



DynTek's Enterprise Security Solution

Providing end-to-end security & automation for the borderless environment

In the past, businesses looking to secure their IT environments could easily box in their network to protect it from outside threats. With the overwhelming migration to cloud applications and open access, this has become impossible. Networks no longer have edges so the security approach must be borderless as well. That's why more than eight out of 10 companies want an integrated security portfolio.

Once an attacker establishes a beachhead on your network, it takes about two hours on average to move laterally and dig into the deeper elements of your infrastructure and wreak havoc. Containing the attack within the first hours significantly increases overall security and minimizes the outside threat. That requires a robust security strategy that encompasses all aspects of your network.

The DynTek Solution

DynTek helps you design your security system using an "assumed breach" approach focused on identity and access – the pillars of a dynamic, effective threat defense. This type of security architecture is built around the key elements of your IT environment – end points, systems, and data. Gaining visibility into each of these components and understanding how they influence each other is the key to developing a cohesive security fabric around your entire infrastructure.

There are now over 2,000 cybersecurity companies on the market. However, using multiple layered security products doesn't result in more security. A typical enterprise can generate close to 200,000 alerts every week, but lack of resources results in less than 10 percent of those actually being reviewed in most organizations. That means 90 percent of organizations miss most of what is happening in its network.

That's why a conglomeration of separate applications is ineffective in protecting your organization. You need an integrated security platform to fully address the widespread threats to your business.

DynTek's strategic approach aligns and integrates the most advanced security controls to produce actionable intelligence in real time to enable enhanced protection, containment, and remediation. Our executive level security experts help you assess your security posture and risk, build a comprehensive security architecture, and optimize technology solutions.

Our Security Solution Engagement Approach

Each of our solutions is built on four main values:



Establish an in-depth understanding of your business



Design and develop with a customer-first attitude



Execute with our experienced, expert staff



Build on a security-first architecture foundation



KEY BENEFITS:

- ✔ Peace of Mind with 24/7/365 Coverage
- ✔ Security Subject Matter Experts On-Demand for Rapid Escalation
- ✔ Faster Response Time
- ✔ Meaningful Incident Data
- ✔ Increased Accuracy and Lower Rate of False Positives
- ✔ Near Real-Time Alerting
- ✔ Cloud-hosted Solution, Easy Implementation

Our engagements include extensive strategic consulting, assessments, planning and architecture development, product vetting and recommendation, proof-of-concept, implementation, migration, optimization, and a comprehensive support program.

Our deployments include training, technical and operational support, and staff as needed. Every solution can be implemented in the way that best fits your organizational needs—on-premises, hybrid, or cloud-based.



DYNTTEK
DYNAMIC TECHNOLOGY SOLUTIONS

Our Security Offerings

+ LEGAL AND REGULATORY

- + **Compliance:** PCI, SOX, HIPAA/ HITECH, FFIEC, NY DFS, NIST SP-800s | NIST CSF
- + **Privacy:** EU GDPR, CCPA, ISO 27018: Protecting PII in the Cloud
- + **Audit:** SOC2, SSAE 16, NIST SP500-53A, ISO 27001, FISMA, FedRAMP
- + **Investigations:** eDiscovery & Forensics

+ RISK MANAGEMENT

- + Governance and Strategy Development
- + Three Line Defense
- + Security Strategy Roadmap
- + Risk Assessments
- + Vendor and Supply Chain Risk Management
- + Disaster Recovery and Business Continuity Planning
- + Policies, Procedures, and Risk Treatment

+ DATA SECURITY

- + Data Classification
- + Data Protection Strategy
- + Risk Mitigation
- + Technical Infrastructure Design, Data Mapping and Protection

+ THREAT MANAGEMENT

- + Threat Surface Reduction
- + User Awareness Training
- + Vulnerability Assessment
- + Network and Application Penetration Testing
- + Malware Analysis and SOC Services



+ SECURITY SOLUTIONS

- + Network Segmentation
- + Firewalls
- + Advanced Endpoint Protection
- + Endpoint Detection and Response
- + Intrusion Detection and Prevention
- + Autonomous Response
- + Vulnerability Management
- + Network Access Control
- + Security Orchestration, Automation, and Response (SOAR)
- + Mail Security
- + DNS Security
- + IOT Security
- + ICS/SCADA Security
- + Cloud Access Security Broker
- + Privileged Access Management
- + Application Security/Secure Code Review
- + Data Loss Prevention
- + Identity and Access Management

+ SECURITY OPERATIONS

ADVISORY SERVICES

- + **Incident Response:** Compromise and Readiness Assessment
- + **Network Security Monitor:** SIEM and Log Management, High Value Indicators
- + **Threat Intelligence:** Threat Sources, Hunting, and Adversarial Actor Correlation
- + **Forensics:** Management and Analysis
- + **Command Center:** Legal Notification and Internal/External Reporting
- + **Self-Assessment:** Configuration Monitoring, Threat Modeling and Tabletop Exercises

+ DYNTEK SOC OFFERINGS

- + Advanced Internet IDS/IPS Monitoring & Alerting
- + Email + End Point Security Monitoring & Management
- + Threat Intelligence and Analytics
- + Mitigation and Remediation
- + Incident Response
- + Forensics