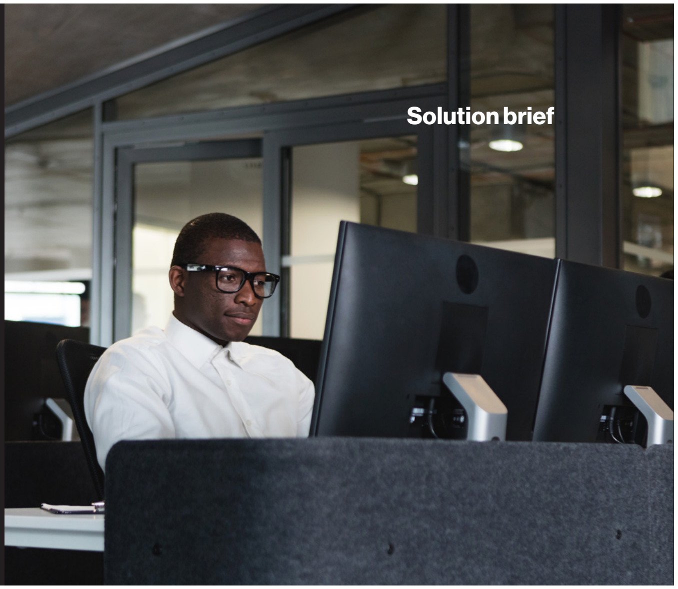
Today's IoT demands intelligent security.

Verizon IoT Security Credentialing

verizon



Solution brief

Introduction

The Internet of Things (IoT) is in the spotlight for a good reason. A connected world promises new opportunities that can help businesses create efficiencies, control costs, engage customers and grow.

There are many benefits to full-time connectivity, but as the popularity of IoT and machine-to-machine (M2M) applications continues to rise, businesses also need to be aware of the risks. Wide-scale use of IoT can open the door to security breaches, leaving your business more vulnerable to attack. To stay protected, you need to be able to lower the risks without losing the benefits of IoT.

Verizon IoT Security Credentialing helps keep bad things from happening to good IoT solutions by adding an extra layer of protection over and above your existing security. This solution integrates security with your IoT services, so wireless connections, applications data and device infrastructure can all be protected with one solution.

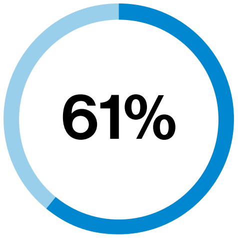
Don't gamble with the security of your business.

No one thinks they'll be the target of a cyber attack. But businesses that haven't suffered a data breach are either very well prepared, or very lucky. Large or small, no business is immune. For those who don't want to gamble with their future, the *Verizon Data Breach Investigations Report* (DBIR) dissects literally thousands of confirmed data breaches and security incidents from around the globe to provide insights on understanding and mitigating threats.

Attackers are constantly using new tactics and tricks, but their overall strategies remain relatively unchanged. In 2014, we identified nine attack patterns, and the 2017 report shows that 88% of security incidents still fall into those patterns:

- Cyber espionage
- Denial of service (DoS)
- Crimeware
- Insider and privilege misuse
- Miscellaneous errors
- Physical theft and loss
- Payment card skimmers
- Web application attacks
- Point-of-sale (PoS) intrusions

Understanding these attack patterns helps struggling security professionals gain insight on where and how to invest their limited resources. For everyone else, these patterns help provide a quick and easy way to assess where the most likely danger will arise. And with IoT Security Credentialing, you can add layers of security where you are most vulnerable for better peace of mind.



Sixty-one percent of the data breach victims in the 2017 DBIR are businesses with under 1,000 employees.

Traditional security isn't enough.

Even with the best defenses in place, traditional IT security only offers a perimeter-based approach. This works for cyber-security issues, where a firewall mentality can protect corporate data. But because IoT is always changing, it requires more than conventional security. To stay better protected, your IoT security strategy must address:

- Many IoT connections from many locations.
- Hijacking of physical devices.
- The security of a variety of devices that come from many different manufacturers.
- Device identification and management.

Get dynamic protection.

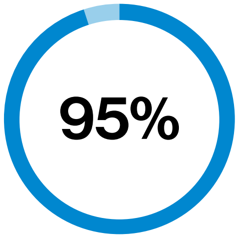
Just as your employees' credentials limit access to your resources and systems to only trusted people, IoT Security Credentialing only allows known and trusted devices in your IoT solution to connect to your network and resources. The Verizon IoT Security Credentialing solution integrates security with your IoT services, so wireless connections, applications data and device infrastructure can all be protected with one solution. The platform consists of many security tactics working together.

- Trusted credential creation and chaining
- On-demand and bulk provisioning of security credentials to your IoT devices
- Embedded encryption protecting your data and privacy
- Credential validation and secure life-cycle management

Create security built on trust.

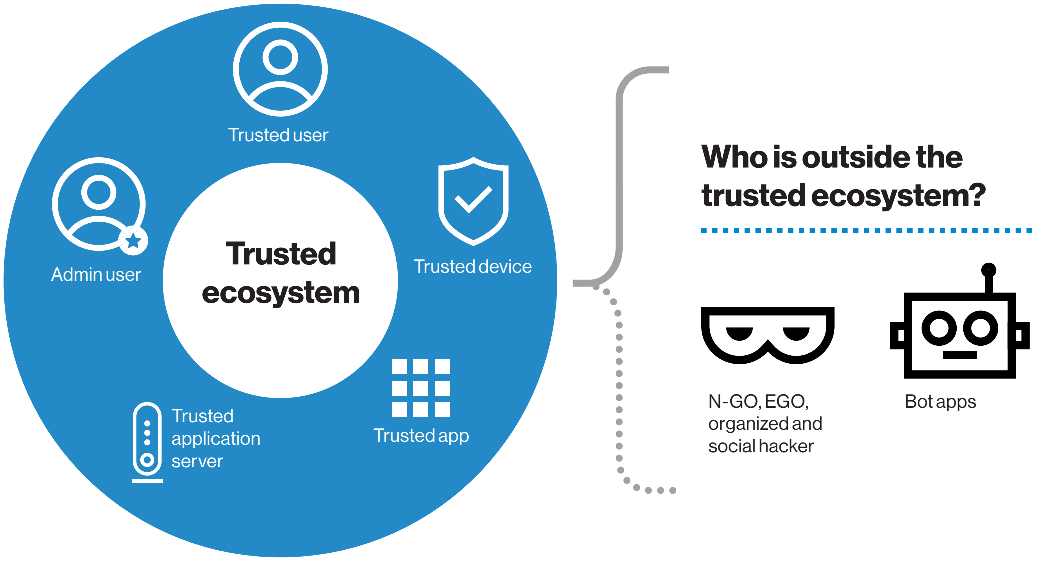
The trusted identity loop is at the root of IoT Security Credentialing. This loop:

- Means only authentic firmware, applications and configurations can be deployed and installed on an embedded SIM.
- Creates a trusted ecosystem that is established by making roots and certificates for trusted users and devices.
- Protects the privacy of the management and control channel.
- Prevents anything outside the loop from receiving certificates.



According to the 2017 DBIR, 95% of phishing attacks that led to a breach were followed by some sort of software installation.

IoT Security Credentialing: Trusted identity loop


Trusted user
Admin user
Trusted ecosystem
Trusted device
Trusted application server
Trusted app
Who is outside the trusted ecosystem?
N-GO, EGO, organized and social hacker
Bot apps

Why Verizon

When it comes to security, the network matters. We offer America's largest, most reliable 4G LTE network.

Our annual *Data Breach Investigations Report* has become one of the most anticipated information security reports in the industry. Working with 11 years of historical data, we've analyzed more than 100,000 incidents and earned our position as a trusted source for data protection, privacy and security.

We also run one of the largest IP networks in the world, which gives us a unique perspective when it comes to security and transiting the network. In fact, 96% of the Fortune 500 rely on our communication services and technologies. We offer complete solutions, with expertise in cloud, M2M and IoT. And we're a leading communications and wireless service provider to the public sector.

More coverage, fast speeds and reliable connections. So you can protect what's important, with help from a trusted partner.

Learn more:

To learn more about IoT Security Credentialing, please contact your Verizon Wireless business specialist or visit us at **VerizonEnterprise.com/contact-us.**

✉ **securitycredentialing@verizon.com**

Source: *2017 Verizon Data Breach Investigations Report*