WHITE PAPER

CALIAN®

# Data and its importance to endpoint security

How a data-centric security approach can control proliferating endpoints and escalating cyberattacks

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

In today's ever-connected world, the ability to access corporate data from virtually any device, such as tablets, phones and laptops, from any location, poses a significant threat to organizations and their cybersecurity teams. With the proliferation of connected devices on networks, including virtual machines, point-of-sale (POS) terminals and IoT devices, IT security professionals are increasingly spending more and more time managing and securing these devices and the variety of applications they deliver.

This is a major challenge, as many of these are privately owned personal devices, making it difficult for cybersecurity teams to monitor and secure them. This is a security nightmare, as a personal device can expose an entire network to risk with just one security incident. And these devices are proliferating. In its 2011 Annual Security Report, Cisco found that three out of four employees worldwide have multiple devices, such as a laptop and smartphone, and one in three young professionals uses at least three different devices for work (Cisco, 2011).

With the number of endpoints increasing—according to Intel there will be more than 200 billion connected devices by 2020—there is a corresponding increase in the vulnerability of the network to a vicious cyberattack from malware threats and online sources (Intel, n.d.). A frightening scenario, as Cisco's report also found that the most popular mobile platforms—Apple iPhones and iPads and Google Android devices—are now targets for malware.

## Endpoints primary target

The primary challenge for many organizations is how to implement controls that allow users to benefit from the functionality and inherent ability of their personal devices to access networks while simultaneously ensuring that no corporate data is being taken and no malicious code is being introduced into the network.

Far too often, the greatest risk of data breaches comes when employees simply take files without permission or upload malware by mistake. In fact, research shows that accidental breaches—caused, for example, by devices being lost or by employees being unaware that their device is infected—account for the majority of issues that companies face. The challenge is how to control device access while simultaneously allowing some types of data to be accessed or transferred.

So, based on this scenario, where do IT security professionals start when planning for new security measures? They should start with endpoints because they are, by far, the most susceptible to attack by cybercriminals. The difficulty, however, is choosing the right set of tools that can address the greatest number of needs—critical considering that the main target for cybercriminals is still the endpoint.

With data being the one consistent thread that binds endpoints together, it makes sense to take a data-centric approach to security. This is essential when taking into account the numerous and evolving cyberthreats facing organizations today—with endpoints at the epicenter.

CALIAN®

## Threats to the business

Cyberattacks are continuously evolving and increasingly creative. According to Check Point Research's mobile threat team, "The results are stark: enterprise mobility is under constant attack, affecting all regions and industries, on both major mobile platforms, Android and iOS. Threats to mobile users are myriad and powerful, and ultimately capable of compromising any device, accessing sensitive data at any time" (n.d.).

Here's a brief look at some of the major threats facing businesses today:

- Malware Attacks

  Malware covers every kind of malicious software that attacks the network. The purpose behind malware is to damage devices, steal data, cause havoc and, obviously, to make money. Hackers make money easily by selling their malware on the dark Web. Malware includes ransomware, viruses, Trojans, and spyware.

  The 2019 *State of Malware* report states that, "Malware authors pivoted in the second half of 2018 to target organizations over consumers, recognizing that the bigger payoff was in making victims out of businesses instead of individuals. Overall, business detections of malware rose significantly over the last year—79% to be exact—and primarily due to the increase in back doors, miners, spyware, and information stealers."

  And, according to the Beazley Breach Response (BBR) Services team, ransomware attacks skyrocketed in the first quarter of 2019: a 105% increase in the number of ransomware attack notifications against clients compared with Q1 2018 (Beazley, 2019).

- Distributed Denial of Service

  The primary goal of a distributed denial of service (DDoS) attack is to slow down or crash an organization's website by deploying large numbers of internet bots—from hundreds to hundreds of thousands. After an attack, the server, network, or application is overwhelmed, resulting in denial of service to legitimate users. A recent security survey found that 32% of serious DDoS attacks coincided with a network intrusion (Cox Business, n.d.).

  A 2017 Cisco report found that the number of DDoS attacks exceeding one gigabit per second of traffic will rise to 3.1 million by 2021, a 2.5-fold increase from 2016.

- Insider Cyber Security Threats

  Unfortunately, employees can be behind crippling cyberattacks, sometimes unintentionally and sometimes intentionally. The latter effort is usually aimed at delivering spiteful damage to the company for what the employee perceives as an injustice, perhaps downsizing, new management, or lack of promotion. When the organization fails to revoke access to data, it leaves the door open for an attack such as ransomware.

  The US Computer Emergency Response Team (CERT) study found that almost 40% of IT security breaches are perpetrated by people inside the company, with the most likely perpetrators of cyberattacks being system administers or IT staff with privileged system access. Another insider vulnerability is when attackers gain and use an employee's trust to access a network, or when an employee accidentally downloads malicious internet content (Whittle, 2008).

- Weak Password Policies

  Weak, reused, or stolen passwords cause 81% of breaches. The average adult possesses more than 25 online accounts, with corresponding passwords. Therefore, it is not surprising that passwords are weak or reused—leaving them open to being stolen and increasing the risk of either an internal or external breach (Palfy, 2018).

  Password policies need to be enforced, particularly for brute force and key logger attacks. An identity access management (IAM) system should be implemented to secure, store, and manage user identities and access privileges. The most common IAM practices are single sign-on (SSO), multi-factor authentication (MFA), and access management; all of these can be deployed on-premise or in the cloud.

  By combining three major concepts—identification, authentication, and authorization—IAM makes certain that specified users have the authorization and access they need to work productively. Meanwhile, unauthorized users do not have access to sensitive corporate data, which helps to safeguard the privacy and security of the organization and the individual.

Combined, these threats to the business—approximately one million cyberattacks are attempted every day—underscore the necessity of implementing cybersecurity measures, regardless of the financial, technological, or other constraints (Carbon Black, 2019). The attitude to take in this climate of evolving and worsening cyberattacks should not be one of complacency, but one of expectancy. When will it happen? How much will it cost? Because a cyberattack is a given: it is a question of being prepared to spend money today to save money and reputation in the future. The key to a successful response to a data breach is this: be prepared.

## Costs to the business

Security solutions continually evolve to meet the increasing threats to the business, while cybercriminals continually evolve their methods of attack to overcome them and breach the organization.

According to the Ponemon Institute and Accenture's 2019 *Cost of Cybercrime Study*, malware and malicious insider-related cyberattacks jumped 12% in 2018, accounting for one-third of all cyberattack-related costs. On average, the cost of malware to companies increased 11% to more than US$2.6 million per company. Malicious insider incidents—caused by employees, temporary staff, contractors, and business partners—jumped 15%, costing each company an average of US$1.6 million (Ponemon Institute and Accenture, 2019).

The history of cybercrime underscores how nasty and greedy cybercriminals can be. Since 2013, 3,809,448 records have been stolen through breaches every day—that's 158,727 per hour, 2,645 per minute, and 44 every second of every day. And by the end of this year, 2019, cybercrime will have cost businesses more than US$2 trillion. In 2020, the average cost of a data breach is expected to exceed US$150 million as additional business infrastructure gets connected (Brooks, 2017).

In addition to the financial costs of a breach, there are the hidden costs that can threaten the survival of the company: negative impact on reputation, reduced productivity as employees spend time on recovery, loss of trust by customers and stakeholders, and non-compliance with mandatory regulations, resulting in heavy fines and other penalties.

CALIAN®

## How to protect the business

Without an effective endpoint systems management solution, the impact on the business can be catastrophic. In fact, vulnerable endpoints have become a primary target for nefarious attackers who view remote-device accessibility as the perfect opportunity to exploit an often forgotten—and therefore open—gateway to infiltrate corporate systems.

And though increased endpoint security has always been an important weapon in the fight against cybercrime, many of the tools used to manage traditional endpoints are no longer relevant or as useful as they once were. Whether it is antivirus software, or even more sophisticated intrusion-detection systems, the majority fall short when detecting modern endpoint threats.

Moving to a data-centric security approach—an approach that emphasizes the security of the data itself rather than the security of the networks, servers, or applications—places the focus on protecting the data, rather than the system where the data resides. When the focus is on protecting the system, it does not protect the data when it is moved elsewhere. The system remains protected, but sensitive data is left unprotected, exposed—and vulnerable to a cyberattack.

The first step in the data-centric approach is to automatically identify sensitive data as soon as it enters the organization's IT ecosystem. It should then be secured with policy-based protection that is with the data throughout its life cycle. A common practice is to install software agents on every IT asset where sensitive data resides, such as laptops, servers, mobile devices, and more. Administrators control these agents from a centralized management console, applying the right type of protection for each data type and use case (PKWARE, n.d.).

When the data is either created or modified, the file is scanned to see if it contains sensitive information. The system then automatically applies the appropriate security. This protected data is available only to authorized users; unauthorized users have no access. Having a data-centric security approach implemented throughout the organization means that when network or device security fails, the impact on data is reduced or eliminated (PKWARE, n.d.).

This is just a very brief overview of the data-centric security approach and how it protects sensitive data throughout the data life cycle. With such an approach to security, users gain the amount of control they need with a level of security that effectively prevents a cyberattack. To accomplish this, an organization should combine user awareness, cybersecurity training, and next-generation antivirus and data protection to generate the multifaceted solutions that are essential to protect endpoints from current and future cyberattacks.

The answer on where to go from here is simply this: protect sensitive corporate data throughout its life cycle by implementing a data-centric security approach.

Contact us for a **free consultation or to receive a FREE cloud security audit** to assess the effectiveness of your current cybersecurity initiatives.

**1.877.225.4264**

**www.calian.com**

CALIAN®

## References


Beazley, (2019, May 23). *Beazley breach insights – May 2019*. Retrieved from https://www.beazley.com/news/2019/beazley_breach_insights_may_2019.html?gclid=EAIaIQobChMIsYPP66y_4wIVg47ICh3LNQTyEAAYAyAAEgJcqfD_BwE

Brooks, C. (2017, March 21). *Keep calm and… Here is a list of alarming cybersecurity statistics*. Retrieved from https://itspmagazine.com/from-the-newsroom/keep-calm-and-here-is-a-list-of-alarming-cybersecurity-statistics

Carbon Black (2019, January). *Global threat report: Year of the next-gen cyberattack*. Retrieved from https://www.carbonblack.com/resources/threat-research/year-of-the-next-gen-cyberattack/

Check Point Research (n.d.). *Mobile cyberattacks impact every business*. A Check Point mobile threat research report. PDF

Cisco (2011). *Cisco 2011 Annual Security Report. Highlighting global security threats and trends*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/security_annual_report_2011.pdf

Cox Business. (n.d.). *12 DDoS statistics that should concern business leaders*. Retrieved from https://www.coxblue.com/12-ddos-statistics-that-should-concern-business-leaders/

Intel (n.d.). *A Guide to the Internet of Things. How billions of online objects are making the Web wiser*. Retrieved from https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

Malwarebytes Labs (2019). *2019 state of malware*. Retrieved from https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf

Palfy, Sandor (2018, June 14). *How much do passwords cost your business?* Retrieved from https://www.infosecurity-magazine.com/opinions/how-much-passwords-cost/

PKWARE (n.d.). *A blueprint for data-centric security.* Retrieved from https://pkware.cachefly.net/webdocs/pkware_pdfs/us_pdfs/white_papers/WP_Data_Centric_Security_Blueprint.pdf

Ponemon Institute LLC and Accenture (2019). *The cost of cybercrime. Ninth annual cost of cybercrime study: Unlocking the value of improved cybersecurity protection*. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Whittle, Sally (2008, March 10). *The top five internal security threats*. Retrieved from https://www.zdnet.com/article/the-top-five-internal-


CALIAN®


www.calian.com

1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8