Comprehensive IoT Security

Fact sheet

IoT Security Assessment

verizon

Your business has never been more connected – or more vulnerable. With such innovation comes a new paradigm of potential security problems where companies need a holistic perspective to combat ever-evolving threat actors and vectors. Our IoT Security Assessment assists clients in closing the gap of emerging security concerns with IoT.

Address threat risk associated with IoT ecosystems and deployments.

Our IoT Security assessment focuses on reviewing operational and technical risks that threaten IoT-device ecosystems. Using our deep understanding of threats and attacks, we form a threat baseline for the IoT service and recommended risk avoidance and reductions measures to shrink client's IoT risk exposure. We use the following methodology for addressing risk factors:

- Prioritized risk matrix to rate the probability of exploitation and exposure
- Tactical and strategic recommendations to help mitigate unacceptable risks
- Vulnerability assessment that encompasses technical, operational, management, and governance areas of improvement

Targeted approach for addressing IoT device specific security concerns.

Infrastructure and application testing play a key role in understanding and mitigating vulnerabilities associated with your IoT devices. Our IoT Security Assessment provides you with a thorough testing of the infrastructures that your devices ride on and a look into the underlying applications that support them.

Verizon IoT security testing includes:

Wireless M2M Protocol Security Penetration

Verizon will analyze the wireless capability of the device and test applicable classes of attacks against the wireless protocol(s) in use. For 802.11 wireless capabilities, the analysis will include brute force decryption attempts, setting up rogue access points to perform man-in-the-middle attacks, and wireless client-side attacks. For non-802.11 protocols, Verizon's analysis may include replay attacks, protocol analysis and dissection, eavesdropping, and forging wireless messages.

Embedded Device Security

- Input validation bypass – Verizon will remove client-side validation routines and bounds-checking restrictions to confirm controls are implemented on application parameters sent to the server.
- Parameter Tampering – Verizon will modify query strings, parameters and hidden fields in attempt to gain unauthorized access to IoT device.

IoT Security Assessment

IoT Security Assessment is available as a fixed or custom-priced service.

Fixed-Price Service Packages

Fixed pricing is available in three levels:

S	M	L
Small	Medium	Large

Pricing level determinants include the number of IoT service processes, the specific testing parameters such as the number of business units and their locations and the number of unique IoT devices. Your sales representative can help you determine the fixed-pricing level appropriate for your business or organization.

verizon

Why Verizon

The better your security partner, the more useful your IoT security assessment will be. We've investigated many of the largest data breaches on record, and regularly do incident investigations.

Our security team has collected and examined security data for more than a decade, analyzing more than 250,000 incidents and over 8,000 confirmed data breaches.

Lean on our experience and expertise to help find the risk factors associated with deploying your IoT products, solutions and infrastructure.

Learn more:

For more information, contact your account representative or contact us:

verizonenterprise.com/support/sales

For more information about the other products and services we offer, visit:

verizonenterprise.com/products/security