Cy-Quest Security Platform

An all-in-one platform that protects your organization against the latest threats

The increasingly treacherous and sophisticated cybersecurity landscape puts businesses of every size at risk. Spurred by lucrative ransom payouts over the last few years, many criminal organizations modernized their operations, resulting in the growth of a sophisticated underground market with products and tools anyone can purchase to execute a cyberattack.

Financial gain is at the root of these changing dynamics. Cybercriminals have many ways to monetize their efforts, which makes any business an attractive target. They can demand a ransom, sell information and access to the highest bidder, re-route payments without a trace, and so much more.

The costs for a business extend far beyond the initial hard costs of a breach. Following a cyber incident, businesses are hit by dozens of additional impacts from reputation damage and operational downtime to legal fees and lost customers.

To defend our clients in this environment, we leverage an all-in-one platform that checks the box for each item listed in in the "What Makes for Effective Cybersecurity?" column to the right, providing every business with:

- A mature Zero Trust security architecture thats quick and easy to deploy
- A comprehensive security program with one platform and one agent, with each solution purposefully integrated to eliminate security system complexity
- Advanced AI and ML to identify, prevent, and detect threats faster
- A team of highly trained security analysts to overcome the security skill shortage

Benefits

Defense-in-Depth Security
Our platform makes it easy to implement a comprehensive, highly effective security program that spans prevention, detection, and response

Unparalleled Visibility and Control
Our platform helps us see everything that's occurring across security and technology stacks while gaining granular control over your security program and user experience

Levels the Playing Field
Our platform brings enterprise-leading capabilities to small businesses and mid-market companies, purpose-built for their needs

What Makes for Effective Cybersecurity?

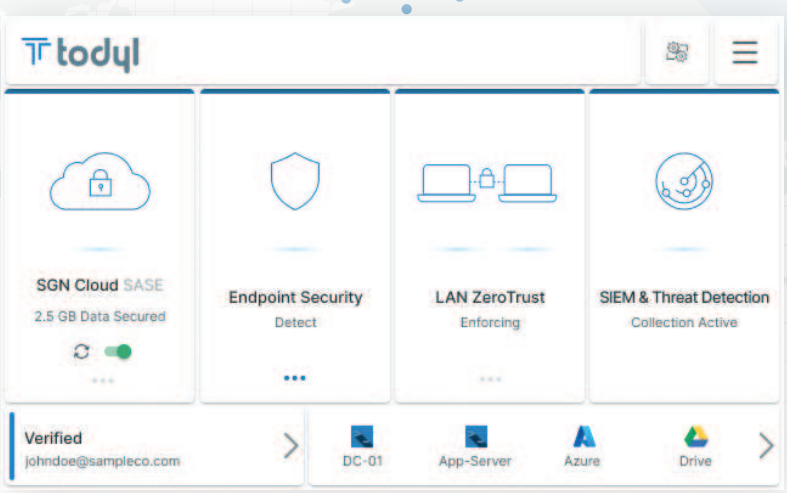
According to the 2022 IBM Cost of a Data Breach Report, there are several factors that significantly reduce the cost of a breach that are critical in a cybersecurity program, including:

Zero Trust Security
Adoption of Zero Trust drove a 20.5% reduction in cost of a breach. More mature Zero Trust adoption increases the cost reduction to 35.9%

Simple Security Systems
The more complex the security system, the greater the cost of a breach. A highly complex system with multiple products and tools, significant management overhead, and integration challenges can increase the cost of a breach by up to 58%

Artificial Intelligence (AI)
AI platforms help reduce the cost of a breach by up to 55.3% through faster identification and rapid remediation of threats

Security Expertise
A lack of security talent drove a 12.8% increase in the cost of a data breach



Capabilities the Todyl Security Platform Delivers

Our all-in-one platform eliminates the complexity, cost, and challenges of managing dozens of products and tools while providing highly effective, comprehensive security. It unifies best-in-class cybersecurity technology into a platform purpose-built for the needs of small businesses and mid-market companies. Each capability was carefully designed to interoperate for maximum efficiency and effectiveness. It's also highly customizable, allowing you to pick and choose the security capabilities you need aligned to your budget.

SASE (Secure Access Service Edge)

Combine networking and security in the cloud to deliver Zero Trust Network Access (ZTNA) and low latency, secure connections to any resource, regardless of where users connect

Cloud Managed SIEM (Security Information and Event Management)

Gain unprecedented visibility across endpoint, user, network, and cloud for real-time, correlated threat detection, investigation, and response

Endpoint Security (EDR+NGAV)

Unify NGAV and EDR to secure endpoints with cutting-edge ransomware, malware, malicious behavior, and memory threat protection

MXDR (Managed Extended Detection & Response)

Eliminate threats faster with a named account manager, monthly updates, direct lines of communications, and a 24×7 managed SOC providing customized threat hunting, prevention, detection, and response

GRC (Governance, Risk & Compliance)

Take charge of compliance and identify opportunities to strengthen security postures with real-time visibility

LAN Zero Trust (LZT)

Stop the spread of threats like ransomware and APTs while securing internal networks with next-generation, user-aware network access control

Contact us today at 210-761-3332 to learn how our all-in-one platform can protect your business from the latest threats, so you can focus on your business.