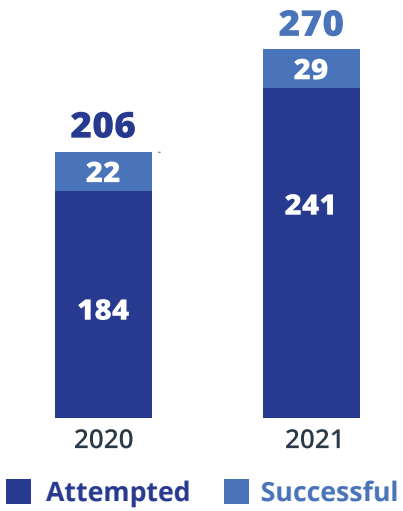
THREATQUOTIENT™

ThreatQ for Technology Companies

A large attack surface, early adoption of new technologies and a wealth of high-value data creates a perfect storm situation for technology organizations. Cybercriminals have multiple means and motivations to launch attacks. What's more, some technology companies, like managed service providers, cloud storage and service providers, and vendors of file-sharing solutions can serve as stepping stones into other enterprises and industries since they provide critical infrastructure to other organizations.

Despite their technology expertise and commitment to innovation, technology companies still fall victim to compromises and breaches. In fact, Accenture reported that tech companies experience numerous serious breaches — In 2021 there were just over 240 attempts with the success of those attempts just shy of 30 that got through[1]. When attacks are successful and data is stolen, the average total cost of a data breach for technology companies is now soaring towards $5 million — an increase of almost 2% over the previous year[2].

AVERAGE ATTACKS PER COMPANY[3]



KEY CHALLENGES

LARGE ATTACK SURFACES

Technology companies have a dual challenge of protecting their own infrastructure from cyberattacks as well as the products and services they provide to customers. Many rely on distributed operating models and cloud computing for business agility and competitive advantage. However, these models can create blind spots and security gaps that attackers use to their advantage. Compromises not only affect their immediate environment but can have dramatic ripple effects. Over the past few years, companies including LinkedIn, Facebook and Yahoo[4], to name a few, suffered attacks that affected users of their solutions. And in late May of 2023, MOVEit a managed file transfer (MFT) software company, discovered a zero-day vulnerability. MOVEit is used in the healthcare, finance, technology, and government industries[5]. Visibility across their entire infrastructure, as well as a proactive and anticipatory approach to security operations, will help high-tech companies strengthen defenses.

There were on average **270 attacks** (unauthorized access of data, applications, services, networks or devices) per company over the year, an **INCREASE OF 31%** compared with 2020[3].

EARLY TECHNOLOGY ADOPTERS

Many high-tech organizations are early adopters of new technologies and more willing to take business risks than their counterparts in other industries. Steeped in innovation, they and their employees are faster to adopt cutting-edge devices and applications as well as open technologies they may not be secure. Focused on collaboration, creativity and communication with teams that are often global, and frequently working under tight deadlines to outpace fierce competition, they sometimes prioritize speed and simplicity

over security. To close the security gaps these new technologies expose, they need insights into new threats as they emerge and an understanding of relevance to their organization to determine how to mitigate risk.

HIGH VALUE DATA

From intellectual property to employee and customer data, technology companies have a wealth of high-value information that is attractive to cybercriminals. Personally identifiable information (PII) including credit card information and employee records can be used for fraud or identity theft or resold to other threat actors. The average data breach cost per record has increased to $4.97M for technology companies — the fourth highest across industries and higher than the overall mean of $4.35M[6]. This includes the cost of detection and escalation, notification, post data breach response and lost business.[4] But this number can pale in comparison to instances when intellectual property (IP) such as trade secrets and unpublished patent applications are leaked, stolen or used by a competitor, putting a company's viability at risk. Technology companies need real-time knowledge of how adversaries and campaigns operate and the infrastructure used to accelerate response and prevention.

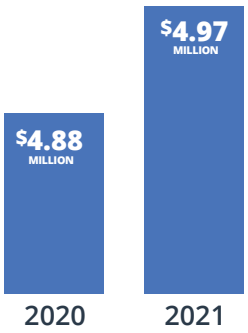
CREATING A LEADING DATA-DRIVEN SECURITY OPERATIONS

Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including critical infrastructure sectors, quickly.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external (e.g., IT-ISAC, OSINT) and internal (e.g., SIEM, EDR) threat intelligence and vulnerability data in a central repository
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities
- **PRIORITIZE** what matters most for the technology system environment
- **INTEGRATE** only relevant indicators into your security policies
- **PROACTIVELY HUNT** for malicious activity which may signal IP compromise, payment card fraud, compromise of solutions or services being sold to customers, and other harm to employees, customers and the business
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture
- **ACCELERATE ANALYSIS** and response to attacks against multiple targets including internal systems, emerging technologies and devices, solutions delivered to customers, and supporting infrastructure
- **AUTOMATICALLY** push threat intelligence to detection and response tools

AVERAGE COST OF A DATA BREACH IN THE TECHNOLOGY INDUSTRY[6]



> The average data breach cost per record has increased to **$4.97M** for technology companies — the fourth highest across industries and higher than the overall mean of $4.35M[6]

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

1. https://www.accenture.com/us-en/industries/high-tech-index
2. https://www.ibm.com/downloads/cas/3R8N1DZJ
3. https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40
4. https://www.zerofox.com/blog/top-5-industries-most-vulnerable-to-data-breaches-in-2023/
5. https://cyberint.com/blog/research/moveit-supply-chain-attack/
6. https://www.ibm.com/downloads/cas/3R8N1DZJ

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

TQ-IDB04-0823-02

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885