taken to develop a quantitative ROI for Pentera involves reviewing, under familiar and reasonable assumptions, a typical security validation-related CISO budget before and after deployment of the platform.[9] Such an approach serves to highlight how an investment in Pentera provides tangible reductions in line-item components of a budget. The spend categories considered in-scope for the quantitative ROI are shown in Figure 2 below.

Consulting Costs	**This includes the often-extensive operating expense costs associated with the provision of expert contractors and external consultants to augment the employee team focused on penetration testing and related security validation programs and tasks.**
Security Platforms	**This category of operational expense can include any deployed tools, systems, or platforms that are being used for security test and control validation purposes. These systems can include on-premises, cloud-hosted, and SaaS-based platforms.**
Security Services	**This includes services used for testing, control, validation, and other means for establishing real-time attack surface posture. Also included are services for responding to incidents, since security validation programs are designed to reduce the likelihood and impact of such incidents.**

Figure 2. Quantitative Spend Summary

Our quantitative estimation includes two baseline scenarios in which we identify a typical enterprise security budget under reasonable circumstances and view their budget finances before and after use of Pentera. The specific instantiation of these quantitative factors as shown in the case study examples below will demonstrate significant returns for enterprise teams who decide to implement Pentera to leverage the benefits of automated security validation.

To work the case studies with representative dollars, we introduce estimates including a sample license cost for Pentera that will help to illustrate a realistic scenario. Obviously, local factors will determine the specific fees paid for the platform, so readers should not use these numbers as the basis for actual license fees, but rather as the basis for ROI planning. We describe below the main quantitative benefits that a typical security team will experience upon deployment and use of Pentera.

Quantitative Benefit: Reduction of Contractors

One of the primary quantitative benefits involves reduced need for contractors. Every CISO knows that this is a component of every security budget – namely, the need to plan for, select, hire, manage, and retain contractors, to augment employee staff.[10] In the context of security validation, contractors may be involved in effort-intensive manual assessment and testing tasks, such as password strength assessments and network configuration checks. The reduction in contractors will thus have a measurable impact on in-year operating expenses for the security team.

Quantitative Benefit: Reduction of External Penetration Testing Service Expenses

This benefit includes reduction of the need for expensive security testing services. The need to engage quality individuals targeted penetration tests or to use accredited external pen testers for compliance purposes is not likely to be completely eliminated. The overall need for testing services, however, can be reduced significantly with the comprehensive automated security validation capabilities provided by

Pentera. Every practitioner will attest to the increasing costs associated with expert manual penetration testing services, as well as the concerns around variance in human expertise levels. The use of Pentera for continuous automated support in this area is therefore a welcome way to reduce expenses while increasing consistency.

Quantitative Benefit: Reduced Incident Response Service Expenses
Cybersecurity incident occurrence and impact will inevitably be reduced through the use of smart automation to patrol and reduce the attack surface, which is where Pentera excels. This is not dramatically different from how many other types of cybersecurity controls reduce incidents. This is, after all, the purpose of deploying security tools and platforms. The Pentera solution, however, is focused on validation of the effectiveness of the overall security program, and the detection of actual exploitable weaknesses. It reduces incident response service expenses due to the reduction of incidents, as well as the provision of attack surface and vulnerability information to support triage and forensics in case an incident occurs.

Additional Benefits Not Factored in the ROI Analysis
It is key to mention that while automation of penetration testing tasks reduces the workload of internal security staff currently handling these tasks manually, the reduction of expert payroll workforce (i.e., employees) is usually not considered a reasonable option at a time when security talent is difficult to find, hire, and retain. This is true for employees with the talent to perform penetration testing or comparable tasks.[11] This ROI analysis thus does not consider internal employee productivity as a quantitative budget reduction factor. However, readers may choose to add this to their own ROI calculations.

Finally, we should mention risk reduction – namely, the overall lessening of the potential for attack by performing continuous security validation with an automated platform. The general benefits will tend to pervade all aspects of an organization's risk profile, and the overall quantitative benefits might be difficult to pinpoint in an ROI calculation. In this ROI analysis, we take the conservative approach of reflecting and embedding the reduced likelihood of incidents as a reduction of incident response service expenses in the budget. Readers are welcome to add other risk reduction factors into their own ROI calculations.

Our approach has been to take a mostly conservative view for ROI factors. We have not incorporated potential benefits such as smoother audit processes, reduced burden during the cyber insurance acquisition process, and simplification of formal risk registers, which can reduce governance, risk, and compliance (GRC) costs. As evident from the two case studies below, even without inclusion of these additional benefits, a significant ROI is still demonstrated.

CASE STUDY: MIDSIZED BANK

The first use-case involves a hypothetical midsized bank, one that is perhaps serving a community (in contrast to a larger global bank), and that maintains a modest-sized security team protecting assets on the order of USD $5B.[12] We can assume that this team engages an annual penetration test using an external consultant and that it employs a typical security architecture to deal with compliance and avoidance of threats such as ransomware.

We assume that the security team for this bank includes eight employees and two contractors, and that the budget for security includes use of Microsoft E3 and additional security tools for governance, risk, and compliance (GRC), identity and access management (IAM), use of an external managed security service (MSS), and engagement in annual incident response costs with the reasonable expectation that at least one meaningful security event occurs annually.[13]

The security financials associated with such a familiar midsized banking scenario would include costs for security staff, which we assume to have an annual loaded cost per headcount (employees and contractors) of USD $200K, as well as costs in each of the three categories listed above – namely, consulting, security services, and security platforms. These costs are sketched below – and we reference typical vendors one might expect in this environment.[14]

Annual Security Budget Line Items	Annual Operating Expense (USD)	Rationale
Staff Salaries (8 FTE @ $200K per annum)	**$1,600,000**	**Team supporting day-to-day security tasks (including CISO)**
Contractor Fees (2 FTE) @ $200K per annum)	**$400,000**	**Additional staff supporting day-to-day security tasks (contracted)**
Platform Expenses	**$2,500,000**	**Deployed security platforms for premise and cloud**
CrowdStrike EDR	$500,000	Protection for endpoints
Microsoft E3	$500,000	Basic security services including email and data security
MetricStream GRC	$500,000	Compliance and risk support
Okta IAM	$500,000	IAM and authentication
Additional Miscellaneous	$500,000	Various additional platforms and tools (e.g. awareness)
Service Expenses	**$1,400,000**	**Security services externally contracted**
Managed Detection and Response (MDR)	$700,000	Proves support for FW, MDR, SOC, SEIM
On-Demand Incident Response Services	$300,000	Based on estimated response support for one major incident per year
Penetration Test (Manual)	$150,000	Annual engagement with an external tester to run a pen test
Additional Miscellaneous	$250,000	Subscriptions and security assessments
Total Annual Security Operating Budget	**$5,900,000**	**Total annual security expenditure**

Figure 3. Security Costs for Midsized Bank Before Use of Pentera

If this midsized bank were to select Pentera to provide continuous security validation and test, we can reasonably expect the bank's annual security financials to improve, reflecting the quantitative benefits which mostly come from (1) the reduction in need to engage an external penetration test,[15] (2) the reduction of one contractor, and (3) the reduced likelihood of an in-year incident, thus resulting in the ability to reduce the security incident service budget and associated incident-related external consulting costs. These new costs are sketched below.[16]

Annual Security Budget Line Items	Annual Operating Expense (USD)	Rationale
Staff Salaries (8 FTE @ $200K per annum)	**$1,600,000**	**Team supporting day-to-day security tasks (including CISO)**
Contractor Fees (1 FTE) @ $200K per annum)	**$200,000**	**Additional staff supporting day-to-day security tasks (contracted)**
Platform Expenses	**$2,600,000**	**Deployed security platforms for premise and cloud**
CrowdStrike EDR	$500,000	Protection for endpoints
Microsoft E3	$500,000	Basic security services including email and data security
MetricStream GRC	$500,000	Compliance and risk support
Otka IAM	$500,000	IAM and authentication
Pentera Platform	$100,000	Continuous security validation
Additional Miscellaneous	$500,000	Various additional platforms and tools (e.g. awareness)
Service Expenses	**$975,000**	**Security services externally contracted**
Managed Detection and Response (MDR)	$700,000	Proves support for FW, MDR, SOC, SEIM
On-Demand Incident Response Services	$75,000	Reduced response support - reduced based on lower probability of events
Additional Miscellaneous	$200,000	Subscriptions and security assessments - reduced need for ext. assessment
Total Annual Security Operating Budget	**$5,375,000**	**Total annual security expenditure - $525,000 net savings (525% ROI)**

Figure 4. Security Costs for Midsized Bank After Use of Pentera

The reduction in cost factors here is based entirely on our TAG analyst participation in such exercises as CISOs, our day-to-day work with roughly 120 different CISO-led teams where we review security product and service portfolios routinely, and our discussions with customers of Pentera who share (anonymously) their experiences with these types of budget impacts based on improved security control validation.

An expenditure of $100K for Pentera (again, just a representative number used for this example) thus results in an overall reduction in the CIO's operating budget. Specifically, if we observe that this $100K increase in the budget for Pentera results in an aggregate $525K drop in total expenses, then the investment produces a 525% quantitative ROI measured against the original budget.

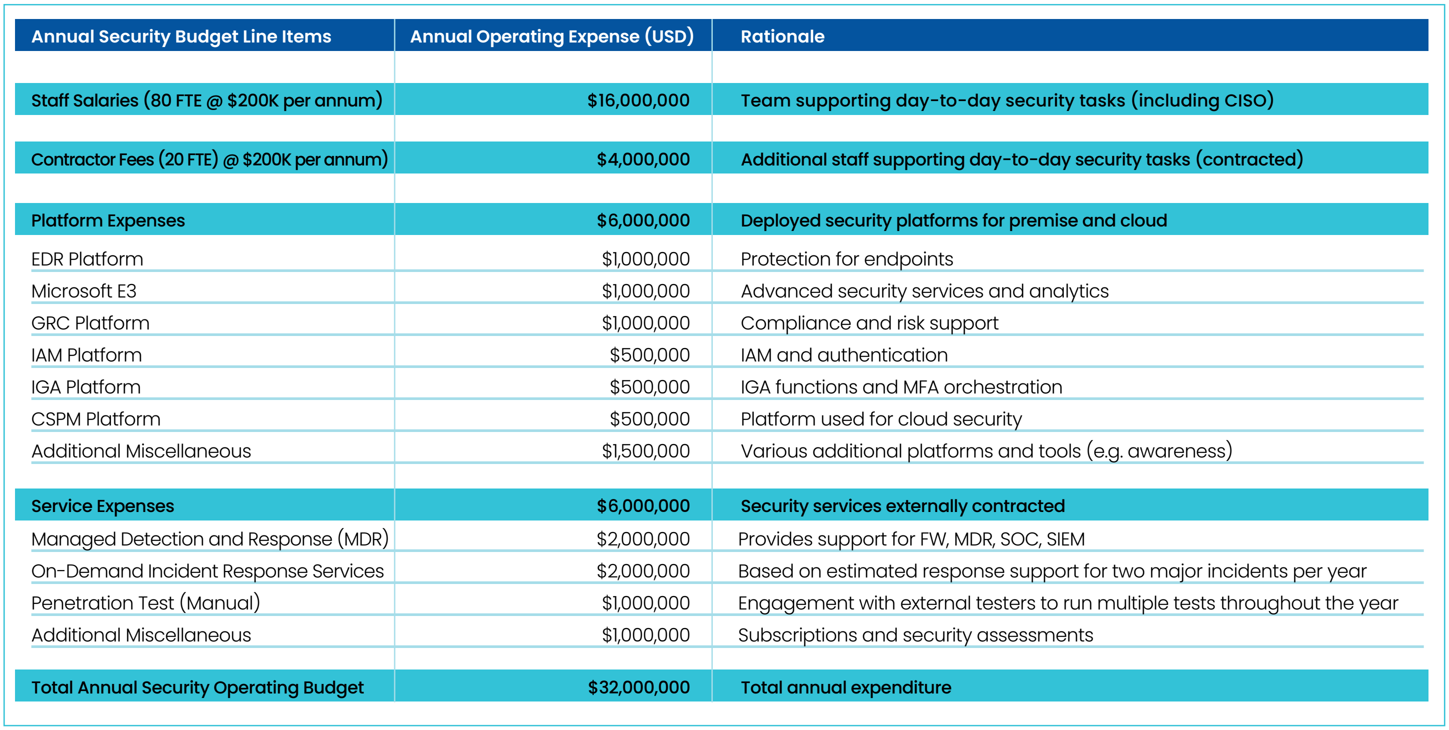
CASE STUDY: LARGE MANUFACTURING COMPANY

The second use-case involves a hypothetical large sized manufacturing company, one that is perhaps operating as a global entity, and that maintains a well-staffed security team. We can assume that this team also engages internal penetration test resources and that it employs a best-in-class security architecture to deal with regulatory compliance and avoidance of serious threats such as ransomware and nation-state exploits.

We assume that the security team includes eighty employees and twenty contractors, and that the budget for security includes Microsoft E5 as well as many additional security platforms supporting governance, risk, and compliance (GRC), identity and access management (IAM), use of an external managed security service (MSS), and engagement in annual incident response costs with the expectation that at least two meaningful security events occur annually.[17]

The financials associated with this large organization include $20M in employee and contractor expenses, which suggests that many tasks are being done by individuals perhaps using home-grown or open-source tools that would not show up on an income statement. The budget also includes $12M in platform and services expense which seems typical for a large manufacturing company assumed to have around $20B in revenue.[18]

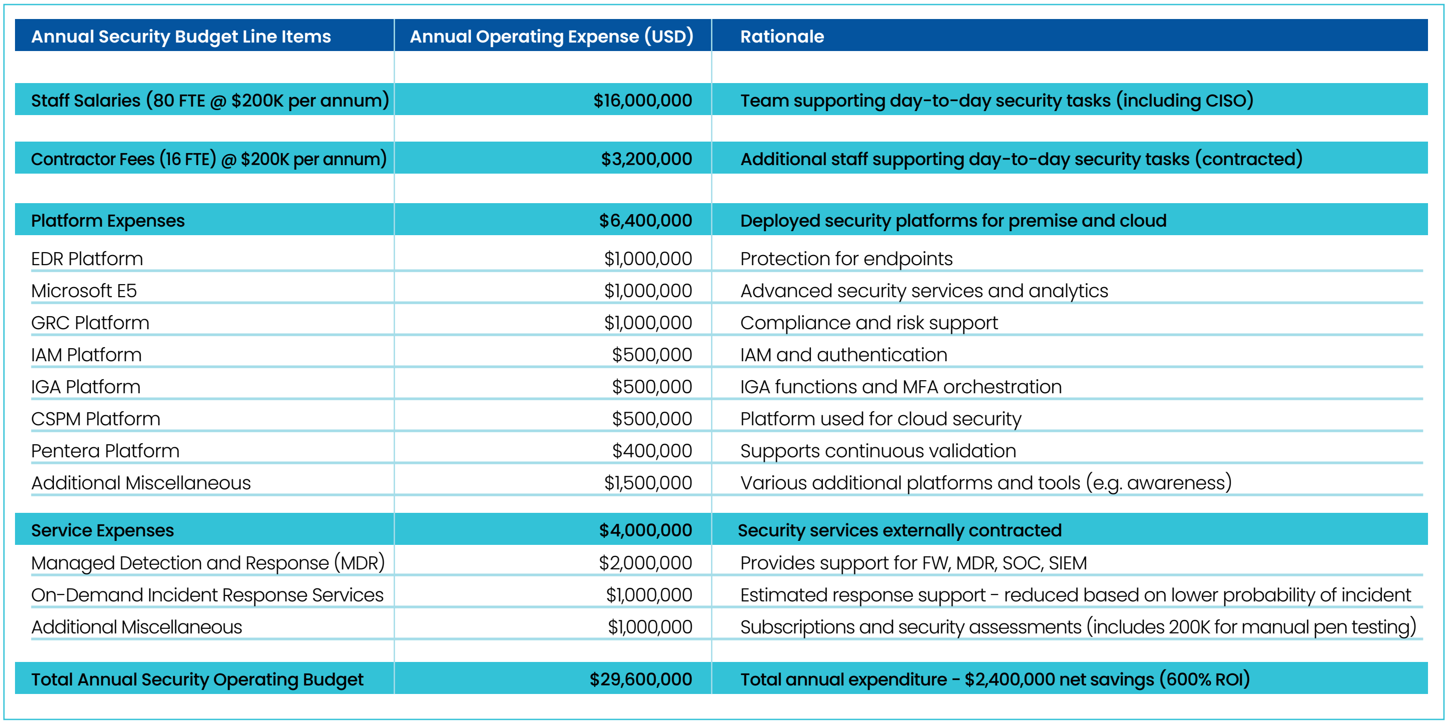
The security financials associated with such a large manufacturing company scenario would include costs for employee staff, which we assume to have an annual loaded cost per headcount (employees and contractors) of USD $200K, as well as costs in each of the three categories used in the prior use case example – namely, consulting, security services (including response), and security platforms. These costs are sketched following.



Annual Security Budget Line Items	Annual Operating Expense (USD)	Rationale
Staff Salaries (80 FTE @ $200K per annum)	**$16,000,000**	**Team supporting day-to-day security tasks (including CISO)**
Contractor Fees (20 FTE) @ $200K per annum)	**$4,000,000**	**Additional staff supporting day-to-day security tasks (contracted)**
Platform Expenses	**$6,000,000**	**Deployed security platforms for premise and cloud**
EDR Platform	$1,000,000	Protection for endpoints
Microsoft E3	$1,000,000	Advanced security services and analytics
GRC Platform	$1,000,000	Compliance and risk support
IAM Platform	$500,000	IAM and authentication
IGA Platform	$500,000	IGA functions and MFA orchestration
CSPM Platform	$500,000	Platform used for cloud security
Additional Miscellaneous	$1,500,000	Various additional platforms and tools (e.g. awareness)
Service Expenses	**$6,000,000**	**Security services externally contracted**
Managed Detection and Response (MDR)	$2,000,000	Provides support for FW, MDR, SOC, SIEM
On-Demand Incident Response Services	$2,000,000	Based on estimated response support for two major incidents per year
Penetration Test (Manual)	$1,000,000	Engagement with external testers to run multiple tests throughout the year
Additional Miscellaneous	$1,000,000	Subscriptions and security assessments
Total Annual Security Operating Budget	**$32,000,000**	**Total annual expenditure**

Figure 5. Security Costs for Large Manufacturing Company Before Use of Pentera

If this large organization were to select Pentera for continuous security validation and test implementation, then the quantitative impact would be considerable. As in our previous case, we can adjust the company's annual security financials and roughly calculate the quantitative benefit which comes from (1) the reduction in need to engage external penetration testing, (2) the reduction of four contractors, and (3) the reduced likelihood of incidents by 50%, thus resulting reduction of security incident-related external service costs. These new costs are sketched below.



Annual Security Budget Line Items	Annual Operating Expense (USD)	Rationale
Staff Salaries (80 FTE @ $200K per annum)	**$16,000,000**	**Team supporting day-to-day security tasks (including CISO)**
Contractor Fees (16 FTE) @ $200K per annum)	**$3,200,000**	**Additional staff supporting day-to-day security tasks (contracted)**
Platform Expenses	**$6,400,000**	**Deployed security platforms for premise and cloud**
EDR Platform	$1,000,000	Protection for endpoints
Microsoft E5	$1,000,000	Advanced security services and analytics
GRC Platform	$1,000,000	Compliance and risk support
IAM Platform	$500,000	IAM and authentication
IGA Platform	$500,000	IGA functions and MFA orchestration
CSPM Platform	$500,000	Platform used for cloud security
Pentera Platform	$400,000	Supports continuous validation
Additional Miscellaneous	$1,500,000	Various additional platforms and tools (e.g. awareness)
Service Expenses	**$4,000,000**	**Security services externally contracted**
Managed Detection and Response (MDR)	$2,000,000	Provides support for FW, MDR, SOC, SIEM
On-Demand Incident Response Services	$1,000,000	Estimated response support - reduced based on lower probability of incident
Additional Miscellaneous	$1,000,000	Subscriptions and security assessments (includes 200K for manual pen testing)
Total Annual Security Operating Budget	**$29,600,000**	**Total annual expenditure - $2,400,000 net savings (600% ROI)**

Figure 6. Security Costs for Large Manufacturing Company After Use of Pentera

The use of Pentera is thus shown to have the following impact: First, four contractors can be removed from the budget, resulting in $800K in savings; second, the probability of incident is cut in half, thus resulting in half the expected response costs in-year which saves $1M; and third, the reduced need for on-going external penetration testing and assessment services also saves $1M in costs per year – and this is not an unusual savings given the complexity of a larger organization.[19]

An investment of $400K in Pentera thus results in $2.4M in savings which represents a 600% ROI. The result is that the company's cybersecurity budget can be reduced from $32M to $29.6M based on an investment in Pentera. Obviously, this would be useful if the CISO is under pressure to reduce budget in the range of 8-10%. The clear preference from most practitioners would be to reinvest these savings into the program.

ACTION PLAN

The implication of our analysis is that buyers who find themselves in the pre-state described by our use-cases, and we assume this to be a common state, should review the qualitative and quantitative return estimates included in this report as a baseline for understanding the ROI impact from the use of Pentera. We understand that an interpretation of our generalized analysis will need to be done for the local environment and recommend that the local security team perform this task, optionally with the help of Pentera experts and ROI calculation tools.

If the returns appear to be relevant locally, our recommendation is to contact Pentera for discussion about a proof of value (POV) or other first steps toward selection, deployment, and use of the security validation platform. As always, TAG analysts are available to help Research as a Service (RaaS) customers with this and any other source selection analysis or decision process for security solutions such as from Pentera.

Footnotes

[1] TAG Infosphere is a New York City-based research and advisory firm founded by former AT&T senior executives, including Dr. Edward Amoroso, former AT&T Senior Vice President and Chief Information Security Officer (CISO). Since 2016, TAG has focused on the provision of expert insight and tailored guidance for practitioners in hundreds of enterprise teams, government agencies, and commercial vendors located around the world. TAG offers customer 24/7 access to a modern AI-powered SaaS platform that supports the need for on-demand detailed research and insights in cybersecurity and related areas including artificial intelligence. TAG has been developing ROIs since 2018.

[2] See https://pentera.io/ for more detailed and up to date information on the company history, management team, range of solution offerings, value proposition, and contact information for Pentera.

[3] This return on investment (ROI) report is the result of a collaborative review, assessment, and set of calculations between the Pentera and TAG teams. TAG performs ROI calculations on the best available commercial solutions in cyber, AI, and sustainability for which great confidence is achieved that the qualitative and quantitative benefits to users are meaningful and confirmed through feedback from live customers.

[4] TAG provides research and advisory assistance and support to many of these venture capital firms and can confirm the considerable due diligence review and attention that are driven by these organizations in advance of making any investment in a cybersecurity startup company.

[5] Additional information about Pentera's funding strategy is available from several different public articles and press releases including this one from Reuters: https://www.reuters.com/markets/us/israeli-security-startup-pentera-raises-150-mln-funding-round-eyes-ipo-2022-01-11/.

[6] Detailed description of the Pentera platform is beyond the scope of this ROI report, but inclusion of a high-level diagram of the functions supported will help readers understand the types of qualitative and quantitative benefits that come from deployment of this type of continuous security validation solution. Readers are encouraged to review the Pentera website (https://www.pentera.io/) for more detailed information including video and written materials that describe how the platform works.

[7] TAG works on an on-going and daily basis with roughly 100 different enterprise and government teams supporting the research and advisory needs for cybersecurity protection of their infrastructure. This practitioner community extends to research and advisory support at TAG for vendors which also often includes assistance to their CISO. Recent new rulings from the US Securities and Exchange Commission (SEC) have increased the need for CISOs to engage expert assistance and coaching from experts. TAG provides exactly that type of personalized assistance via former CISO practitioners team members. To that end, we are involved in the rationalization of dozens of annual security budgets including providing expert assistance in the selection of tools and platforms, as well as identification of strategies for dealing with budget cuts.

[8] This recently posted video interview from the lead author of this ROI report with a senior executive expert from a leading insurance broker covers this topic in some detail: https://www.youtube.com/watch?v=PfFdr_Jop5g. Pentera has reported cases where customers who provided proof of risk mitigation practices were able to obtain 20%-30% cybersecurity insurance premium reduction. While we recognize the quantitative benefit potential, we list this here as a qualitative benefit due to the constantly changing nature of the cyber insurance market.

[9] Our interpretation of security validation-related CISO budget includes those tools that are directly involved in testing, validating, and measuring the existence of exploitable vulnerabilities, holes, or bugs through a range of test cases – as well as to demonstrate that controls are either working sufficiently or can be bypassed. Traditional penetration testing, for example, is a main component of this budget.

[10] We choose to use the terms contractors and consultants synonymously, even though we recognize that practitioners might make some distinction. Staff augmentation is also a common term for what we imply to mean team members who work in a day-to-day setting but who are non-payroll staff working with employee staff.

[11] That said, a reduced workload on repetitive tasks that can be automated frees internal security experts to focus on more advanced use cases requiring human attention and creativity, an important benefit considering the shortage of talent.

[12] As part of the research for this ROI report, we spent time with a mid-sized financial services firm that uses Pentera, albeit one that processes considerable amounts of money. Their guidance in terms of validating our qualitative and quantitative assessments here were invaluable. Obviously, we maintain the confidentiality of the identities of all companies and individuals who participate in the research for these reports.

[13] We try here to make reasonable practical assumptions regarding the typical types of cybersecurity staffing, platforms, services, and tools that would be engaged for this use-case. This lead author spent time on the board of directors (independent director) of somewhat larger financial institution (M&T Bank), which helped to provide guidance on how a well-managed bank would typically allocate their security resources. We also reviewed industry reports such as IBM's Cost of a Data Breach (see https://www.ibm.com/reports/data-breach) which underscore the intensity of breach response. In many cases, the costs associated with a breach can be massive, which will obviously increase ROI of prevention.

[14] Readers will note that our analysis includes those costs of the security program for this mid-sized bank that are likely to be relevant to the use of Pentera. Certainly, there might be many additional program-related costs that are not listed here including administration, training, recruiting, and so on. Readers can easily adjust our numbers to include their own specific costs to achieve a more tailored assessment.

[15] As suggested above, we fully understand that in some cases, there might be some residual budget used to engage an external penetration tester – and for larger companies, this might be done internally. If readers expect to continue to engage such work, then they can make the local adjustment to the ROI calculation accordingly.

[16] We also include a small change ($50K reduction) in the security assessment services budget. We've found this to be a feasible option with the use of a continuous automated security validation platform that provides attack surface and vulnerability assessment capabilities like Pentera..

[17] We make this estimate based on experiences with TAG Research as a Service (RaaS) customers rather than based on any external reporting metrics such as with the US Securities and Exchange Commission (SEC). We expect that with new SEC reporting rules, that research teams such as ours at TAG will be able to utilize and trust metrics for external reporting to entities such as the SEC. For now, however researchers must use their practical experience and an estimate of two meaningful cyber events per year for a large manufacturing company seems justifiable.

[18] Readers will note that for this manufacturing company, we have not included any designation in the budget for operational technology (OT) security. Our observation is that the IT and OT budgets for security will eventually merge, but for most companies in this sector, that has not occurred. If readers choose to include OT security in the calculation, then this is an easy adjustment.

[19] Many organizations will choose to maintain some level of manual penetration testing, perhaps based on compliance or external pressure from customers. We believe that internal staff salary and security service budgets will more than compensate for this situation financially. It might be the case, for example, that 80-90% of the manual penetration testing before deployment of automated security validation need not be performed after use of the platform.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science.