Lookout®

WHITEPAPER

Cyber threats facing the manufacturing industry and strategies to mitigate risk

Executive Summary

Manufacturers are transforming the way they produce and deliver goods - moving toward industrial automation and the flexible factory. This transformation, known as Industry 4.0, puts pressure on mobile devices and cloud solutions as manufacturers realign themselves to make sure they can effectively transition their work from the design studio to the shop floor. Mobile apps, data analytics, and internet of things (IoT) devices offer an unprecedented opportunity to create innovative new products, drive revenue, and increase operational efficiency.

Cybersecurity risk cannot be underestimated. 25% of major security compromises experienced by manufacturers have had lasting repercussions.[1] Every smartphone and tablet should be treated as a potential source of threat. This is true whether it is in the hands of an engineer, a business development executive, or the HVAC service person. Adopting a security solution that adheres to a Zero Trust model, where the health of all mobile devices are monitored in real-time, will ensure your organization's data is secure.

This whitepaper provides an overview of key threat trends faced by manufacturers and their potential impact on your business; from the inherent risks of cloud apps to the ongoing need to protect intellectual property and maintain industry compliance. Finally, we'll share use-cases highlighting how other manufacturers are protecting their businesses against the latest phishing and other mobile threats.

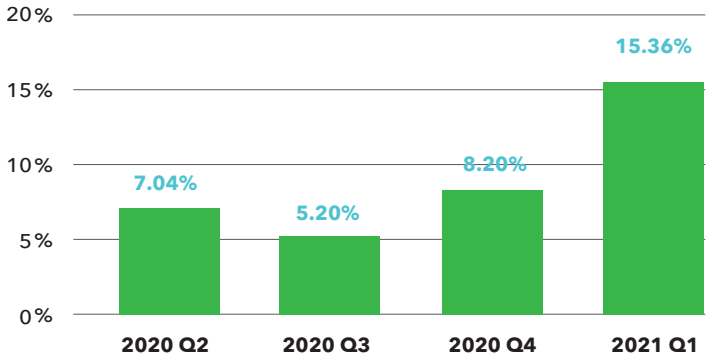
Key takeaways

1. Phishing and malware remain the primary threat vectors targeting the manufacturing industry.
2. A Zero Trust security strategy is more critical than ever as threats evolve to take advantage of an expanded remote workforce that rely on mobile devices and cloud applications to be productive.
3. Mobile threat defense is a necessary component for securing a mobile workforce that is increasingly targeted by phishing, application, device, and network attacks.
4. CASB and ZTNA solutions are essential for manufacturers to securely collaborate with and access sensitive data within private enterprise and public cloud applications.

1 2021 Verizon Mobile Security Index, p.30

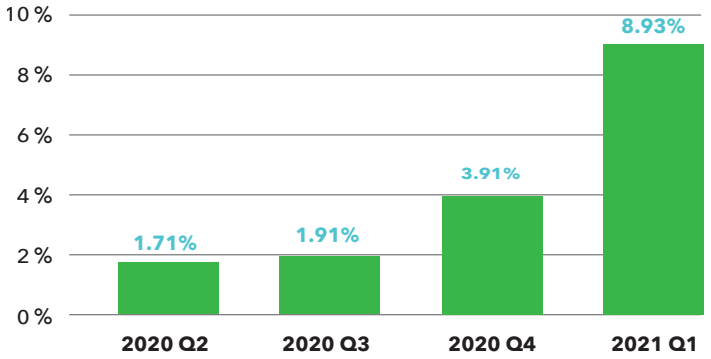
Mobile Threats in Manufacturing by the Numbers[2]

Mobile Phishing Exposure Rates for Manufacturing



Global phishing exposure rates increased 118 percent over the 12 month period between Q2 2020 and Q1 2021.

Mobile Phishing Exposure Rates for Manufacturing users of Microsoft 365



Mobile phishing exposure for users of Microsoft 365 also increased significantly over this same time period.

NUMBER OF MOBILE PHISHING LINKS MANUFACTURING EMPLOYEES CLICKED ON				
# Urls clicked	1	2	3-5	6+
Android	68.79%	17.38%	11.70%	2.13%
iOS	56.63%	18.55%	17.28%	7.54%
Total	58.27%	18.39%	16.53%	6.81%

During 2020, most manufacturing employees with phishing protection on their device only clicked one link. This indicates they are learning to spot and avoid phishing attacks. However, nearly 7 percent clicked six or more urls.

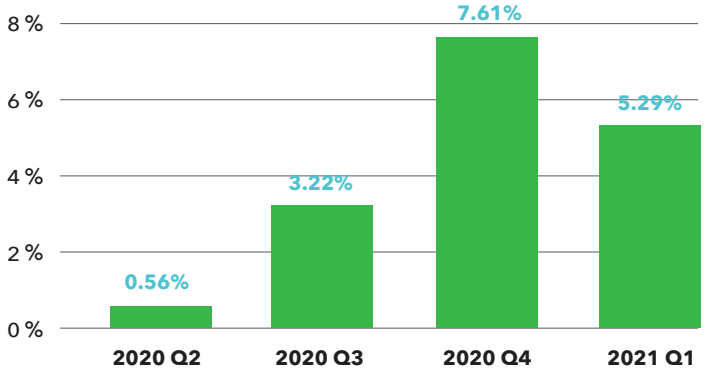
ANDROID - EIGHT MONTHS AFTER ANDROID 11 RELEASE		
OS Versions	# of devices	# of vulnerabilities
11	30.33%	>50
10	31.81%	>260
9	15.88%	>170
8	11.83%	>63

Nearly 70 percent of manufacturing employees using Android devices are running an outdated OS version.

IOS - EIGHT MONTHS AFTER IOS 14 RELEASE		
OS Versions	# of devices	# of vulnerabilities
14	81.06%	>50
13	11.92%	>195
12	6.0%	>65
11	0.72%	>130

Manufacturing employees on iOS devices remain more up-to-date with over 80 percent on the latest OS release.

App Threat Exposure Rates for Manufacturing



App threats experienced an 844 percent increase over the past twelve months. This is due to a major increase that started in Q3 2020 when a popular advertising SDK was reclassified as riskware due to excessive access permissions.

2 2021 Verizon Mobile Security Index, p.30

Phishing and malware remain major threats

People are busy, device screens are small. We work quickly, instinctively, and often distractedly on our mobile devices. So it's no surprise that phishing is the primary way malicious actors trick people into downloading malware. Attackers are clever about targeting and tricking individuals, especially executives, sales, and finance, into downloading malware or inadvertently granting them access to corporate resources

118% increase in mobile phishing exposure rates over the past 12 months

Globally during 1Q2021, over 15 percent of manufacturers were exposed to mobile phishing threats, a 118 percent increase over the past twelve months. At a regional level, European manufacturers' exposure was 21%, outpacing the global rate. North American organizations were slightly less exposed at nearly 12 percent.[3]

There are many real-world examples of ways phishing and malware can exploit mobile device vulnerabilities to steal data, change the configuration of the device, lock out the user until ransom is paid up, or brick the device. Malware can allow the attacker to jump over to the operational technology (OT) network, spreading disruption and destruction.

WhatsApp can now be hacked to change the text of a message and identity of a sender. We learned this from an attack that tricked one of the most prominent tech executives. Malware such as Flubot can arrive via text message faking the shipment status of deliveries from Deutsche Post & DHL, Saturn, and UPS, only to wreak havoc by intercepting and sending SMS messages, displaying screen overlays, and stealing contacts. Pegasus spyware can bypass device security without a user's knowledge then take action and steal information like contacts, location, and passwords. The surveillanceware Monokle uses advanced data exfiltration techniques and can install an attacker-specified certificate to the trusted certificate store on an Android device to facilitate a man-in-the-middle attack.

Permanent shift to remote work creates new risks

The pandemic accelerated everyone's digital transformation and cyberattackers took advantage of the confusion. Lookout data shows a 118 percent increase in the mobile phishing exposure rate for the manufacturing industry, globally.

As remote work becomes an integral part of how we work, manufacturers must ensure their workers are protected against phishing, malware, and other mobile attacks, no matter where they are.

In March 2020, Lookout identified an Android app called "corona live 1.1." Upon launch, the app informs the user that it doesn't require special access privileges, then goes on to request access to the phone's media, files, device location and permission to take pictures and record video. The app is a trojanized version of the legitimate "corona virus" app, which provides an interface to the data used in the John Hopkins coronavirus tracker.

Prior to the pandemic when travel was frequent, manufacturing leaders had been concerned about the digital protection of their people, devices, and data traveling to Asia.

For example, one Lookout customer had told us that after 10 employees travelled to Asia, more than 100 incidents, including malware, were found on those devices. Some companies have even implemented a one-phone-per-trip policy, and when an employee returns from a trip to Asia, their phone is thrown away.

These 'burner phone' strategies are likely to return for many as global covid-19 cases decrease and international travel rebounds. However, organizations that have deployed mobile threat defense are protected from mobile threats and can go without a burner phone strategy.

A recent Lookout mobile threat discovery of four interconnected surveillanceware tools originating in China, further exemplifies the cybersecurity risk that China can present. The primary aim of the malware is to gather and exfiltrate personal user data to attacker-operated command-and-control servers. Activity across these tools dates back to 2013.

3 Lookout threat data from 2Q2020 to 1Q2021

Manufacturers have embraced software-as-a-service (SaaS) for productivity and collaboration, customer management, human resources, finance, manufacturing execution and supply chain. The benefits are many. With cloud tools, employees, customers and partners can collaborate more effectively. Mobile apps and devices improve planning and control and provide greater transparency on the shop floor. Machinery operators can add descriptions, pictures, and videos on their mobile devices, reducing paperwork. Workers use self-learning resources for safety training and to acquire new skills.

At the same time, manufacturers need to be aware of cyber threats targeting the increased use of cloud applications. In fact, phishing attacks against Microsoft 365 users are on the rise. Lookout data shows that nearly 9 percent of Microsoft 365 users were exposed to mobile phishing threats in 1Q2021. This is a 246 percent increase over the average rate for all of 2020.[4]

100% rise in nation-state cyberattacks in last 3 years[5]

In early 2021, Microsoft Exchange Servers suffered an exploit of four critical vulnerabilities that had a large scale impact on businesses globally. When exploited, these vulnerabilities could all lead to Remote Code Execution (RCE), server hijacking, backdoors, data theft, and potentially further malware deployment. As a result, organizations are re-evaluating how they monitor for security incidents and how they deliver secure access to critical applications whether they are on-premise or in the cloud.

One preferred solution for secure access to enterprise applications has been to replace legacy Virtual Private Networks (VPN) with Zero Trust Network Access (ZTNA). VPNs have long been the standard for securing remote access to private internal applications such as on-premise Microsoft Exchange. Unfortunately, if cyber criminals exploit a VPN, they can gain access to the entire corporate network and move laterally throughout.

ZTNA, on the other hand, provides very granular access controls, content inspection and anomaly detection. So not only do organizations get stronger protection against cyber threats, but they also gain greater control. With ZTNA, users are restricted to accessing only a specific application rather than becoming an extension of the corporate network.

Mitigating third-party risk

An expansive supply chain puts manufacturers at greater third-party risk. Manufacturers rely on a web of external workers, contractors, and service partners to maintain equipment on the factory floor, clean machinery, package products, manage waste, ensure worker safety, and much more.

Technicians from one vendor may share the same device among the team as they access applications in the cloud. They may access a manufacturer's email or HR system or take training courses from these third-party devices. Some vendors might have mobile device management (MDM) installed to adhere to the manufacturer's security policies.

When it comes to collaboration in the public cloud, manufacturers need to secure access to their data and protect their data wherever it goes. Manufacturers deploy Cloud Access Security Broker (CASB) solutions with advanced data protection capabilities to get this level of protection. With strong user behavior analytics, data loss prevention and data encryption, a strong CASB solution will prevent intentional and unintentional data leakage, encrypt downloaded data and detect malware in files.

Connected manufacturing spreads risks

To remain competitive, manufacturers are investing in intellectual property and new technologies like digital twins. Digitizing manufacturing, inventory tracking, operations, and maintenance increases agility and efficiency, with less production downtime and a greater nimbleness.

4 Lookout threat data from Q2 2020 and Q1 2021
5 AWS Cloud Security Report 2020 for Management: Managing the Rapid Shift to Cloud

While the connectedness of a smart factory accelerates innovation in products, manufacturing and supply chain management, it also creates cybersecurity risk. The manufacturing floor is no longer air-gapped from the corporate IT network. Threats from mobile devices can spread from the corporate IT network to the OT network. Industrial control systems are now vulnerable. IoT strategies are enabling new ways to drive customer service and business efficiency, but the security of many IoT devices is not field-proven.

Protecting intellectual property

Protecting intellectual property and trade secrets is paramount. Automotive manufacturers are building safer cars that can reduce accidents. Pharmaceutical companies invest billions in drug development, and must protect information from their proprietary research and clinical trials. Data from research labs is more valuable than ever as accurate tests and vaccines are developed to eradicate the coronavirus. In aerospace and defense, the stakes for protecting innovation are not just a matter of competitive advantage, but also of national security.

Compliance requirements are rising

Europeans place a high value on personal privacy. The EU's General Data Protection Regulation (GDPR or DSGVO in Germany) has created stringent breach notification requirements and stiff fines on companies that do not adequately protect personal data. In 2020, 18 companies were fined at least €100,000, according to a GDPR fine tracker[5].

Organizations have been working to operationalize these new legal requirements, and those who fall to data breaches face serious financial penalties. Manufacturers have increased audit frequency to ensure they remain in compliance, which consequently calls for new ways to streamline security reporting.

Manufacturers should adopt a Zero Trust strategy

Mobile and cloud security help manufacturers adopt a Zero Trust approach. Here at Lookout, we continuously monitor device risk-level and protect users and enterprise data in the cloud from the latest phishing, app, device, and network threats. In short, all devices are guilty until proven innocent. And with unparalleled visibility into the risk-level, identity, and context of the apps, device, network, and corporate data, we continuously adapt our machine learning models to detect emerging threats with high fidelity.

Lookout creates a fingerprint of each mobile device and compares it with data from nearly 200 million mobile devices. iOS and Android devices, whether company-owned or personal, are validated during authentication. Lookout then provides continuously validated, conditional access to corporate data.

Lookout mitigates mobile threats and delivers cloud security for manufacturers

Lookout provides comprehensive endpoint-to-cloud security by protecting manufacturing organizations against the entire spectrum of mobile risk and protecting intellectual property wherever it goes - all while ensuring secure access to cloud applications.

5 Coreview. "Major GDPR Fine Tracker - An Up-To-Date List of Enforcement Actions". Coreview Blog, July 13, 2020.

Lookout Mobile Endpoint Security (MES)

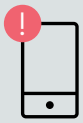
Mobile endpoint security must detect threats in apps, the device and network connections. It must protect the user, the device and the organization while respecting privacy. It must work equally well for employee-owned and company-owned devices.

Mobile phishing

Lookout detects and tracks thousands of active phishing sites every day. We can monitor phishing attacks coming from all sources, including email, SMS, social media platforms and messaging apps and any app communicating with the internet. Our AI-driven platform proactively determines the reputation of internet sites and detects phishing kits as they are being built, long before any user is targeted or an attack is executed.

App threats

Lookout has analyzed more than 140 million applications, which provides us with visibility into risks such as trojans and spyware. As a founding member of the Google App Security Alliance, Lookout also scans every app in the Google Play Store and reports malicious apps for removal.



Device risks

Lookout also protects against device-based risks that occur when the built-in security of the operating system has been bypassed. Lookout can identify behavioral anomalies, rooting or jailbreaking, out-of-date operating systems, and device configuration risks.

Network risks

Lookout protects against network risks, which is especially important as so many more employees work from home and will continue to use public Wi-Fi hotspots. Lookout analyzes network connections and can accurately identify man-in-the middle attacks, host certificate hijacking, hijacked SSL traffic, and TLS protocol downgrades.

Lookout Cloud Access Security Broker (CASB)

To get the most of your countless cloud apps without risking your data, you need to know exactly what's going on. You also need to be able to detect and respond to threats and have the ability to dynamically control access. Lookout Cloud Access Security Broker (CASB) provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls.

With continuous monitoring of user and entity behavior analytics (UEBA), you can detect and respond to insider threats and advanced cyberattacks. We provide advanced data loss prevention that can classify, encrypt and restrict sharing of your data on the fly so that only authorized users have access. We also perform automated assessment of all your cloud apps and infrastructure to ensure they are properly configured.

Lookout Zero Trust Network Access (ZTNA)

Your workers want easy access to what they need. Lookout Zero Trust Network Access (ZTNA) provides seamless connection to your apps – whether they reside in data centers, on public clouds or in hybrid environments – without putting your data at risk. To do so, we only grant access to specific apps that your users require for work. We also continuously monitor the identity and risk level of users and endpoints to restrict access accordingly.

To ensure your infrastructure is secure, we can hide your apps from the public internet, ensuring that only authorized users have access. We also extend cloud app security benefits to your legacy apps by providing integration with multifactor authentication and identity access management.

Enforce data privacy policies and protect employee information

Lookout helps companies maintain their data privacy policies, both internal and industry regulations and laws. If regulated content is being accessed and shared improperly, the security team will be promptly notified. If a device exceeds an acceptable level of risk, we will notify the employee and the IT manager and can log the employee out of corporate resources. With a data-driven platform, we also do not inspect the content we protect, respecting the privacy of your organization and your employees.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.