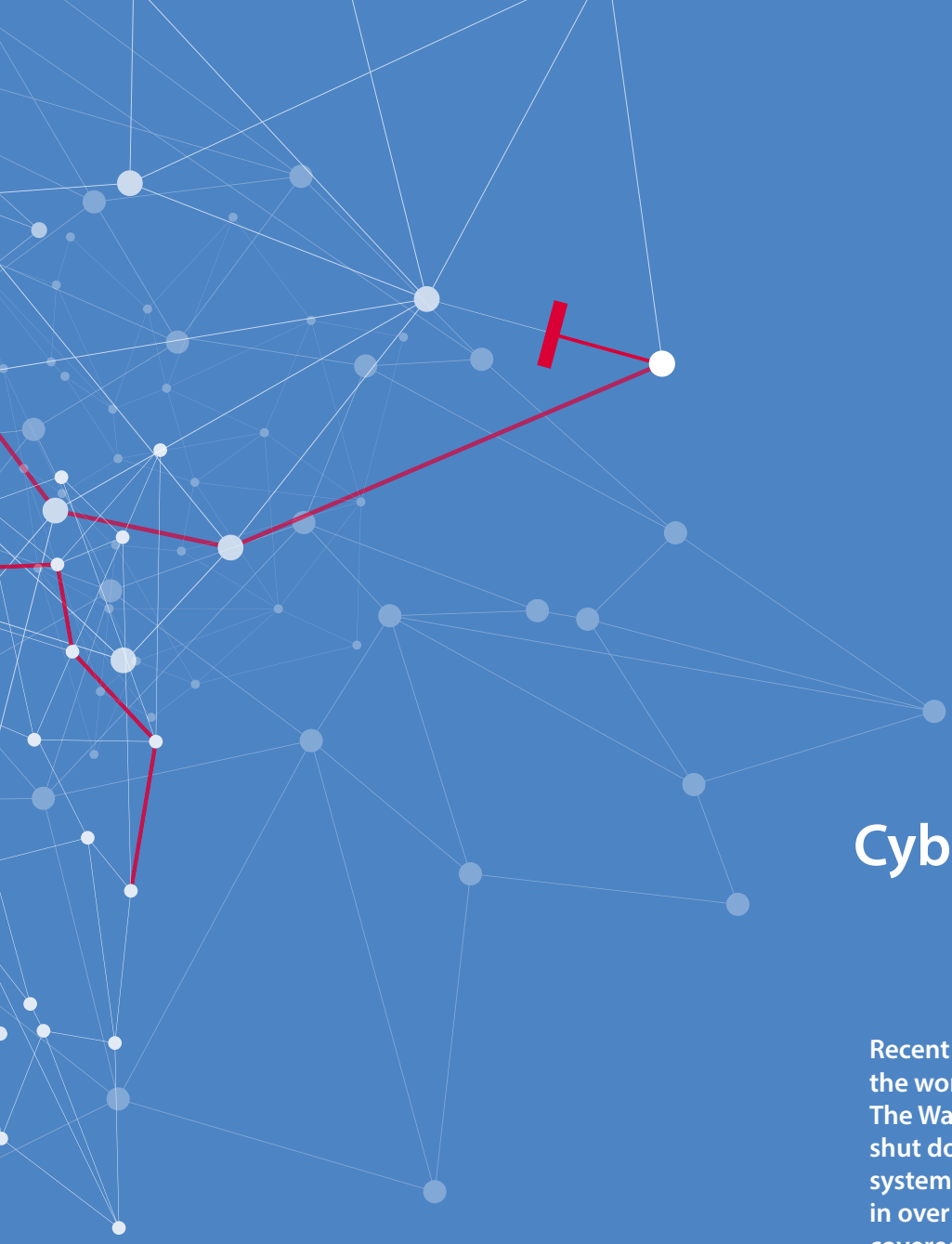


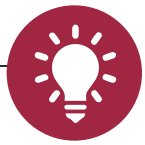
S2 SECURITY

Cybersecurity at Every Product Phase

Recent high-profile cyber attacks have exposed the world to the magnitude of their impact. The WannaCry ransomware attack effectively shut down the United Kingdom's healthcare system and affected many other organizations in over 150 countries. Target's extensively covered cybersecurity disaster in 2014 resulted in the theft of more than 70 million customers' personal financial information. The company continues to pay fines to the US government, and was even forced to reverse its planned expansion into Canada.

When it comes to physical security, the complexity and interconnectedness of today's systems provide multiple potential entry points for would-be attackers. This is why S2 Security incorporates information security into every phase of our products. Our comprehensive approach also empowers our customers to implement cybersecurity best practices while remaining vigilant.

Design



At S2 Security, we design secure products from the ground up. This means designing within a secure environment and reviewing all of our code to minimize potential vulnerabilities. The entire S2 system architecture is protected from cloud to network to server to panels using the TLS 1.2 protocol. Inaccessible from outside our facility, our design process ensures that would-be attackers cannot gain an early advantage. Our teams operate within a series of firewalls and antivirus redundancies, and access to these systems is also highly restricted within the company.

Development and quality assurance

Our developers follow coding best practices so that no shortcuts are taken which could result in a product weakness. Both the development and quality assurance teams run a variety of scans to detect any potential vulnerabilities along the way. These scans range from static scans to dynamic scans, each of which detect different types of vulnerabilities. Our teams also run daily scans on new and existing codebases to ensure no vulnerabilities have cropped up over time.

Manufacturing

Once development and quality assurance have signed off on the product code, a golden copy – verified to be secure and virus free – is provided to manufacturing.

As in the other stages of the process, manufacturing does its job almost entirely offline and always behind a series of firewalls. When manufacturing is "online," it is on a closed network. In fact, no product spends more than approximately five minutes connected to any sort of intranet. These brief periods are used for quick testing and licensing to make sure the product is working as intended.

Installation and deployment

The installation and deployment phase involves collaboration between S2 Security, systems integrators and end users. Once systems are installed or in use, they run the risk of being compromised if appropriate measures are not taken to secure the operating environment. To mitigate this risk, we provide cybersecurity best practices training to our installation experts. Our product requirements and guidelines – from forced default credential changes to networking recommendations – help secure systems in the field.

When an installation is complete, we suggest the systems integrator perform a survey that reviews safe computing practices with the end user. This empowers the end user to employ best practices while monitoring for potential vulnerabilities.

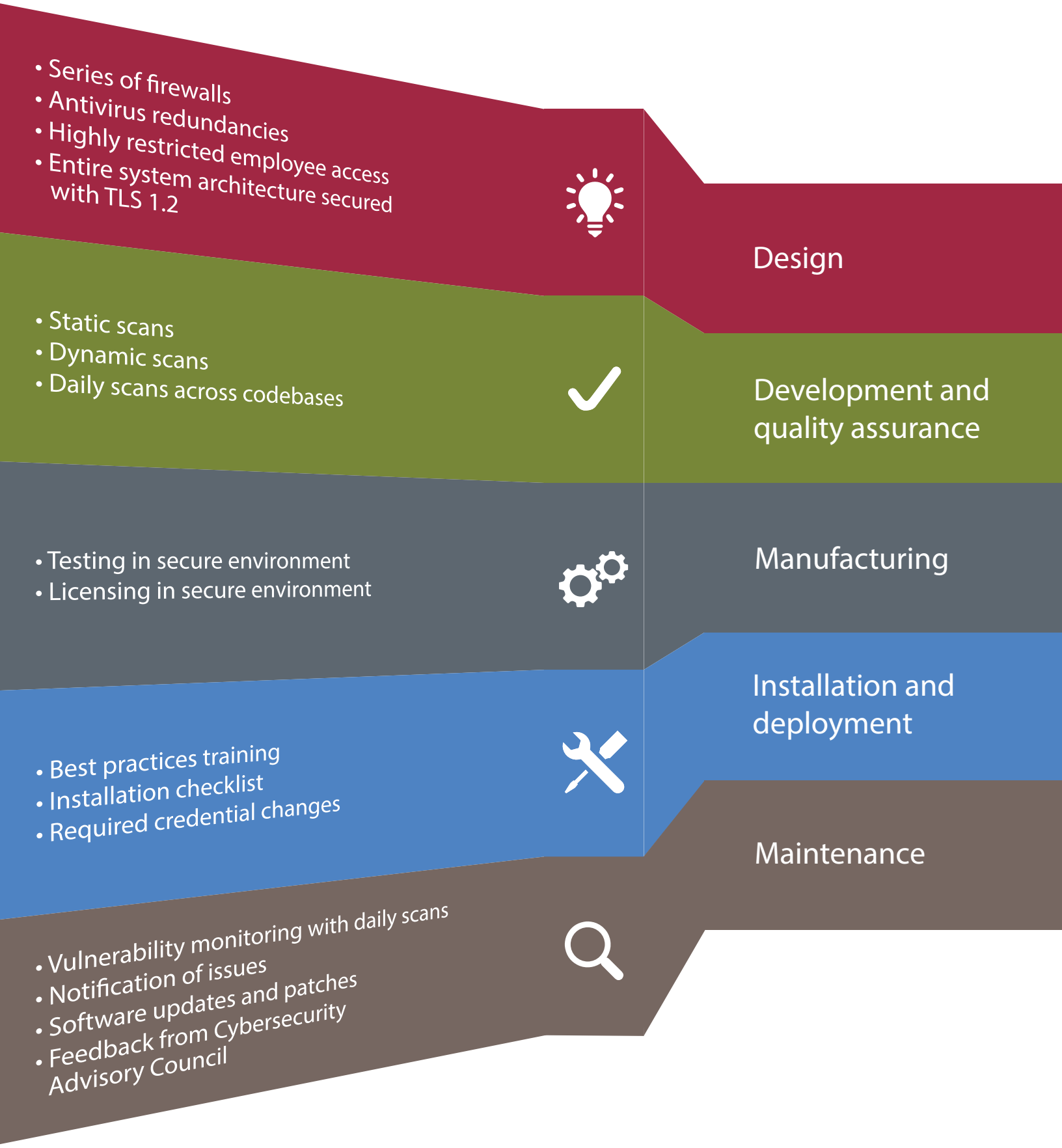
Maintenance

Following deployment, integrators receive timely updates with the information and tools they need to keep systems secure. We conduct daily scans for vulnerabilities and monitor for generalized cybersecurity threats. The S2 Technical Support team also immediately reports issues to our customers.

If a vulnerability or exploit is found, we systematically determine the best course of action – be it an immediate patch within 24 hours, or a notification to raise awareness.

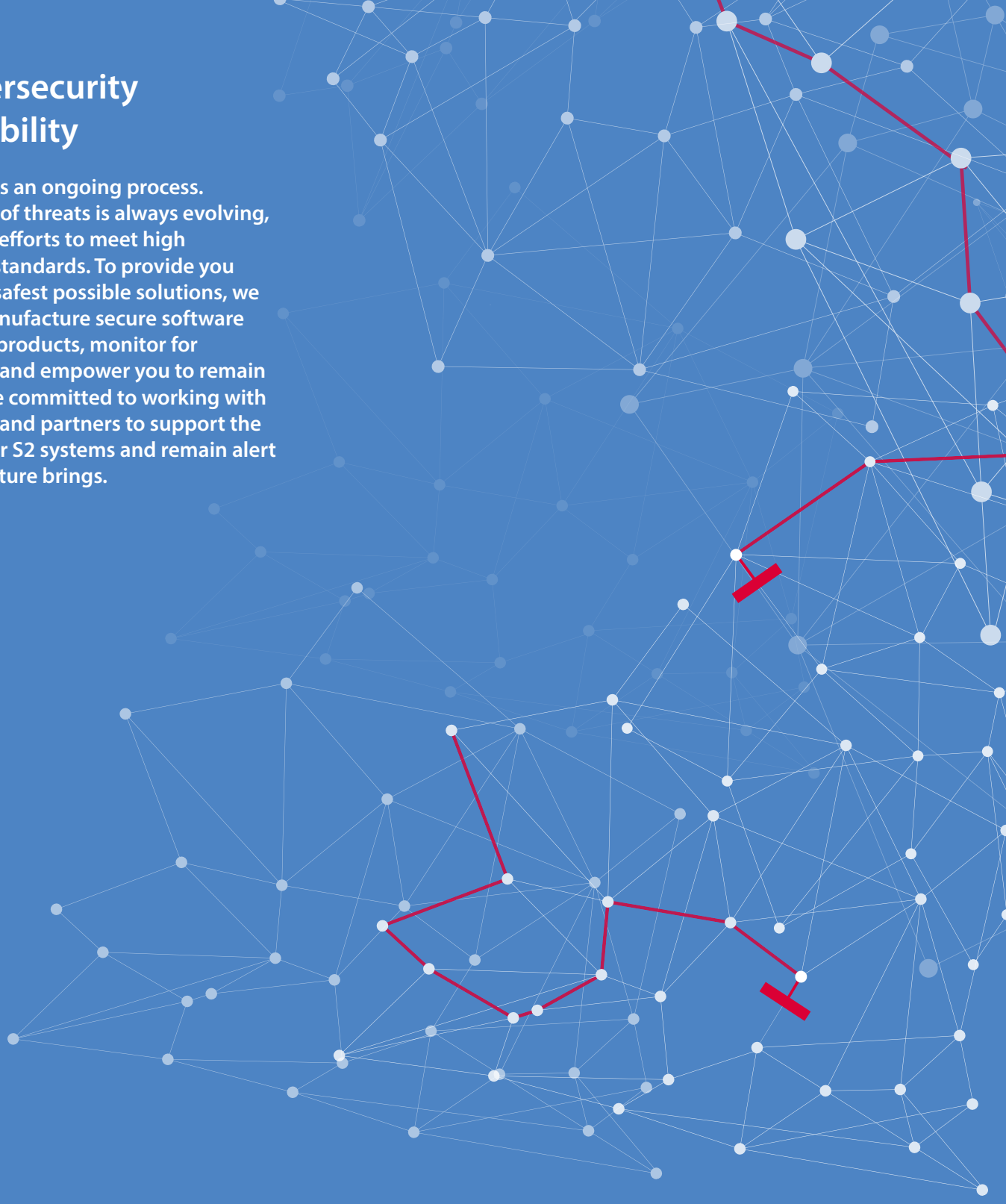
We also receive bi-annual feedback from end users on our Cybersecurity Advisory Council to address emerging concerns.

Security at every product phase



Our Cybersecurity Responsibility

Cybersecurity is an ongoing process. The landscape of threats is always evolving, and so are our efforts to meet high cybersecurity standards. To provide you with the best, safest possible solutions, we design and manufacture secure software and hardware products, monitor for vulnerabilities and empower you to remain vigilant. We are committed to working with our customers and partners to support the security of their S2 systems and remain alert for what the future brings.



s2sys.com

S2 SECURITY®