CATO NETWORKS

SOMMITA TECHNOLOGY GROUP, LLC

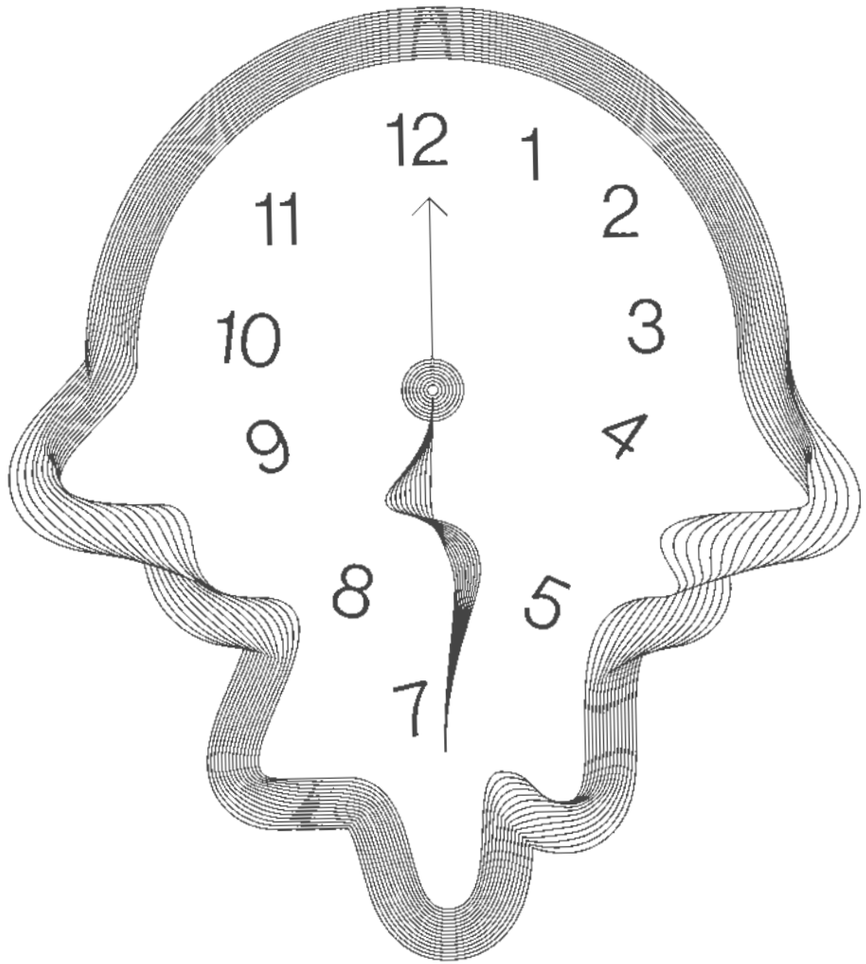
Ransomware Is On The Rise
Cato's Security-as-a-Service Can Help

Ransomware is not going away, in fact, as technology advances the attacks are becoming more sophisticated and with broader delivery capabilities. Not only that, but attackers realized that corporations would pay ransoms upwards of 7 figures to restore productivity.

Organizations that fall victim to ransomware face significant long-term damage, not just the obvious costs of paying the ransom or restoring the data.

1 Immediate Loss of Productivity

The loss of productivity cannot be universally quantified, as it varies from organization to organization. But if you consider the dependence of every organization on data and applications for day-to-day operations, it becomes easy to imagine the financial implications of everything coming to a complete halt. Payments cannot be sent or received, products cannot be designed, manufactured, or shipped. For some global enterprises, the losses could be millions of dollars per hour. It can take IT teams days or even weeks restore backups or attempt data recovery, making it very appealing to businesses to pay the ransom.



2

The Primary Ransom: Data Decryption

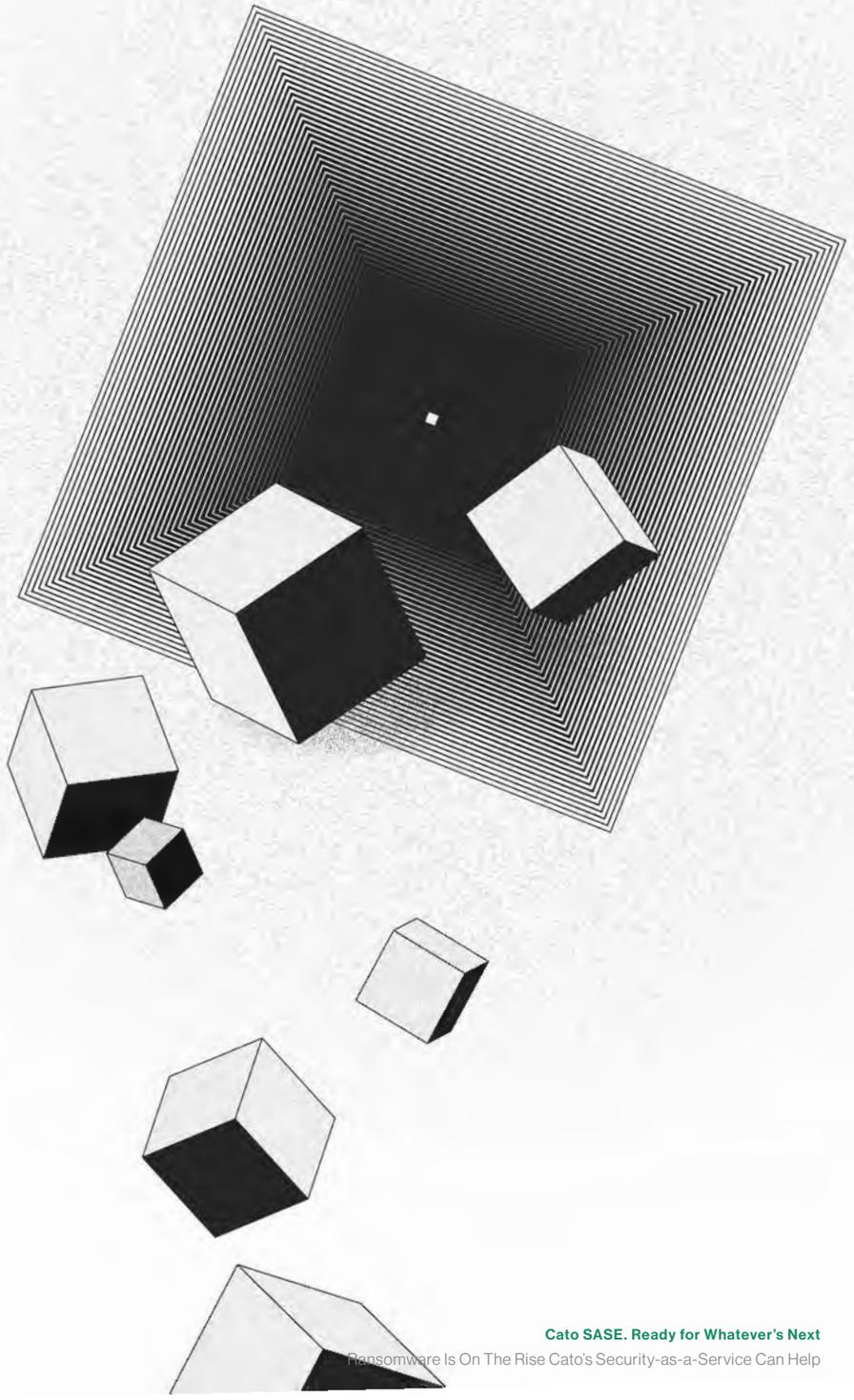
The primary ransom is the first hard cost of an attack. When your data is encrypted, a message will be displayed on impacted systems with instructions on how to send a payment. The ransom amount varies based on the type of ransomware; many will generate a price based on the volume of files that were encrypted. Or, if the attack is targeted towards a specific organization, the amount may be pre-determined. To further motivate victims, two tactics may be used: destruction of the private key after a certain amount of time, and/or increasing of the ransom price as time passed.

According to Cybercrime Magazine, the global cost of ransomware damages will exceed $20 billion in 2021 and $265 Billion by 2031.*

3 The Secondary Ransom: Data Privacy

When thinking about the risks associated with ransomware, it seems straight forward; your systems are infected and data is encrypted, you pay the ransom and can then access your data again. However, attackers have realized that instead of solely encrypting your data, they can also exfiltrate it and then charge a second ransom for keeping it private. The secondary ransom may even be higher than the first, as releasing the data publicly is more disruptive than simply losing access to it.

For example, the data may consist of financial, health or personal information of customers. The public release of this kind of information would violate privacy and protection laws leading to punitive damages and legal action. Alternatively, the data could be proprietary information such as product designs or customer lists. The exposure of this kind of information could result in reduced market share, or even complete loss of business viability. Once again, when faced with this decision, it almost seems logical to simply pay the ransom.



4

Long-term Damage: Organization Reputation

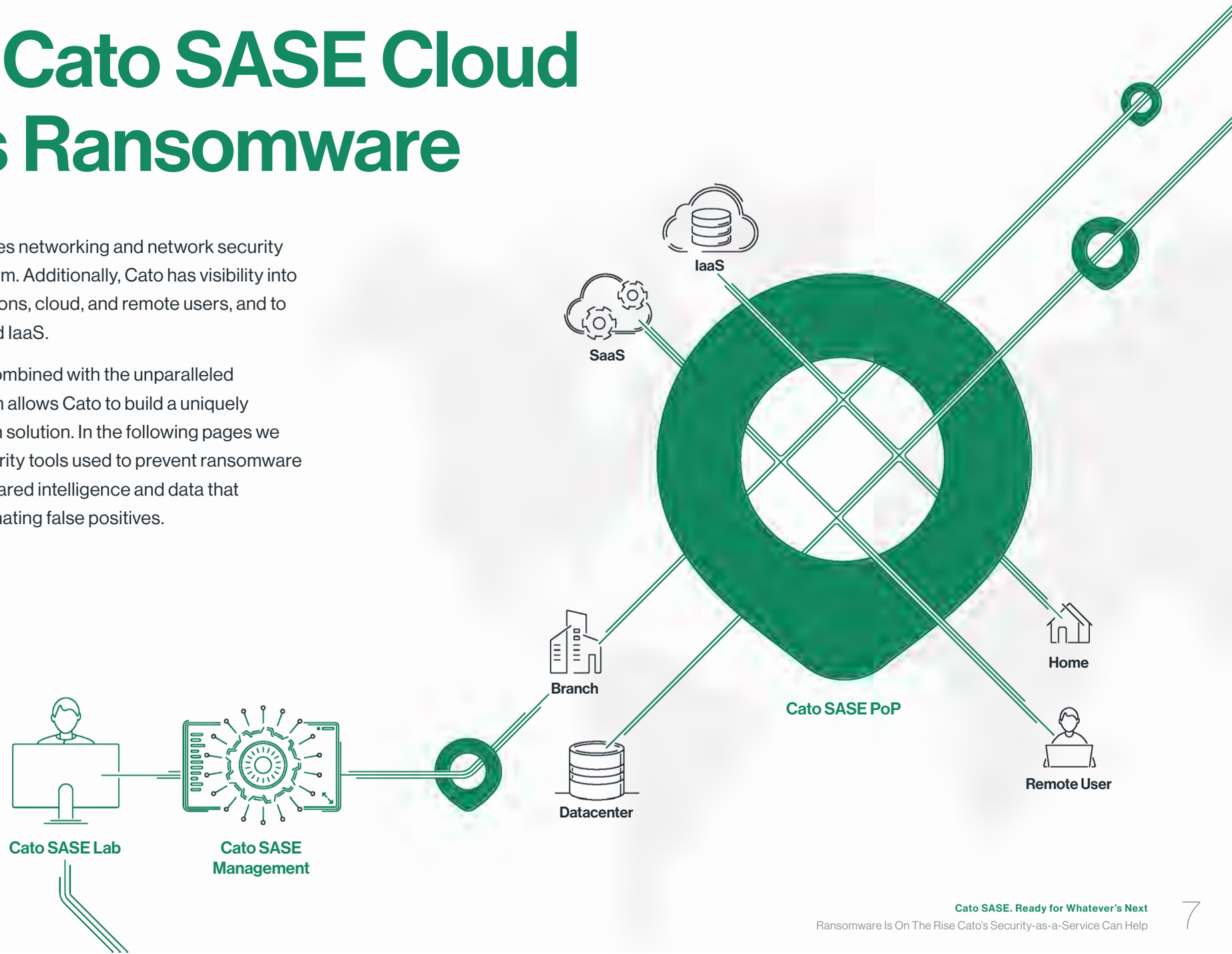
Even if an organization pays the secondary ransom and their data stays private, there is still the potential for long-term ramifications due to reputation damage. There are two fundamental areas for concern here, the disruptions to customers during the loss of productivity period and the perception of customers once they learn that the attack occurred.

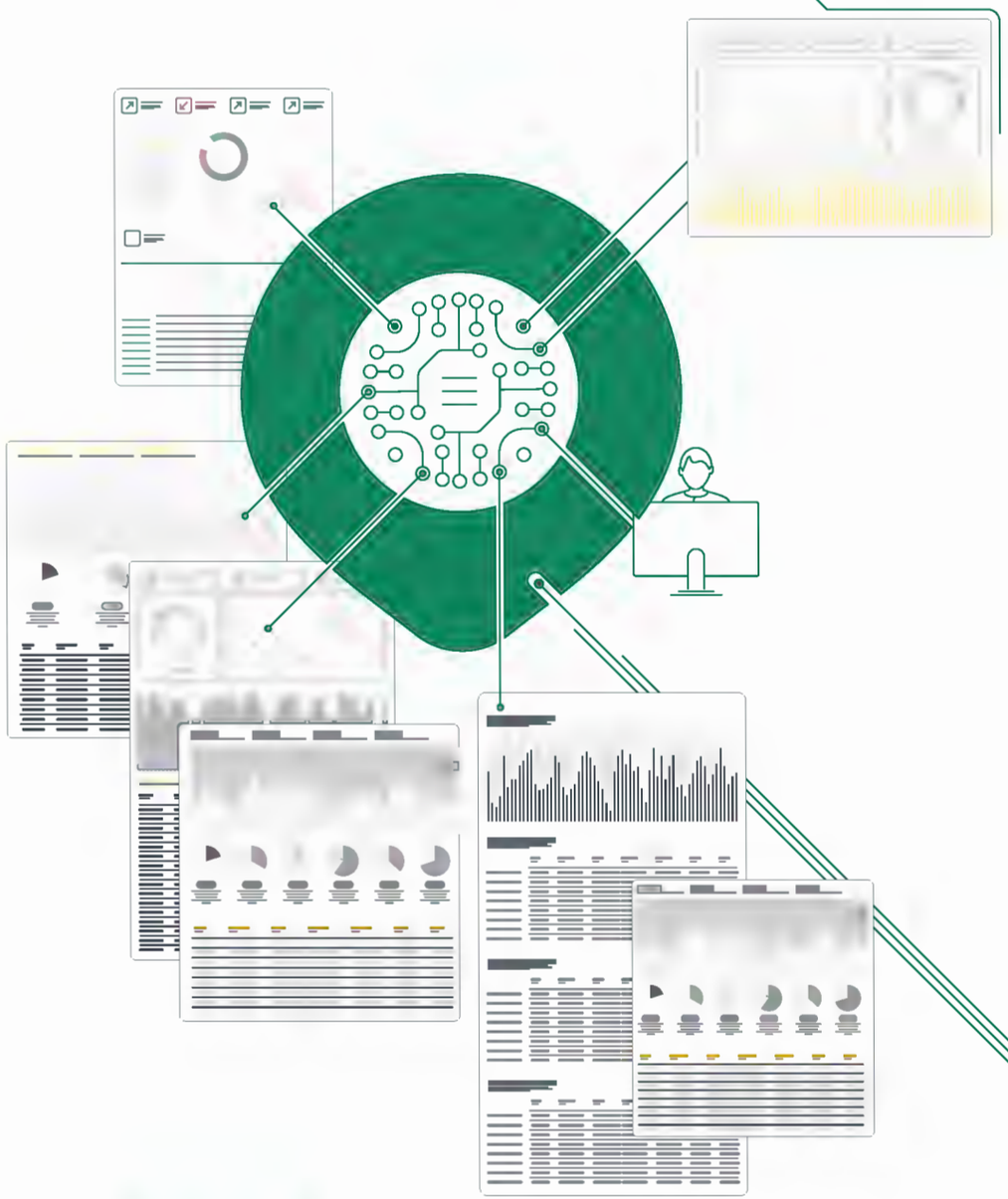
Customers quickly develop negative feelings when their delivery goods and services are delayed or canceled, especially if the chaos of the situation makes it difficult to communicate with the business. Once knowledge of the attack becomes public, customers begin to question if their information is safe and if they should consider doing business with that organization.

How the Cato SASE Cloud Prevents Ransomware

The Cato SASE cloud fully converges networking and network security into a single, cloud-delivered platform. Additionally, Cato has visibility into all traffic flows from all edges: locations, cloud, and remote users, and to all resources: on-premise, SaaS and IaaS.

This fully converged architecture combined with the unparalleled visibility of our cloud-native platform allows Cato to build a uniquely comprehensive malware prevention solution. In the following pages we will detail the multiple layers of security tools used to prevent ransomware and other malware as well as the shared intelligence and data that increase efficacy while nearly eliminating false positives.





Reputation Data & Threat Intelligence

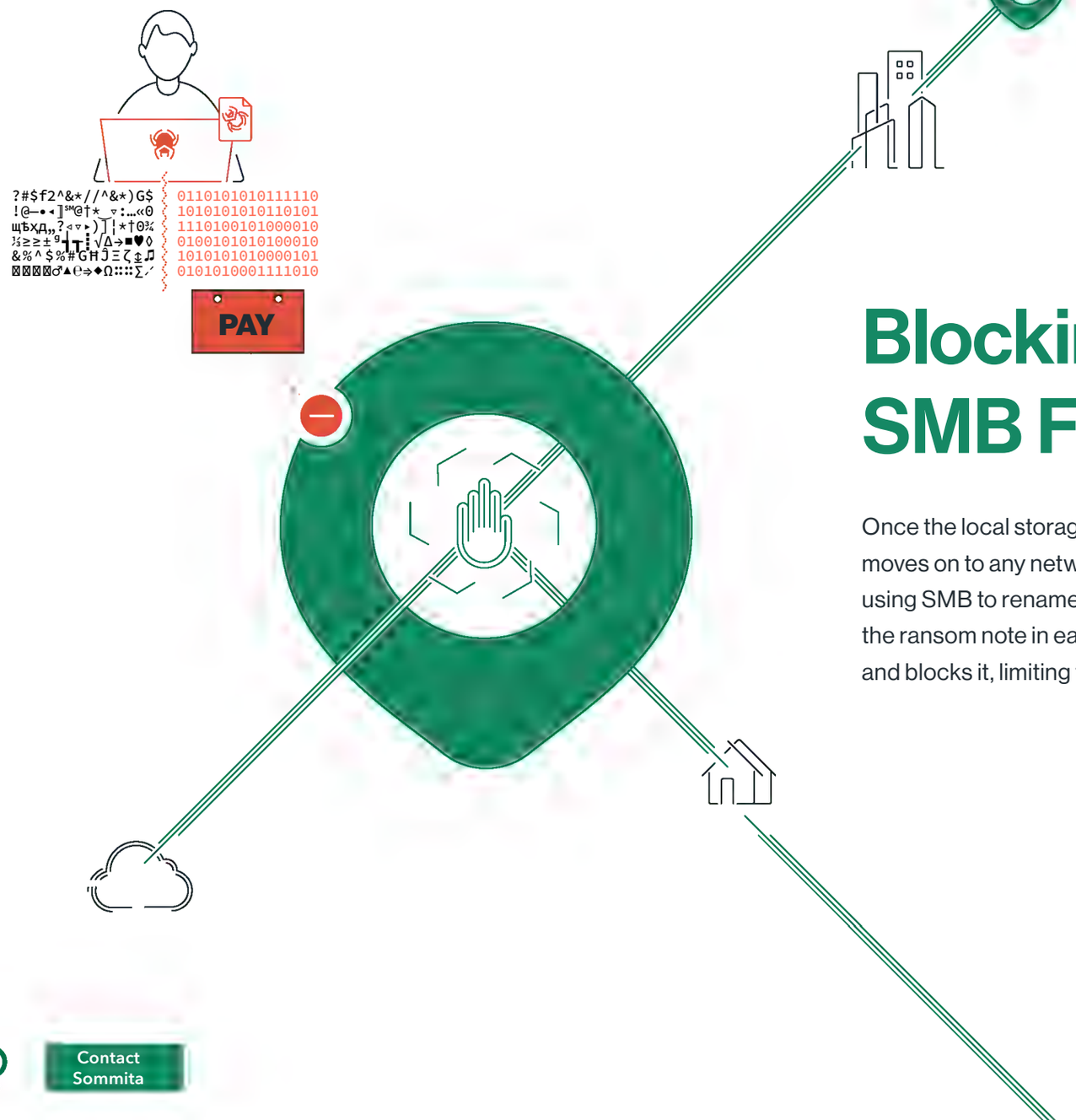
Cato leverages hundreds of threat intelligence feeds to ensure customers always have the best protection. These feeds come from open-source, shared communities and commercial providers have greatly varying levels of quality.

Cato's security team found that even after applying industry best practices, 30 percent of feeds contain false positives or miss IoCs. To eliminate false positives, Cato developed a purpose-built in-house system that uses machine learning models and AI to correlate networking and security information. This system allows Cato to aggregate millions of records from these feeds, scoring them for timeliness and accuracy, and then pushing them into production multiple times per day.

Blocking Command and Control Communication

The first stage of a ransomware attack is delivery and execution of the software payload, whether unknowingly by a user or from another malicious file. Once executed, the software connects to the attacker's command and control server(s) and send information about the host victim.

Cato's IPS prevents delivery of ransomware to machine, but users may be infected via other threat vectors such as USB devices. Once infected, communication with the command-and-control server is still necessary to transfer encryption keys and exfiltrate data. This communication is disrupted by Cato's IPS, preventing encryption of files.

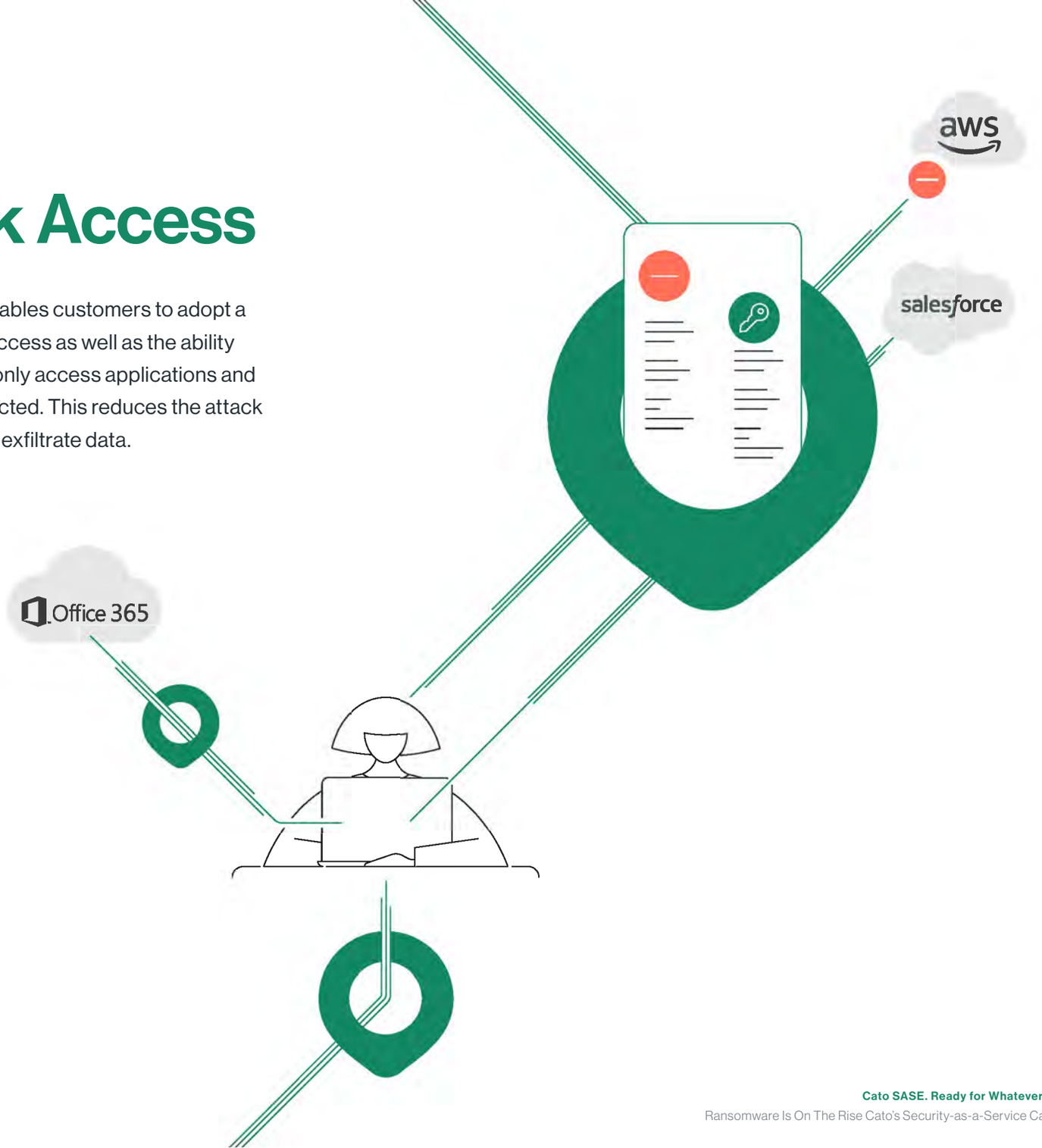


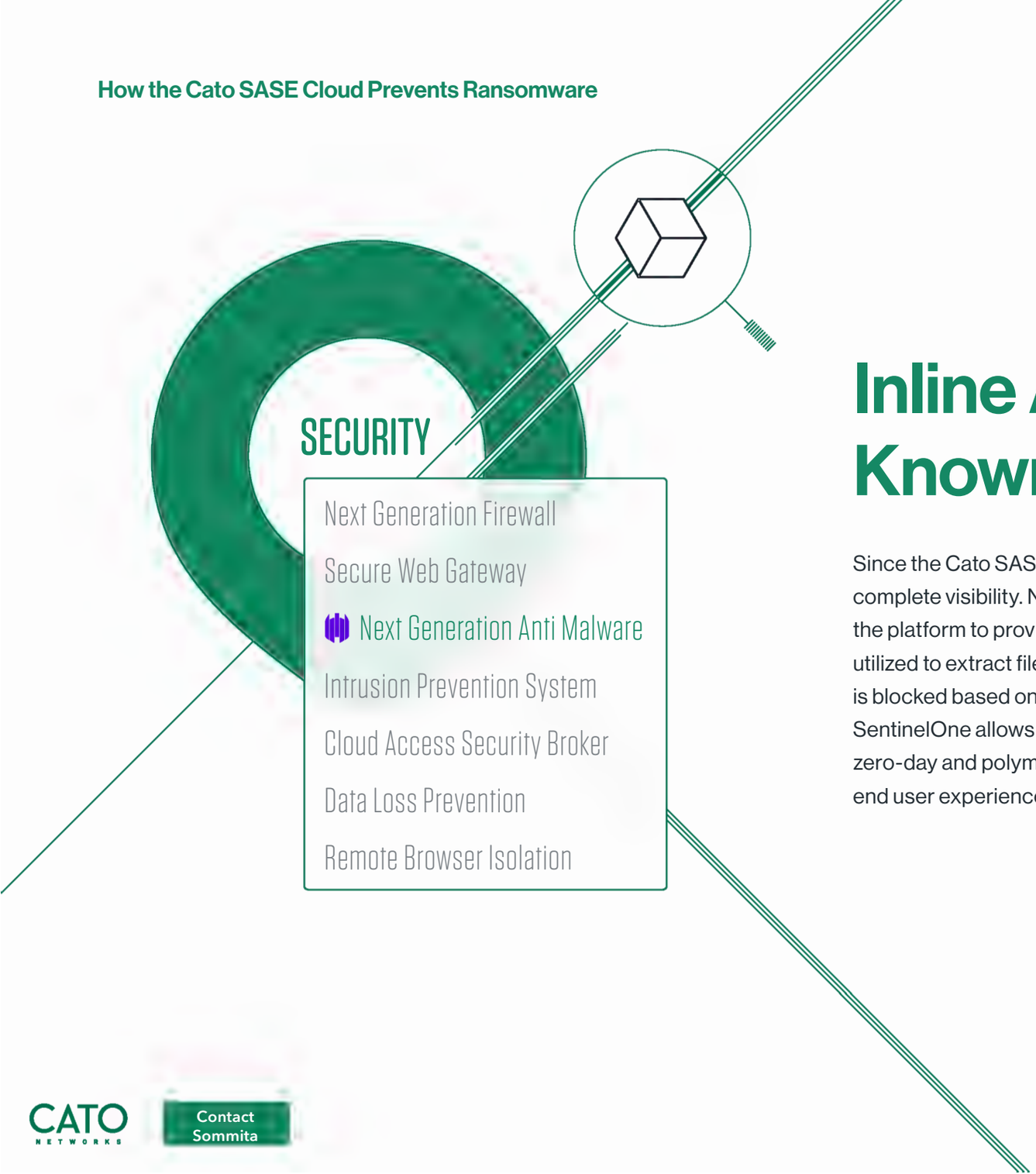
Blocking Suspicious SMB File Activity

Once the local storage and attached USB devices are encrypted, the ransomware moves on to any network attached storage that is accessible. Typically, this means using SMB to rename or change the extensions of as the files encrypted, and leaving the ransom note in each directory. Cato's IPS detects this irregular network activity and blocks it, limiting the impact of the attack.

Zero Trust Network Access

Beyond prevention with Cato's IPS, the Cato SASE Cloud enables customers to adopt a complete zero-trust approach to application and resource access as well as the ability to incorporate network segmentation. Users and hosts can only access applications and resources for which they are authorized, with all traffic inspected. This reduces the attack surface, limiting ransomware's ability to spread, encrypt and exfiltrate data.



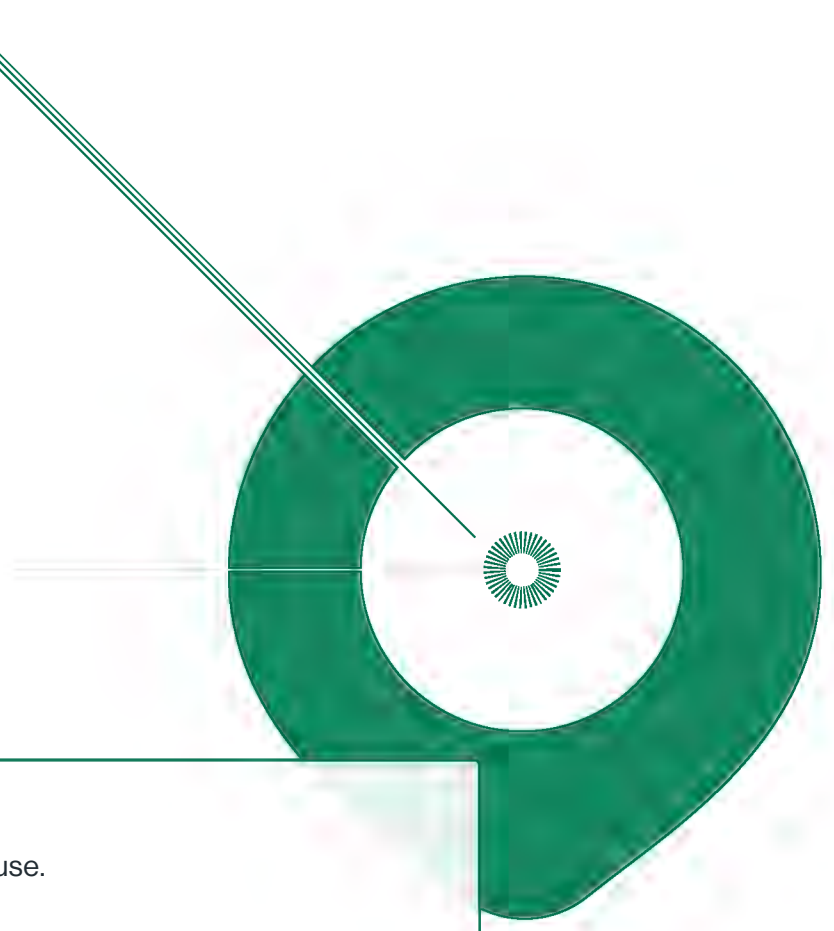


Inline Anti-malware Stops Known and Zero-Day Threats

Since the Cato SASE cloud sits in-line with all user and location traffic, the service has complete visibility. Next-generation firewall architecture and TLS inspection, enable the platform to provide broad coverage for your organization. Deep packet inspection is utilized to extract file objects from the stream and block when appropriate. Known malware is blocked based on global threat intelligence databases, while our partnership with SentinelOne allows us to use machine learning and artificial intelligence to protect against zero-day and polymorphic malware. All of this happens at line speed, with no impact to the end user experience.

An IPS that sees the full picture, not a partial one

Just like Cato's anti-malware, Cato's IPS has access to unique data and capabilities across multiple security layers not typically available to IPS.



Intrusion Prevention System

Layer-7 Application Awareness
Allows visibility and understanding of the application in use.

User Identity Awareness
Enables correlation between network flows and the specific user behind them.

User Agent/Client Fingerprint
Provides visibility to the software agent in use, and identification of non-standard agents.

True File Type
Ensures files are accurately identified, not solely based on their file extension

Target Domain/IP Reputation
Automatically block known bad sources

Traffic Attributes Including Source/Destination Country
Reduce the attack surface by allowing traffic only from trusted countries

Behavioral Signature and Heuristics
Stop zero-day attacks and polymorphic variants of known threats

Reputation Feeds
Detect and prevent inbound or outbound communication with compromised or malicious resources, with nearly no false positives.

Protocol Validation
Reduce the attack surface by ensuring the packet conforms to the specified protocol

Network Behavioral Analysis
Prevents inbound/outbound network scans.

Scale Your Security Team with the Cato MDR Service

Prevention efforts are critical to a strong security posture, but organizations should always address the presumption of infection. Cato can offload this resource and skill dependent process of detecting compromised endpoint to the Cato SOC. This requires no added install footprint as Cato already serves as the customer's SASE platform, supplying unparalleled visibility into all traffic from all devices.

The Cato MDR Service offers the following capabilities:

Automated Threat Hunting

Human Verification

Network-Level Threat Containment

Guided Remediation

Reporting & Tracking

Assessment Check-Ups

Like other types of attacks, the Cato MDR service can help you identify ransomware before it activates. Lateral movement attempts are detected and reported to customers for immediate action in containing and remediating targeted attacks. Additionally, host behavior is baselined, allowing for detection of suspicious activities that might be related to targeted attacks. The Cato MDR service gives your network an extra set of eyes to detect, isolate and remediate threats.

Appendix

Sample Ransomware Attacks

AIDS Trojan

The very first documented example of ransomware was the AIDS Trojan by Dr. Joseph Popp in 1989. What is most interesting about the AIDS Trojan, also known as PC Cyborg, is that Popp mailed 20,000 victims (about the seating capacity of Madison Square Garden) an infected floppy disk labeled “AIDS Information Introductory Diskette.” These disks held software disguised as a survey, but would infect the host machine, and trigger after a number (typically 90) of system reboots. Once triggered, the file names and ext.ensions on the system would be encrypted and could no longer be executed. To regain access, victims had to mail $189.00 to Popp’s P.O. box in Panama.

Whether financially or politically motivated, bad actors will continue to find appeal with the low-risk, easy distribution of ransomware attacks. In just the first half of 2021 the world saw many high-profile attacks, here are just a few:

Colonial Pipeline

Ransomware disrupted the Colonial Pipeline and disrupted gasoline supplies along the East Coast of the United States. $4.4 million worth of bitcoin was paid in ransom, though this was later recovered by the FBI.

JBS Foods

Not long after the Colonial Pipeline attack, JBS foods, one of the biggest meat processing companies in the world, was hit. JBS paid $11 million of bitcoin in ransom, one of the largest payments of all time.

AXA

Around the same time as JBS foods, AXA a European insurance company was attacked. This attack came shortly after announcing that they would stop reimbursing their clients for ransomware payments. Attackers were able to exfiltrate 3TB of AXA’s data.

KIA Motors

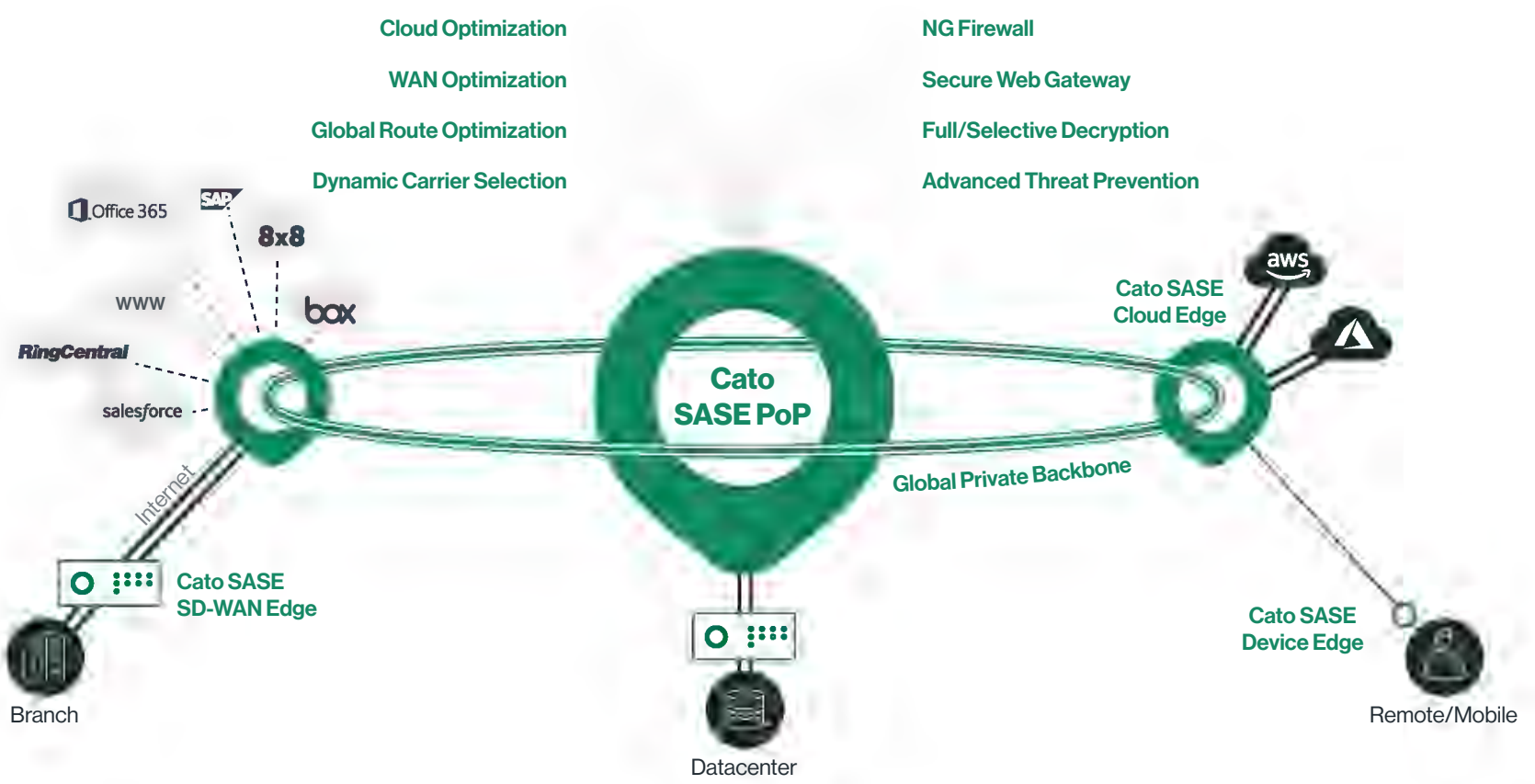
KIA Motors, a subsidiary of Korean automaker Hyundai reported widespread IT and systems outages, but never confirmed an attack. The DoppelPaymer gang claims to have attacked them and demanded a $20 million ransom, even releasing some stolen data.

Ransomware is not only here to stay, but is accelerating, both in frequency and demand amount. In 2019 a new company was affected by ransomware every 14 seconds, in 2021 this is estimated to occur every 11 seconds. The average ransomware demand grew 30X in just over a year, from $6,000 in 2018 to $178,000 in the first half of 2020. **

** https://www.cloudwards.net/ransomware-statistics/
* https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato SASE Cloud, customers easily migrate from MPLS to SD-WAN, improve connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud data centers and remote users into the network with a zero-trust architecture. With Cato, your network and business are ready for whatever's next.



Cato SASE. Ready for Whatever's Next

Cato SASE Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Secure Remote Access
- Unified Management Application

Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management
- Site Deployment

SOC2 Approved

ISO 27001 Certified

GDPR Compliant

Gartner peerinsights Customer first

CATO NETWORKS

Contact Sommita