SECURITY MATTERS.
Protecting your critical infrastructure.
IT’S A MATTER OF SECURITY.

Your critical infrastructure is our priority. Opus Interactive brings two decades of standards and processes to proactively scan, identify, maintain, and protect your environment.

When it comes to security, you can never be too vigilant. Opus Interactive builds custom solutions for mission critical infrastructure used by enterprise and government customers. Security is top of mind from firewall to facility, with formal IT policies and procedures that set standards for physical security, logical access, computer operations, change control, and data communications.

CSO from IDG recently published ‘Top Cybersecurity Facts, Figures, and Statistics’ indicating that cyber crime and data breaches are on the rise. The article included a plethora of examples, including:

- **Average cost of a single cyber attack:** $5 million
- **25% of the cost of a single attack is attributable to system downtime:** $1.25 million
- **30% of the cost of a single attack is attributable to IT and end user productivity loss:** $1.5 million
- **Average time it takes to identify a data breach:** 191 days
- **Ransomware attacks increased by 36% in 2017**

We’ve spent over 20 years developing systems, processes and policies to protect our customers. From geographic location to facility to network to people, the Opus Interactive approach to security is comprehensive.

- Audits and Certifications
- Physical Security
- Network Security
- People Security

For more information, contact sales@opusinteractive.com.
AUDITS & CERTIFICATIONS

Named to CRN’s 2018 Tech Elite 250 List, Opus has been third-party audited and found compliant for HIPAA/HITECH Type 1 Soc 2, PCI-DSS Certified, and has over 20+ years of safeguards and protocols around Administrative, Physical, Technical and Organizational security. The Company is scheduled to attain FedRAMP Ready moderate compliance (316 unique controls) for the OpusCloud by May 2019.

- **PCI/DSS (186 unique security controls)** - The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data, with specific requirements surrounding: network, data, vulnerability management, access control, network monitoring and testing, and information security.

- **HIPAA (59 unique security controls)** – HIPAA administrative safeguards are a critical piece to the larger health data security puzzle that all covered entities must put together. The safeguards governing administrative, physical, and technical security are not only a federal requirement, but they all play an important role in ensuring that sensitive health data remains secure and out of the reach of unauthorized individuals.

- **SSAE 18 SOC 1 (88 unique security controls)** - focuses on a service organization’s controls that are likely to be relevant to an audit of a user entity’s (customer’s) financial statements.

- **SSAE 18 SOC 2 (42 unique security controls)** - addresses a service organization’s controls that relate to operations and compliance, as outlined by the AICPA’s Trust Services criteria in relation to availability, security, processing integrity, confidentiality and privacy.
PHYSICAL SECURITY

We operate from state-of-the-art facilities located in top data center markets carefully selected for their ability to deliver unprecedented levels of energy efficiency, security, and reliable connectivity. The result is optimized performance for your critical infrastructure with providers who have established reputations for delivering security and uptime.

Security protocols at Opus Interactives hand selected facilities include:

- Perimeter fencing
- Security gate with proximity badge reader
- Building perimeter security bollards
- 24x7x365 monitored, video surveillance of all entrances, building exterior, interior corridors and Data Room
- 24x7x365 on-site security staffing
- Security desk at customer entrance always manned
- Staff trained for operations, fire, & life safety incident response
- 8 badge swipes with 2-factor + multi-factor authentication to gain access to the cage level
- Multi-factor cabinet access

All entrances to data centers are restricted by authorized personnel. Controls in our Oregon datacenter are facilitated by Infomart staff and verified by reputable third-party organizations including USGBC (LEED GOLD), and Uptime Institute (M&O Rating). The facility was also selected as LinkedIn’s flagship facility for unprecedented sustainability and renewable energy benefits. Controls in our Virginia datacenter are facilitated by Iron Mountain staff and compliance includes FISMA High Rating, ISO 27001 & ISO 50001. Iron Mountain has over 65 years of operational excellence and provides services to over 100 Federal Agencies. The same is true for Databank in Dallas and Tata Communications in Portland, Oregon.
Opus has over 20 years of experience in building and maintaining critical environments, and the policies and protocols to ensure the ongoing safety of those environments. Our long-standing partnerships and supply chain ensure that our customers have access to the solutions and service they need when they need it. Our state-of-the-art equipment is architected to ensure optimized performance and scale without compromising security at any level.

To ensure utmost protection of your critical systems we’ve taken enhanced security protocols, including (but, not limited to):

- Patches and constant vigilance over updates and settings
- Firewall systems filter unauthorized network traffic
- Software restriction policies
- Advanced Intrusion Detection Systems
- Penetration testing
- Vulnerability scanning
- Block lists
- Antispam settings
- Load balancing
- Managed backup
- Business continuity and disaster recovery as a service
- Ongoing capacity monitoring utilizing the industry’s first end-to-end technology platform to conform to the U.S. government’s security and interoperability standards (DODIN APL)

Opus uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resource. Unique identification (ID) is assigned to each person with access to critical systems or software to ensure that each individual is uniquely accountable for their actions.
PEOPLE SECURITY

Many of our customers are in finance, healthcare, and government industries, so Opus is very selective in the hiring process to ensure that the people that are building and maintaining our customer’s critical data meet the skills, conduct and character to consistently deliver the quality of service that our customers can rely on – at the time of hire and ongoing.

Our team is made up of highly trained professionals that undergo a thorough recruitment, selection, and training process. Applicants that meet strict hiring criteria are invited to a kick off discussion to benchmark skills, certifications, experience, integrity, and alignment with company values. Selected candidates are invited to a second, more thorough, team interview to further gauge skillset and ability to become a high-performing multi-functional team member. This interview also includes review of 10 year work and education history.

Once a candidate is selected to join the OI team undergo additional screening prior to hire, including:

- Check references
- SSN trace
- Criminal database search and Criminal check by jurisdiction
- Nationwide Sex Offender Registry check
- Federal criminal database check
- Drug screening

Specialized training, certifications, exercises and learning are ongoing within the team. In short, your security is top priority.

For more information please contact Opus Interactive at sales@opusinteractive.com.

About Opus Interactive
Founded in 1996, Opus Interactive is a cloud, colocation, and IT services company based in Oregon. Our mission-critical IT services deliver end-to-end support for digital transformation. We’ve spent over 20 years building strong partnerships and honing a service mix that we deliver from Tier III datacenters located in Oregon, Texas, and Northern Virginia (FISMA high rated). A member of VMware and HPE partnership programs since 2005, Opus delivers custom solutions for: Cloud & IaaS, Colocation, DRaaS & Backup, Object Storage, VDI, Public Cloud Monitoring & Management services.
10 Steps to Securing Your Organization’s Critical Data

1. Identify Potential Risks to Your Organization
   - Assess risks to your organization’s information assets with the same vigor you would for legal, regulatory, financial or operational risks. To ensure success, communicate goals and the importance of maintaining security across internal teams and leadership. One person opening one wrong email can make all the difference, so making sure you have full internal support is key.

2. Network Security
   - Protect your networks from attack. Defend the network perimeter, filter out unauthorized access and malicious content. Monitor and test security controls.

3. User Education and Awareness
   - Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4. Malware Prevention
   - Produce relevant policies and establish anti-malware defenses across your organization.

5. Removable Media Controls
   - Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

6. Secure Configuration
   - Apply security patches and ensure the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

7. Managing User Privileges
   - Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

8. Incident Management

9. Monitoring
   - Produce relevant policies and establish anti-malware defenses across your organization.

10. Home and Mobile Working
    - Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.