MANAGED SOLUTIONS

Fact Sheet

CROWN CASTLE

Advanced Threat Protection

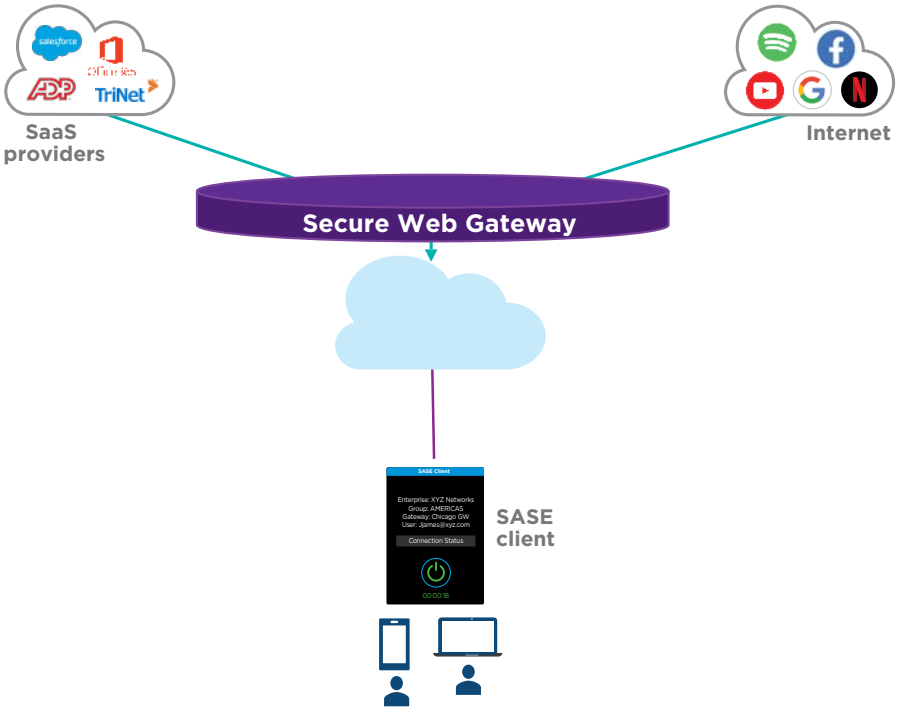
As cyber threats evolve and intensify in both frequency and sophistication, it's clear that traditional security measures are falling short. This reality underscores the need for organizations to proactively bolster their security posture with more advanced, agile and intelligent security systems than ever before to defend against advanced threats like zero-day exploits, advanced persistent threats, ransomware and phishing attacks.

Our Advanced Threat Protection (ATP) can be added to your Secure Remote User solution, combining AI-driven file analytics and sandboxing to create a security shield against these growing cyber threats. By isolating and examining suspicious files in a safe, controlled environment, sandboxing reveals hidden threats and generates invaluable threat intelligence. This intelligence offers real-time insights into emerging threats and attack modes, enabling proactive defenses.

ATP provides in-depth visibility and context for network traffic, user behavior and security events, ensuring your team can respond quickly and allowing you to make informed, proactive decisions to enhance your organization's defenses.

How it works

Our ATP works by performing a preliminary analysis and evaluation of files, followed by cloud multi-sandboxing for zero-day protection.

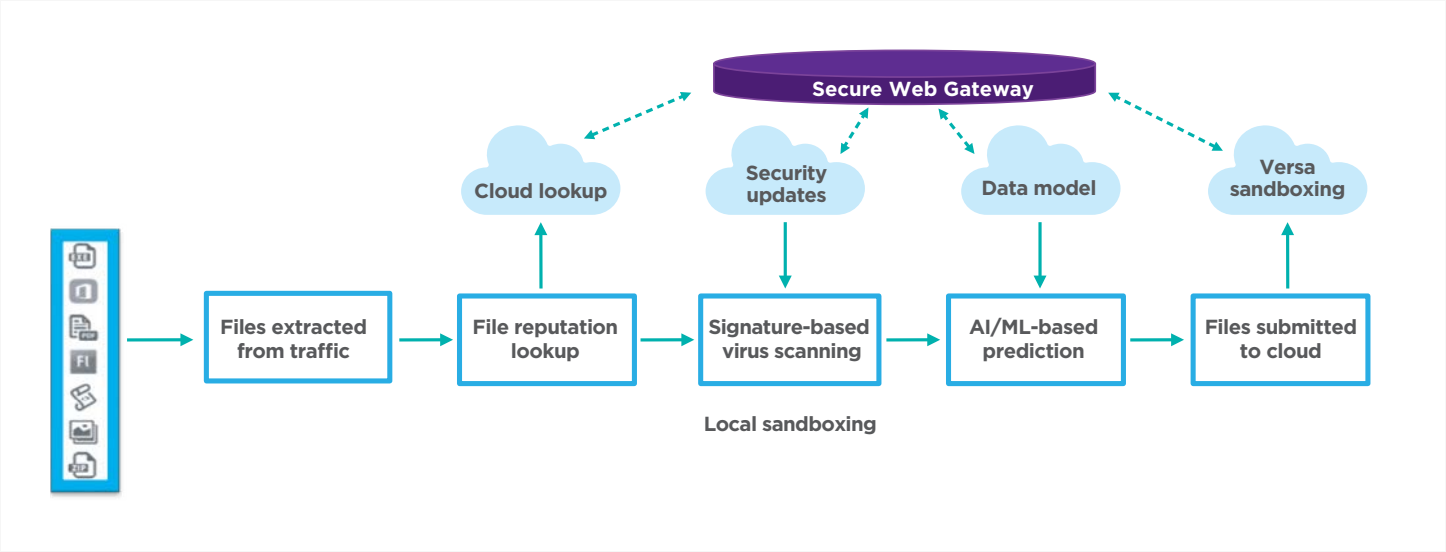


Local file analytics and sandboxing

Our local sandboxing inspects all files and performs file reputation lookup at the on-premises operating system device. Local analysis capabilities allow for potential risks and threats to be identified early in the process, providing faster threat detection and response times.

File reputation and signature analysis: Based on the file type, files are extracted from the traffic and reconstructed to compute an SHA-based checksum. A cloud lookup cross-references the file's checksum reputation in our sandbox cloud. If it's not found, recursive API lookups are performed in third-party databases and cached in our cloud. The onboard antivirus engine analyzes the file, which performs signature and heuristic-based detection. This multi-layered approach ensures known and unknown threats are effectively detected and blocked.

Static and artificial intelligence (AI) and machine learning (ML) analysis: Our ATP leverages AI and ML technologies to continuously enhance its threat detection and response capabilities. A lightweight AI/ML service runs locally on our operating system, receiving data model updates from our sandbox cloud as needed. It then analyzes the file against the trained data model, helping reduce the number of files submitted to the cloud for further sandboxing and enhancing the end-user experience. A static analysis, including a rule-based approach to identify and classify malware families, is also performed to immediately identify any indicators of compromise (IoC).



Multi-sandboxing in the cloud

After local analysis, the cloud sandboxing capability performs multi-layer analysis involving static and dynamic analysis and AI-based detection and identification using multiple antivirus engines. Suspicious files are sent to the cloud, where they undergo comprehensive analysis using multiple detection modules designed to identify hidden malicious behavior. ATP uses multiple unique detection methods and techniques to augment its sandboxing capabilities. This increases the chances of detecting advanced threats capable of evading a single specific type of sandbox environment, providing a more robust defense against sophisticated attacks.

Multiple AV engines: ATP employs multiple cloud-based antivirus engines to bolster its malware detection capabilities. By leveraging the collective intelligence of these engines, the platform can detect and block a broader range of threats, including previously unknown malware variants and zero-day exploits.

Static and dynamic analysis: We incorporate static and dynamic analysis methods to improve our threat detection capabilities. Static analysis examines files without executing them, processes them and analyzes their code structure and content for signs of malicious behavior and indicators of compromise (IoCs). The dynamic analysis also runs files in a controlled environment to observe their behavior and identify hidden threats. Using both methods, ATP ensures a comprehensive and accurate analysis of potential threats, resulting in a more effective defense against advanced attacks.

Sandbox analysis report example.

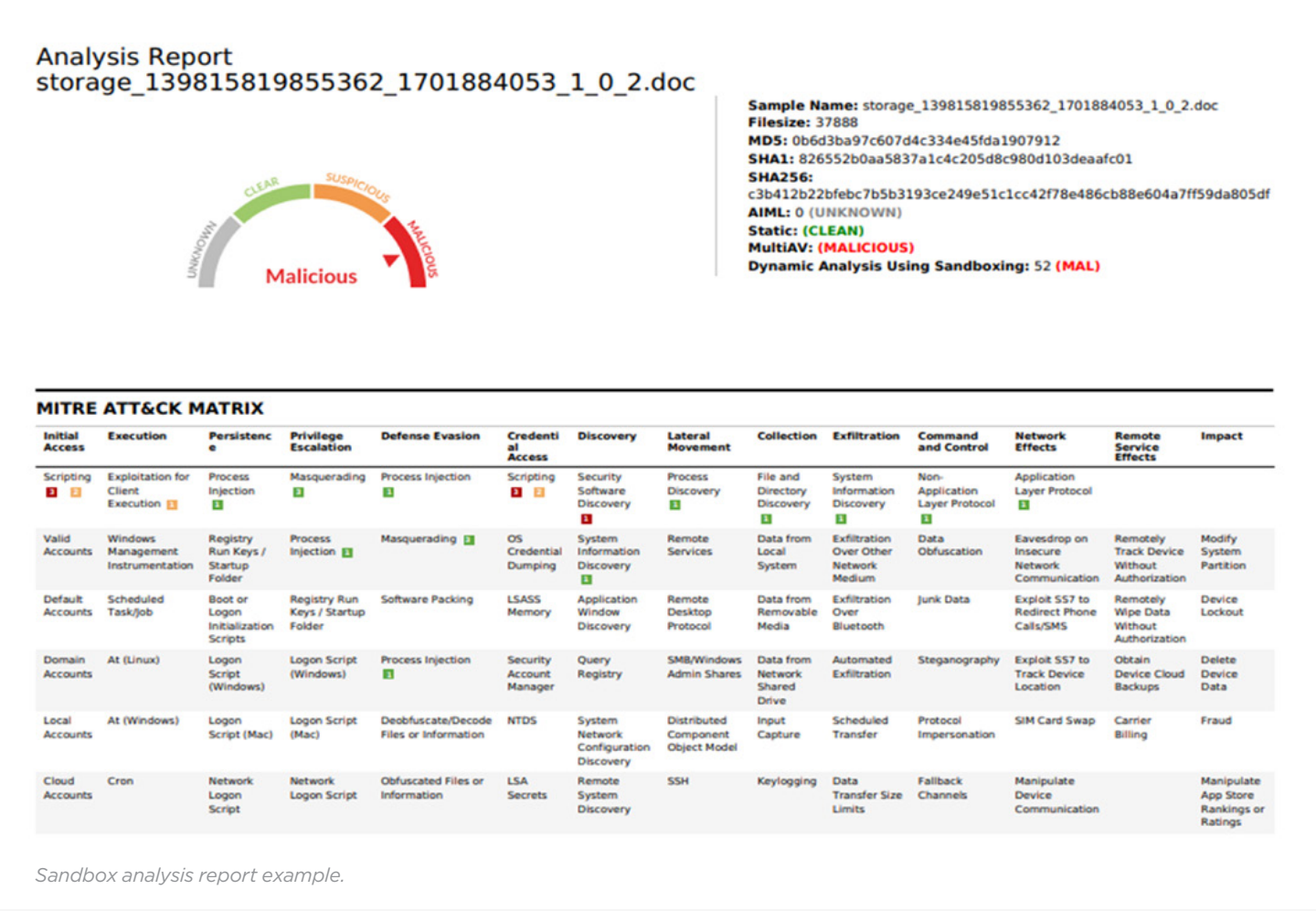
Static and AI/ML analysis: AI and ML-driven threat detection and response capabilities are trained against a sample of eight billion files, enhancing accuracy and efficiency in detecting threats. The data model constantly evolves as it analyzes new samples, which provides fast and precise detection of zero-day and advanced persistent threat (APT) attacks.

Deception countermeasures: Our ATP is designed to counter the deception techniques frequently used by cybercriminals. By incorporating advanced heuristics, behavior analysis and contextual awareness, the system can identify and respond to deception tactics, such as obfuscated code, polymorphic malware and other evasive techniques attackers use to bypass security measures.

Reporting and visibility

With robust reporting and visibility features, our ATP allows you to maintain a proactive and adaptive security approach through in-depth insights into network traffic, user behavior and security events.

Sandbox analysis reports: Sandboxing generates detailed reports on the analysis performed by each detection module. These reports provide insights into the behavior of potential threats, highlighting any malicious activities or patterns detected during the analysis. As a result, you can fine-tune your security policies and strategies to counter specific attack vectors more effectively by understanding the nature of the threats targeting your networks.



Analysis Report
storage_139815819855362_1701884053_1_0_2.doc

Sample Name: storage_139815819855362_1701884053_1_0_2.doc
Filesize: 37888
MD5: 0b6d3ba97c607d4c334e45fda1907912
SHA1: 826552b0aa5837a1c4c205d8c980d103deaafc01
SHA256: c3b412b22bfebc7b5b3193ce249e51c1cc42f78e486cb88e604a7ff59da805df
AIML: 0 (UNKNOWN)
Static: (CLEAN)
MultiAV: (MALICIOUS)
Dynamic Analysis Using Sandboxing: 52 (MAL)

MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Scripting	Exploitation for Client Execution	Process Injection	Masquerading	Process Injection	Scripting	Security Software Discovery	Process Discovery	File and Directory Discovery	System Information Discovery	Non-Application Layer Protocol	Application Layer Protocol		
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Process Injection	Masquerading	OS Credential Dumping	System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder	Software Packing	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Carrier Billing	Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

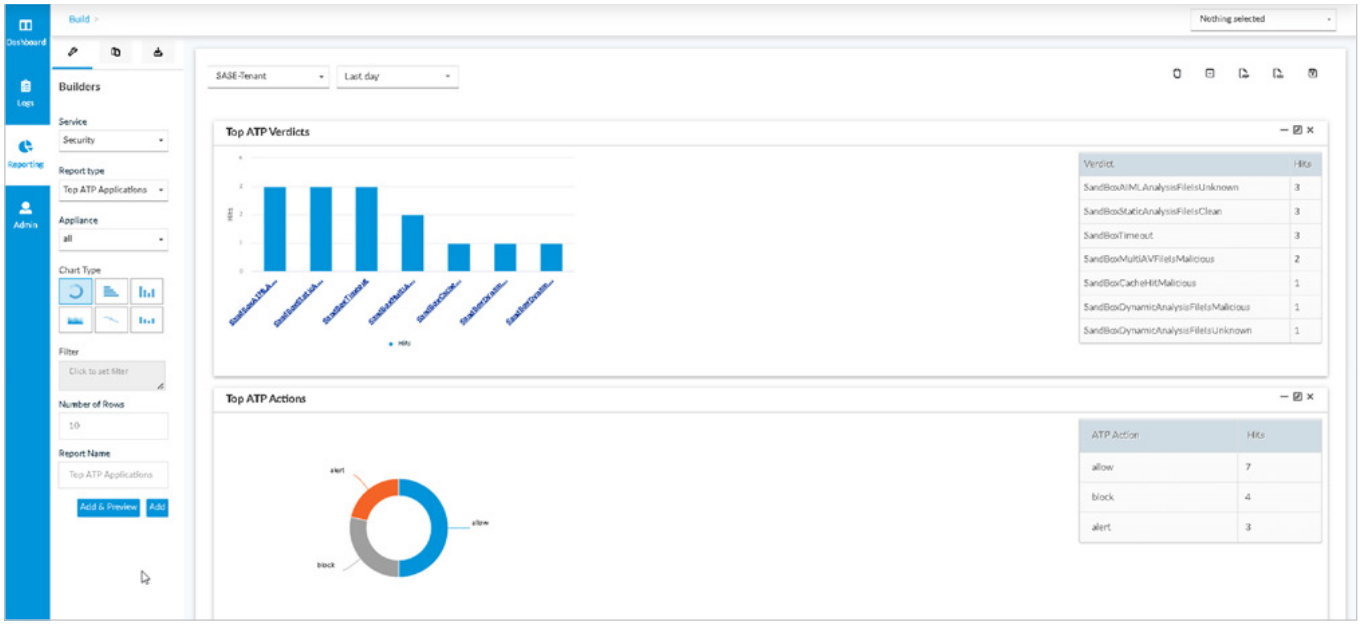
Sandbox analysis report example.

Real-time dashboard: ATP offers a real-time dashboard that provides an at-a-glance view of your security status, network traffic and user activity, including intelligence gleaned from the sandboxing system. This customizable dashboard enables your security team to focus on the most relevant information for your organization and quickly identify and respond to potential security incidents before they escalate.

Traffic logs and reporting: You'll receive a comprehensive traffic logging and reporting system that captures detailed information about network activity. These logs can be filtered and analyzed to identify patterns, trends and anomalies indicating potential security threats to detect and respond to emerging threats more effectively.

Customizable reports: Our SASE solutions allow you to generate customized reports tailored to your needs, including reports on ATP findings. This flexibility allows your security team to focus on the most relevant data and insights, making it easier to identify trends, track progress and measure the effectiveness of ATP performance.

Role-based access control: To ensure that the right individuals have access to the appropriate level of information, our ATP supports role-based access control. This feature allows you to define user roles and assign appropriate access levels to different reports, dashboards and analytics, ensuring that sensitive data is only accessible to authorized personnel.



Example of a customizable report.

Why Crown Castle?

Our unique, nationwide portfolio
With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record
In our 30+ years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise
We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

Our solutions
We have your networking and security needs covered. Visit our infrastructure solutions page to learn more about our suite of solutions and how they can solve your toughest challenges.

CROWN CASTLE

Crown Castle owns, operates and leases approximately 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 1-888-516-5059 or visit **CrownCastle.com**

CC-0725-0122