Managed Security Services

Security operations services for advanced enterprise protection

Protecting your business and critical information from a security breach is a full-time job that requires continuous daily efforts by experienced and certified cybersecurity professionals.

To ensure the integrity of your organization's private and confidential data, effective cyber technologies and policies must be deployed and monitored regularly. Maintaining your foundation of barriers such as anti-virus, next-gen firewalls, monitoring, and off-site data backups are just a few first steps in the front line of defense against the advanced persistent threat your organization faces today. Advanced threat and response services, delivered in partnership with Alert Logic, take security to the next level and include security experts who extend your team to improve detection and disrupt threats. Together, we accelerate your ability to respond so you can focus on your core business.

Attacks are becoming more complex over time

- Attacks are multi-stage using multiple threat vectors.
- The average time to identify a breach in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days.
- Data breaches in the U.S. average total cost of $8.19 million (more than double the global average).
- Breaches caused by a malicious attack are 27 percent more costly than breaches caused by human error.

Source: Ponemon 2019 Cost of a Security Breach

CBTS Cloud Portfolio

Cloud Consulting | Cloud Services | Cloud Infrastructure | Data Center | Data Protection

Fully managed monitoring and remediation

Managed security delivers the outcome that your business requires without putting an undue burden on your in-house IT department that may not have the security experience required. Taking a multi-layered resiliency approach can quickly and effectively protect your enterprise from compromise or loss against unwanted internal or external activity.

- Enable 24x7x365 security defense so that no matter when your enterprise comes under threat you are protected and trained, certified professionals will react quickly to contain and resolve the situation.
- By taking a multi-layered, in-depth approach, organizations can prevent many security breaches and in the event of an incident, quickly respond and vastly mitigate the overall impact to your business.

Avoid costly security infrastructure appliances, devices, and software that quickly become outdated and can require large capital deployments. Instead, evolve to an on-demand model for all of your security needs. Delivered as a service with a predictable monthly fee, security services are an essential feature that can be adopted as part of your managed cloud environment or as a stand-alone solution for remote infrastructure in your existing data center or third-party colocation facility.

Advanced security protection from the professionals

Rely on CBTS as your trusted security operations advisor, relieve yourself of the burden of limited resources to combat security breaches, and reduce your organization's risk with managed security services.

- Without expertise to identify threats and respond to attacks, organizations put their greatest assets at risk.
- Staying ahead of the security game is hard. IT resources struggle to identify, prioritize, and respond to threats because resources are stretched, and budgets are tight.
- It can be difficult for IT leaders to implement a threat detection strategy (lack of knowledge and disparate tools frustrate a comprehensive approach).

A higher level of managed IT security for a more advanced level of protection for your enterprise to defend against ever increasing sophisticated and malicious threats

Base level of security built into the foundation of fully managed CBTS cloud environments that are customized to each client's unique requirements

Security offering	What is included?
Security Assessments and Consulting Services	Access advanced security skill sets for customized and tailored security assessments and consulting services. The CBTS Secure Team has the proven experience and certifications to help you build a plan of resiliency for ongoing protection.
Threat Detection and Response with AlertLogic	Managed threat detection and response delivers a fully integrated end-to-end security solution from detection, response to remediation.
Security Analytics	Get a topology view of your environment and in-depth insights into activity, events and potential incidents.
Threat Risk Index	The Threat Risk Index is a personalized score across assets, networks, and deployments which allows you to track improvements over time.
Intrusion Prevention Service (IPS)	Intrusion prevention includes rule-based software or module on the firewall to defend against known malicious activity. Optional to fully managed cloud agreements.
Network Firewall	Essential base line network protection that accepts or denies traffic based on rules such as source and destination IP address. Included in fully managed cloud environments.
Patch Management	Protect against known vulnerabilities where CBTS will take accountability for patching your servers, network, and operating systems to ensure you are up to date. Included in fully managed hosting agreements.
Monitoring & Reporting	End-to-end network, servers, device, and OS layer monitoring and reporting that serves as an initial layer of tracking activity and making performance decisions. Included in fully managed hosting agreements.
Anti-Virus	CBTS will install and provide ongoing monitoring and system administration functions. Provides both virus and spyware protection (real-time protection). Included in fully managed hosting agreements.
Offsite Data Backup	Off-site data backup is essential in protecting against loss of data due to Ransomware with a second copy of your data that can be retrieved and restored back to your last safe point in time. Included in fully managed hosting agreements.
Multi-factor Authentication	Two Factor Authentication (2FA) requires an additional digital approval on your smartphone, on top of your logon username and password, to gain authorized access. By integrating two-factor authentication, attackers are unable to access your accounts without possessing your physical device needed to complete the second factor. Included in fully managed hosting agreements.