BlackBerry
Intelligent Security. Everywhere.

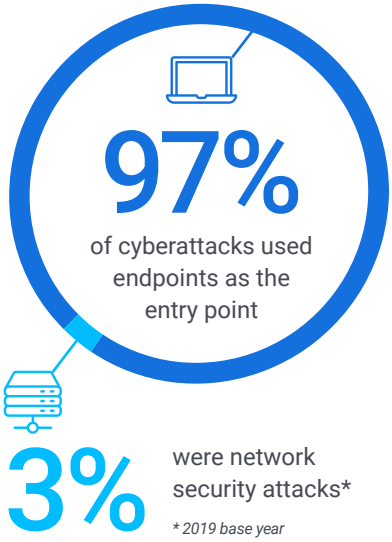
# Frost & Sullivan Report Summary

## BlackBerry® solutions address 96%+ of the enterprise threat landscape

Frost & Sullivan concludes BlackBerry is well positioned to secure all IoT endpoints, and upwards of 96% of the current cyberthreat landscape.

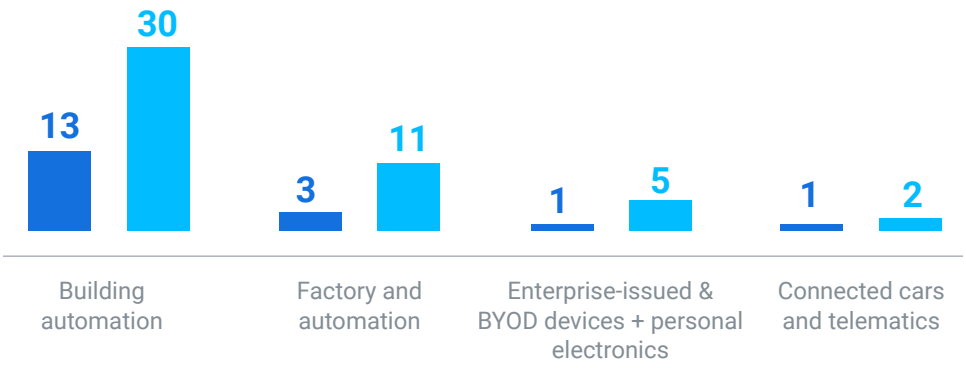
### Current Enterprise IoT Threat Landscape

The swift pace of technological innovation, combined with companies and individuals' ever-increasing demand for mobility, means that the number of connected endpoints will continue to grow exponentially, increasing the cyberthreat surface area to an overwhelming amount. Frost & Sullivan calculates that there were 24 billion new connected devices in 2019, and will rise to 67 billion devices (167%) by 2025.




| Device application | Million devices in 2019 | Million devices in 2025 | CAGR |
|---|---|---|---|
| **Building automation** | 12,964 | 30,155 | 15% |
| **Factory and industrial automation** | 2,768 | 10,824 | 26% |
| **Enterprise-issued and BYO devices plus other personal electronics** | 1,888 | 4,998 | 18% |
| **Connected cars and telematics** | 977 | 1,630 | 9% |
| **Healthcare and medical devices** | 155 | 503 | 22% |
| **Vending/retail terminals** | 104 | 388 | 25% |

### Growth by Volume of Connected Devices (# in Billions)




# 5 TRILLION

USD global cybercrime-related costs are expected to hit in 2020; cybercrimes increased dramatically during the first half of 2020 amid the COVID-19 pandemic remote-working environment

## BlackBerry solutions address 96%+ of the enterprise threat landscape

| Industry/Application | Endpoint vs. Network as Prime Concern | Percentage of Threat Covered by BlackBerry |
|---|---|---|
| **Corporate/BYO devices** | Endpoints. Phishing risk. | 100% |
| **Automotive** | Endpoints. Customer data is high. Vehicle control possible but not common. | 100% |
| **Building automation** | Endpoints. Phishing for credentials. Access surveillance cameras, other devices. Some network. | 95% or more. Some network-only building systems may not be covered. |
| **Vending/transaction terminals** | Endpoints. Customer data. Main way of hacking retail. | 100% of new devices; varies by age of installation |
| **Healthcare and medical devices** | Endpoints. Phishing for target medical records and devices. Unintentional third-party and insider-related attacks are high. | Up to 100% |
| **Manufacturing** | Endpoints. Network possible as well as some devices are only networked. | 90% or more. Some network-only systems may not be covered. Physical entry points (i.e. USB-based attacks) |
| **Finance and banking** | Endpoints. Phishing for credentials and customer info. | Up to 100% |
| **Telecommunications** | Endpoints. Phishing for credentials and customer info. Some network control for disruptions. | 95% or more. Some network-only systems may not be covered. |
| **Energy/utilities** | Endpoints. Phishing risk. Network and even physical control to cause system disruptions. | 95% or more. Some network-only systems may not be covered |
| **Government** | Endpoints. Phishing to gain credentials and launch malware to cause system disruptions. | Up to 100%. |

## Current Enterprise IoT Threat Landscape

**Growth in the number of connected devices will require businesses to…**

**Ensure Control and Visibility across Ever-Increasing Endpoints.** Businesses must track, secure, and update thousands of connected devices internally and across a diverse value chain.

**Simplify the Security Solution Landscape.** The more vendors an enterprise deploys, the greater the risk in terms of point-to-point security vulnerabilities and interoperability maintenance issues.

**Manage Mixing of Personal and Enterprise Devices.** The rise of BYO in the modern enterprise means many businesses are faced with managing a mixed environment of corporate and personal devices. Additionally, as the network perimeter dissolves connected endpoints outside of the traditional enterprise environment add risks.

**Manage Overwhelming Scale.** The Internet of Things (IoT) has created a single connected ecosystem, which crosses traditional enterprise boundaries. The size of the IoT environment, the amount of data and the expanse of cyber threats, are set to make the job of the IT industry unmanageable.

**Manage the Human Factor.** End users bring with them a separate set of risks—in most cases unintentional and not malicious.

---

BlackBerry comprehensively addresses the enterprises' IoT security needs – the endpoint itself, its operating system, data, and transfers, along with edge use cases that come from the dissolution of the traditional network perimeter. It behooves all businesses to take a step back and ensure that endpoint security is the foundation of their strategy, and their solutions are not fragmented across multiple vendors, which has been shown to increase costs and decrease cybersecurity effectiveness. Partnering with a solution provider that has the technologies to comprehensively secure an enterprise's data and communication is by far the most effective way to ensure security, resilience, and uninterrupted business continuity.

Read the full Frost & Sullivan whitepaper.

Join us at the BlackBerry Security Summit to learn more. To speak with a BlackBerry expert, please email BlackBerry@BlackBerry.com.

# BlackBerry Gives Enterprises a Comprehensive Platform for Securing their Connected Environment

From Enterprise Endpoints to Data Shared at the Edge