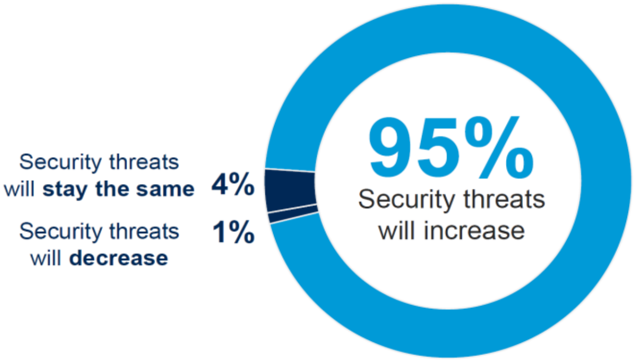
Calance

Calance Information Security Services

Custom fit solutions for an off-the-rack price.

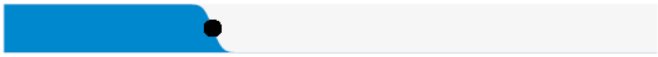
Security Trends



In response to a Gartner survey, 95% of respondents believed that cybersecurity

56% of breaches took months or longer to discover

32% of breaches involved phishing



$3,533 / employee

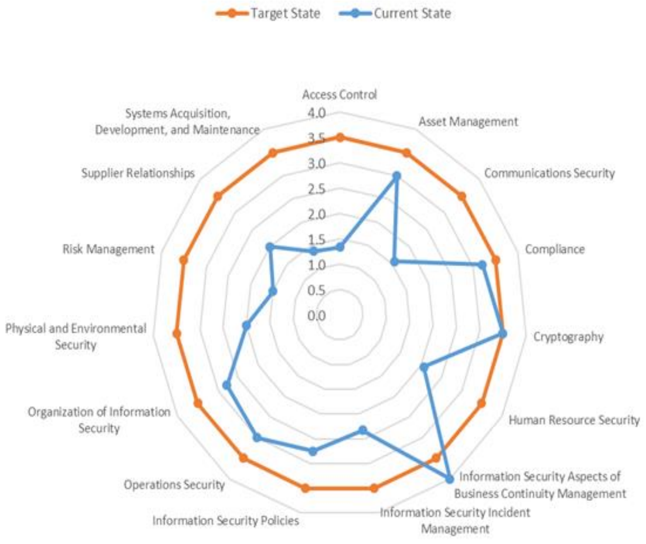
The average breach costs at organization with 500-1,000 employees

Primary Services

- Consulting & Advisory
- SETaaS
- Security Strategy
- Maturity Assessment
- Analytics & Metrics
- Managed Detection & Response (MDR)
- SOCaaS
- Executive Scorecards
- Policy & Standards Development
- Audit & Compliance

Top Technology Partners

ARCTIC WOLF CROWDSTRIKE vmware Microsoft Google Cloud aws SAP solarwinds



Security Consulting & Advisory

Calance has developed a proprietary Information Security Framework specifically designed for small to mid-sized enterprises. The foundations are based on industry leading NIST CSF and ISO 270001 frameworks and determines when your current state is and where you should be.

Managed Detection & Response (MDR)

Providing a dynamic combination of world-class Security Engineers, advanced machine learning, and comprehensive, real-time, threat intelligence. This service combines Security SME & SOC Engineers, 24x7 MDR, Behavioral Analytics, Compliance & Audit Assistance, Vulnerability Scans, and Log Analysis with Machine Learning to proactively protect your business. Our MDR Service benefits include:

- Calance Security Engineer as a single point of contact & can answer your security questions
- SOC based in US
- Comprehensive unified security with centralized view based on proprietary SIEM
- 24x7x365 Managed Detection & Response
- Predictable Pricing with Unlimited Data & Unlimited Logs
- Monitoring capability for both on-premises and cloud resources with virtual and physical sensors

Managed Security Awareness Training & Phishing Simulation (SETaaS)

Helping prepare employees for Phishing and social engineering attacks to create a human firewall. The program is designed to deliver on-demand, interactive, and engaging online training combined with unlimited simulated social engineering attacks through email, phone and text. Training your team on Phishing threats is necessary because:

- Users are unaware of the internet dangers and get tricked by social engineering to click on a malicious link in a phishing email or opening an email attachment they did not ask for.
- Employees have a false sense of security and believe their anti-virus has them covered. With the firehose of spam and malicious email that attack your network, 10-15% make it past your filters.
- Backups sometimes don’t work or it takes days to restore a system.

5 Questions to Get Started

1. Would you know if you had a security breach? Do you know if you have been attacked?
2. Who at your organization is responsible in the event of a security incident?
3. Who is accountable for your organization’s Information Security?
4. What information security risks do you currently have?
5. Do you provide Security Awareness training to your employees? Have you tested them with a simulated Phishing attack?

connect@calance.com | calance.com | 714-736-4332