STRENGTHEN YOUR FIRST LINE OF DEFENSE

The rate of change not only in threats but in the tools at our disposal, and the heightened demands of users, are pushing us to make changes at an alarming pace. A successful strategy for securing data and minimizing incident damage does not lose sight of traditional defenses and core infrastructure security controls. Continued investment in perimeter defense is like keeping your doors locked—some of the threats you face could bypass them, but why let them in without a fight?

- Next-Generation Firewall (NGFW)
- Intrusion Detection & Prevention Systems (IDS/IPS)
- Micro-Segmentation
- Distributed Denial of Service Defense (DDoS)
- Internet of Things (IoT) Security

SECURITY

INFRASTRUCTURE SECURITY

The perimeter as we knew it has dissolved. People are connecting to corporate networks wherever, whenever and however they choose. Organizations need to adapt to this reality to protect the integrity of their business and the financial well-being of their customers. Addressing the threats presented by mobile devices, cloud services and the Internet of Things (IoT) is a critical challenge.

OUR APPROACH TO INFRASTRUCTURE SECURITY

Sirius provides a deep understanding of organizational risks and vulnerabilities, as well as current threats and the most effective policies, processes and technologies to address them.

We help you with all aspects of core infrastructure security using agile architecture and a modern approach at the perimeter. Our recommendations are based on real-world experience and expertise gained in the field, as well as customized testing in our state-of-the-art Technology Enablement Center (TEC). We partner with world-class infrastructure security solution providers and work with you to select the right solution for your environment. Our professional services help you manage, optimize, secure and transform your business.
NEXT-GENERATION FIREWALL (NGFW)
Strengthen your defenses with NGFWs, the new standard-bearers for perimeter defense. NGFWs include not only firewall intrusion prevention and application control features, but also features to detect and protect against advanced malware. They help not only with traditional ingress monitoring but also with egress visibility, which is crucial in identifying breaches.

INTRUSION DETECTION & PREVENTION SYSTEMS (IDS/IPS)
Identify and mitigate both known and unknown (zero-day) attacks with IDS/IPS. Network intrusion detection and prevention systems inspect traffic that has passed through front-line devices such as firewalls, and identify anomalous behavior. They detect threats through a variety of methods that can include signatures, protocol anomaly detection, behavioral monitoring or heuristics, and can also block attacks.

MICRO-SEGMENTATION
Decrease network attack surfaces. Unlike VLANs, micro-segmentation enables granular partitioning of traffic and greater control over east-west or lateral communication that occurs between servers, bypassing perimeter-focused security tools. Security settings can be tailored to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted. If a device or workload moves, security policies and attributes move with it, and if a breach occurs, micro-segmentation limits attackers’ lateral movement, which is what they need to progress through the kill chain and steal critical data.

DDoS DEFENSE
Maintain business continuity and protect your business from DDoS attacks that are increasing in frequency, complexity and scale. DDoS mitigation solutions help to “drop” or “clean” network traffic that is meant to disrupt networks, servers and applications.

IOT SECURITY
Gain visibility into and control over the IoT devices on your network. We provide leading IoT security solutions that facilitate real-time asset discovery and control, enabling organizations to identify and manage the devices on their network. We also offer firewalls that can be used as enforcement mechanisms, and SIEM systems that can enhance monitoring and analytics. We help you bring the tools in your environment together to increase your ability to orchestrate visibility and response.

SIRIUS INFRASTRUCTURE SECURITY SERVICES

<table>
<thead>
<tr>
<th>Discover</th>
<th>Assess</th>
<th>Consult/Design</th>
<th>Architect/Implement</th>
<th>Optimize/Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Review</td>
<td>Network Access Controls Assessment</td>
<td>Secure Cloud Migration Strategy</td>
<td>Solution Design &amp; Deployment</td>
<td>Solution Optimization/ Tuning</td>
</tr>
<tr>
<td>IoT Workshop</td>
<td>DDoS Resiliency Assessment</td>
<td>Remediation Plan Creation</td>
<td>Network Access Controls</td>
<td>Managed Firewall</td>
</tr>
<tr>
<td>Data Discovery</td>
<td>IoT Device Assessment</td>
<td>TEC: Evaluation, PoC, Bake-Off</td>
<td>Firewall Rules</td>
<td>Managed Intrusion Detection &amp; Prevention</td>
</tr>
<tr>
<td>Cloud Workshop</td>
<td>Security Architecture/Design</td>
<td></td>
<td>Intrusion Detection &amp; Prevention</td>
<td></td>
</tr>
</tbody>
</table>