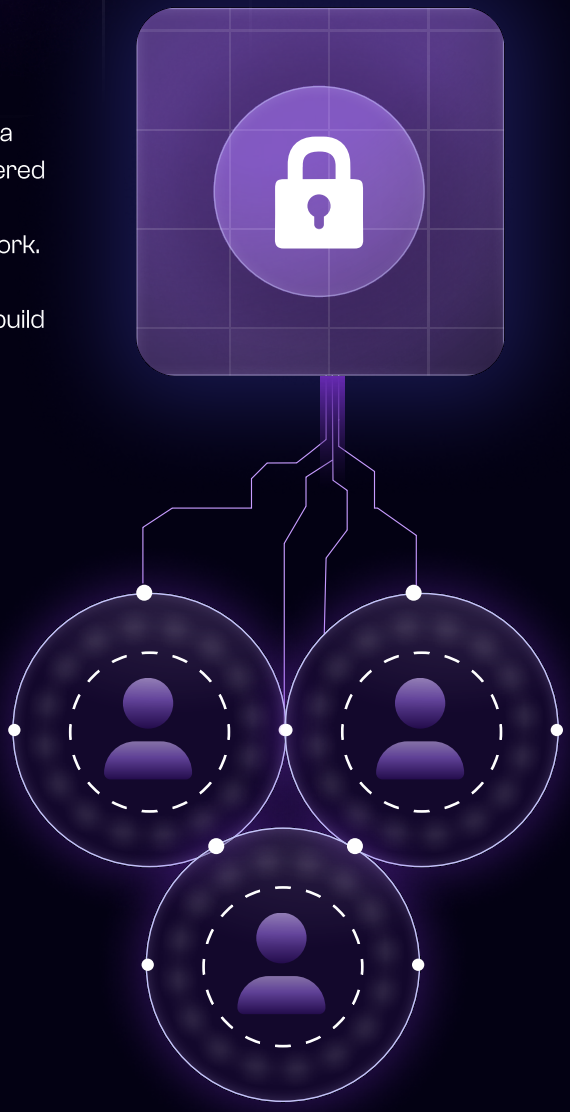
Anzenna

Mitigating Insider Risk through Unified Visibility and Remediation

Case Study: Anzenna & A Large Educational Institution in New York

Overview

A large educational institution in New York, operating over 50 schools, serves a community of more than 4,000 students and faculty. This organization partnered with Anzenna to achieve comprehensive security oversight, prompt incident response, and scalable risk management solutions across its expanding network. Anzenna's first of a kind Agentless AI solution enabled the institution to consolidate security insights, automate and streamline threat mitigation, and build a resilient security foundation.



50 Schools

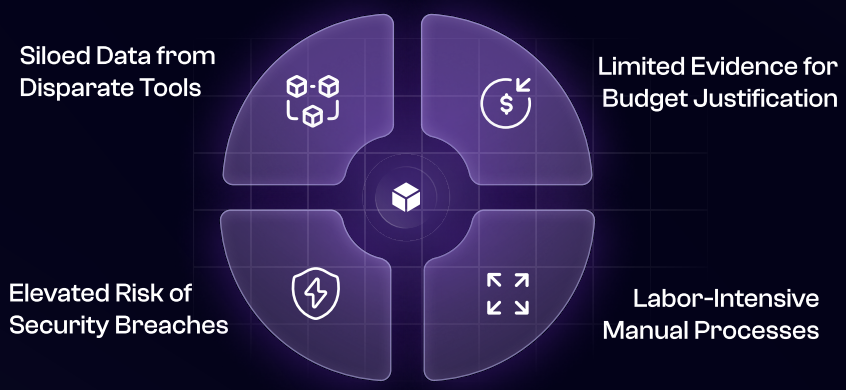
4000 Students & Faculty

Goal

The goal was to create a cohesive security environment with visibility across all systems, enabling the security team to respond effectively and justify ongoing investments in security infrastructure.

Customer Background

Focused on delivering high-quality education and ensuring student safety, this educational institution handles staff, student and other sensitive data daily. Maintaining a secure IT infrastructure is vital to protecting its community and supporting operational resilience. Before adopting Anzenna, the institution faced challenges with fragmented data insights and limited ability to act on security threats proactively. To add, a relatively small security team needed the ability to efficiently detect, investigate and respond to security threats.



Challenges and Pain Points

Siloed Data from Disparate Tools

Security information was distributed across multiple tools, each providing a narrow view of potential threats. This fragmentation made it difficult to gain a complete picture of vulnerabilities, limiting the ability to detect and respond to threats efficiently. The lack of a unified system contributed to critical blind spots in the institution's security posture. They also did not understand insider risk for each school in the district and Anzenna provided them visibility on that aspect.

@douglaskim850@gmail.com

Limited Evidence for Budget Justification

Supporting budget requests for security investments required data-driven insights into vulnerabilities and incident trends. The fragmented nature of the data, however, made it challenging for the Security team to present a compelling case to stakeholders, resulting in budget constraints that affected the institution's ability to proactively address risks.

Elevated Risk of Security Breaches

Without centralized oversight, the institution struggled to identify, prioritize and address vulnerabilities across its network. The disjointed approach heightened the probability of toxic combinations leading to undetected security breaches.

Labor-Intensive Manual Processes

The institution relied heavily on manual processes to gather insights from various security tools. This method was both time-consuming and prone to delays, restricting the IT team's capacity to respond to threats effectively and diverting attention from high-priority tasks.

The Anzenna Solution

Unified Insider Risk Security Dashboard

Anzenna provided a consolidated and enriched view single pane of glass, consolidating data from all security and IT tools into a single prioritized dashboard. This centralization enabled the security team to monitor and address threats in real-time, significantly enhancing visibility across the institution's network

Efficiency Gains without Added Headcount

By automating data gathering, prioritization and reporting, Anzenna eliminated the need for additional staff to manage security monitoring. This automation freed up valuable resources, allowing the team to focus on strategic initiatives rather than routine data aggregation.

Automated Threat Detection and Response

The platform's capabilities extended beyond data aggregation, allowing the Security team to proactively address specific vulnerabilities. For instance, Anzenna identified 228 risky applications installed on employee devices, enabling swift removal and significantly improving device security.

Enhanced Budget Justification with Detailed Reporting

Anzenna's reporting features provided clear, data-backed insights into the institution's security needs. Armed with robust metrics, the security team successfully secured a 20% increase in budget allocation for cybersecurity, further strengthening their ability to prevent and respond to threats.

228

Identified Risky Applications

20%

Secured Increase Budget

Results and Outcomes

Incident Frequency Reduced by 30%

By proactively identifying and addressing vulnerabilities, the institution achieved a 30% reduction in risky insiders that could have resulted in social engineering attacks. This decrease highlighted the effectiveness of Anzenna in providing real-time, actionable insights that allowed the Security team to mitigate threats before they escalated.

Operational Time Savings

The automation of data collection reduced the need for manual monitoring by 25%, giving Securitystaff more time to concentrate on critical security initiatives. This operational efficiency allowed the team to shift its focus from data aggregation to proactive risk management.

Detailed Results of Risky Application Management

Identified and remediated 228 applications across employee devices that posed significant security risks. This insight allowed the institution to act immediately, removing these high-risk applications with a single click and reducing the potential for security breaches related to device compliance.

Streamlined Response with 40% Faster Resolution

Anzenna's platform enabled a 40% decrease in response times by removing redundancies and allowing Securitystaff to focus on validated, high-priority risks. This streamlined approach led to more accurate responses, with a 50% reduction in false positives

Successful Budget Justification through Comprehensive Reporting

With clear, data-backed insights into security vulnerabilities, the Securityteam effectively advocated for increased funding. This led to a 20% budget increase, ensuring the institution had the resources necessary to enhance its cybersecurity framework.

30%
Reduction in risky insiders

25%
Reduced need for manual monitoring

40%
Decrease in response times

Conclusion and Future Impact

The institution's partnership with Anzenna marked a transformative step in its security journey. By consolidating security insights, streamlining workflows, and enabling proactive threat management, the institution has established a strong foundation for ongoing protection.

The collaborative approach has allowed the institution to maintain a secure learning environment, safeguarding students and staff while ensuring scalable, sustainable security management.Anzenna continues to work closely with the institution to refine its security processes, supporting long-term resilience and adaptability in the face of evolving threats. This partnership exemplifies how educational institutions can leverage unified security solutions to manage complex environments effectively and safeguard their communities.