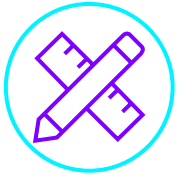




THE ACCENTURE CYBER DEFENSE SOLUTION

A MANAGED SERVICE FOR
CYBER DEFENSE FROM
ACCENTURE AND SPLUNK.

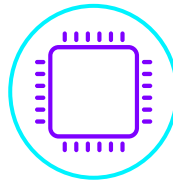


YOUR CURRENT APPROACHES TO CYBER DEFENSE COULD BE PUTTING YOU AT RISK

Cyber-attacks are increasingly threatening and costly. They drain \$450 billion¹ annually from the global economy—a number that some project will reach \$2 trillion² by 2019. Highly sophisticated attackers can hide their tracks for weeks, months and even years without being noticed. Organizations need to match that sophistication in their defensive tactics and in their ability to bounce back quickly if a breach does occur.

Most companies focus cybersecurity investments on detection and remediation. But that alone is not enough to fight the high volume and advanced level of today's attacks, especially across endpoints and networks. Overwhelming data volumes slow the responses of traditional security information and event management tools. Companies also struggle to manage and track the large number of available data center and cloud cybersecurity technologies.

To be successful, three crucial ingredients are needed: visibility across the entire organization, a layered approach to defense, and solutions that are purpose-built from the inside out to provide protection for their industry's specific needs. What's required is an increased ability to see the environment from end-to-end, capturing security events and detecting anomalies as they occur, and a way to quickly generate meaningful insights to respond, strategically and tactically, in near real-time.



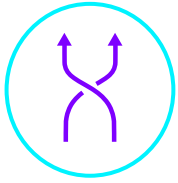
AN ACCENTURE - SPLUNK CYBER DEFENSE SOLUTION

Fortunately, companies now have a new weapon: a highly advanced managed cyber defense solution from Accenture and Splunk. The comprehensive solution employs tools such as machine learning, analytics and automation to provide the advanced search, correlation, threat detection and incident management capabilities needed to more effectively thwart cyber-attacks. To power these tools and processes, Accenture and Splunk collect, analyze and act upon all data that is available to them from structured and unstructured as well as private and public sources. These include logs, clickstreams, sensors, web servers, custom applications, hypervisors, containers, operational technology, social media and cloud services.



THE RESULTS ARE RAPID

Accenture and Splunk's cyber defense solution helps organizations respond to and remediate sophisticated cyber threats at both speed and at scale. This data-driven security solution employs an array of technologies, combining both Accenture and Splunk's unique and proprietary capabilities. It's a platform that provides a comprehensive approach, including behavioral analytics which enable security teams to quickly detect and respond to threats based on a broader context than is possible with legacy security products.

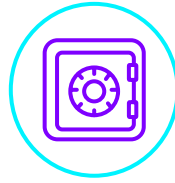


FLEXIBLE AND EFFECTIVE

Companies need to consider how to most effectively deploy their security solutions and resources. Accenture and Splunk provide guidance to help clients understand the best approach based on their unique requirements - on premise, in the cloud or in a hybrid cloud environment with additional options for the solutions to be operated in-house, or managed by Accenture as an integrated service.

With continuing innovations from Accenture and Splunk, companies can:

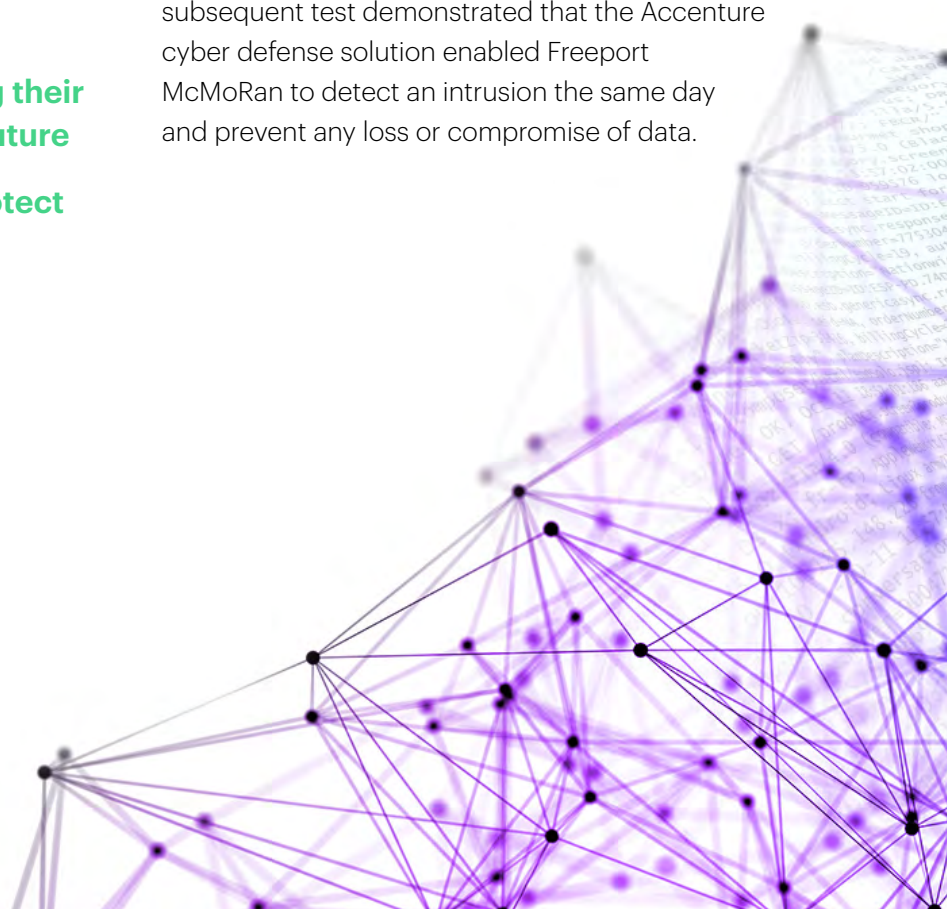
- Reduce the number of point products, which in turn reduces complexity and cost
- Increase resilience
- Mitigate risk
- Prepare for the threats affecting their specific industry, present and future
- Build end-to-end security to protect their entire value chain
- Enhance compliance
- Keep pace with even the most sophisticated attackers



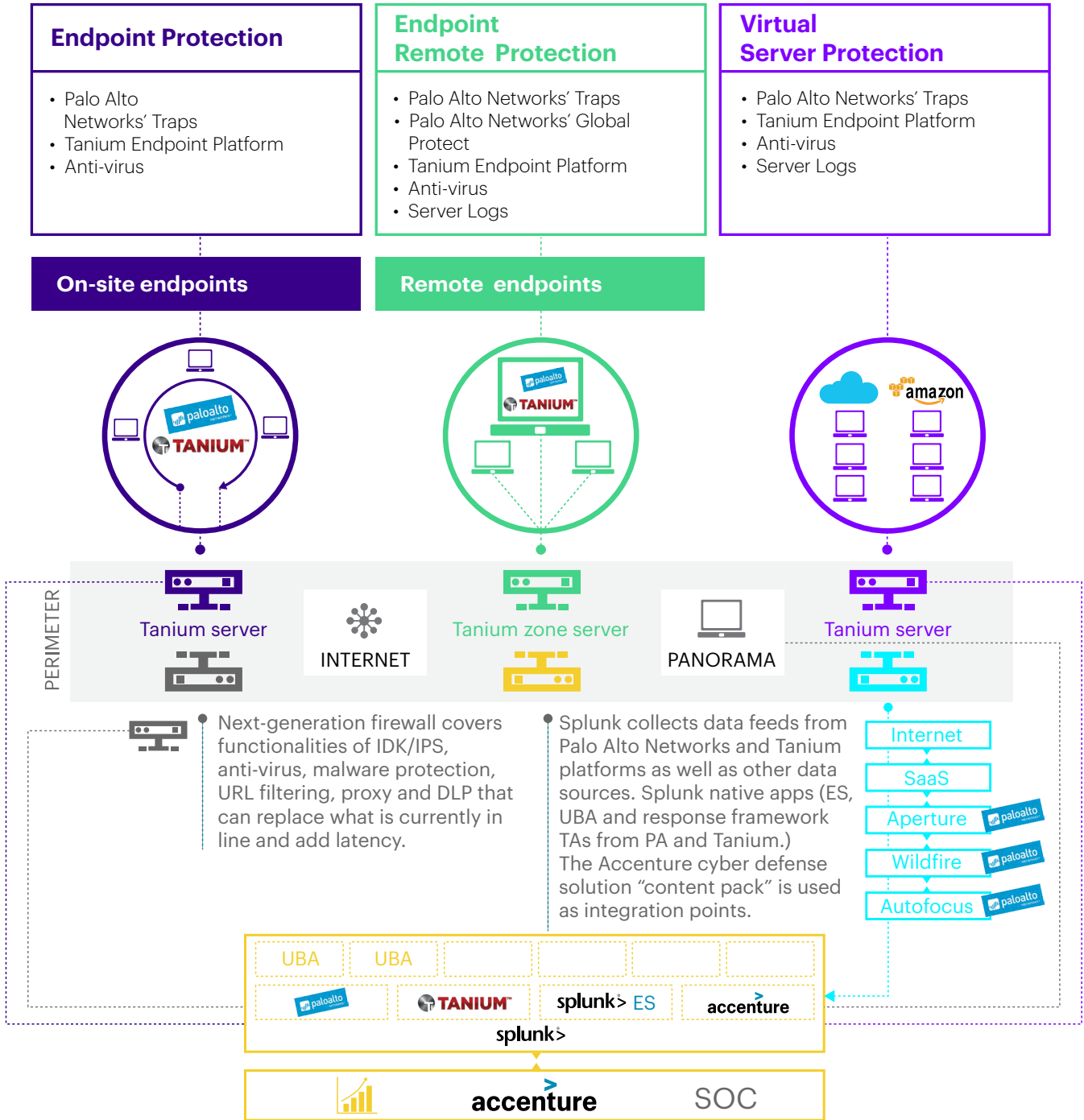
REAL-TIME CYBERSECURITY PROTECTION AT FREEPORT MCMORAN

Freeport-McMoRan Inc., a premier international natural resources company, taps into the Accenture cyber defense solution to help secure its hybrid cloud enterprise as a service. Accenture's solution provides a scalable, affordable, fast and standardized managed security service that helps Freeport-McMoRan rapidly understand its security environment to get ahead of threats that target its hybrid cloud.

Before Freeport-McMoRan began using the Accenture cyber defense solution, a cyber security stress test contractor discovered that its "red team" could reside in the company's systems and extract data undetected for several days. A subsequent test demonstrated that the Accenture cyber defense solution enabled Freeport McMoRan to detect an intrusion the same day and prevent any loss or compromise of data.



CYBER DEFENSE PLATFORM SCHEMATIC





A POWERFUL COLLABORATION BY INDUSTRY LEADERS IN CYBER SECURITY

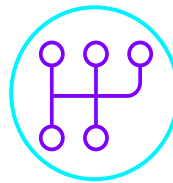
The Accenture cyber defense solution includes members of a broader ecosystem. For example, the solution includes Accenture and Splunk, as well as:

- Palo Alto Networks, a next-generation security company leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide.
- Tanium, which automates and integrates cyber threat intelligence, and delivers precise and granular endpoint threat detection and remediation at network speeds.

The combination and integration of these industry leaders powers a host of integrated solutions. Consider one example: mitigating the risks of ransomware. Ransomware typically installs itself after a victim clicks an attachment or link in a phishing email, or when a victim visits a hacked website that runs code that can exploit vulnerabilities in the underlying operating system of the user's device.

How does the Accenture cyber defense solution respond? In this scenario, Splunk collects logs from an organization's firewalls and endpoints, correlating and analyzing that data to find suspicious events. Splunk can then launch endpoint scans in Tanium and automatically quarantine infected hosts.

Incident responders can download indicators of compromise (IOCs) with Tanium IOC Detect which provides an automated way to run scheduled detection scans against endpoints. In this case, Tanium Connect checks in with the Palo Alto Networks's Next Generation Firewall to see if it has encountered a possible threat. If so, the data will be forwarded to WildFire— Palo Alto Networks's cloud-based threat analysis service. Tanium Connect will query WildFire for the IOC it created. After Tanium downloads the new IOC, an analyst can run a detection scan against the endpoints.



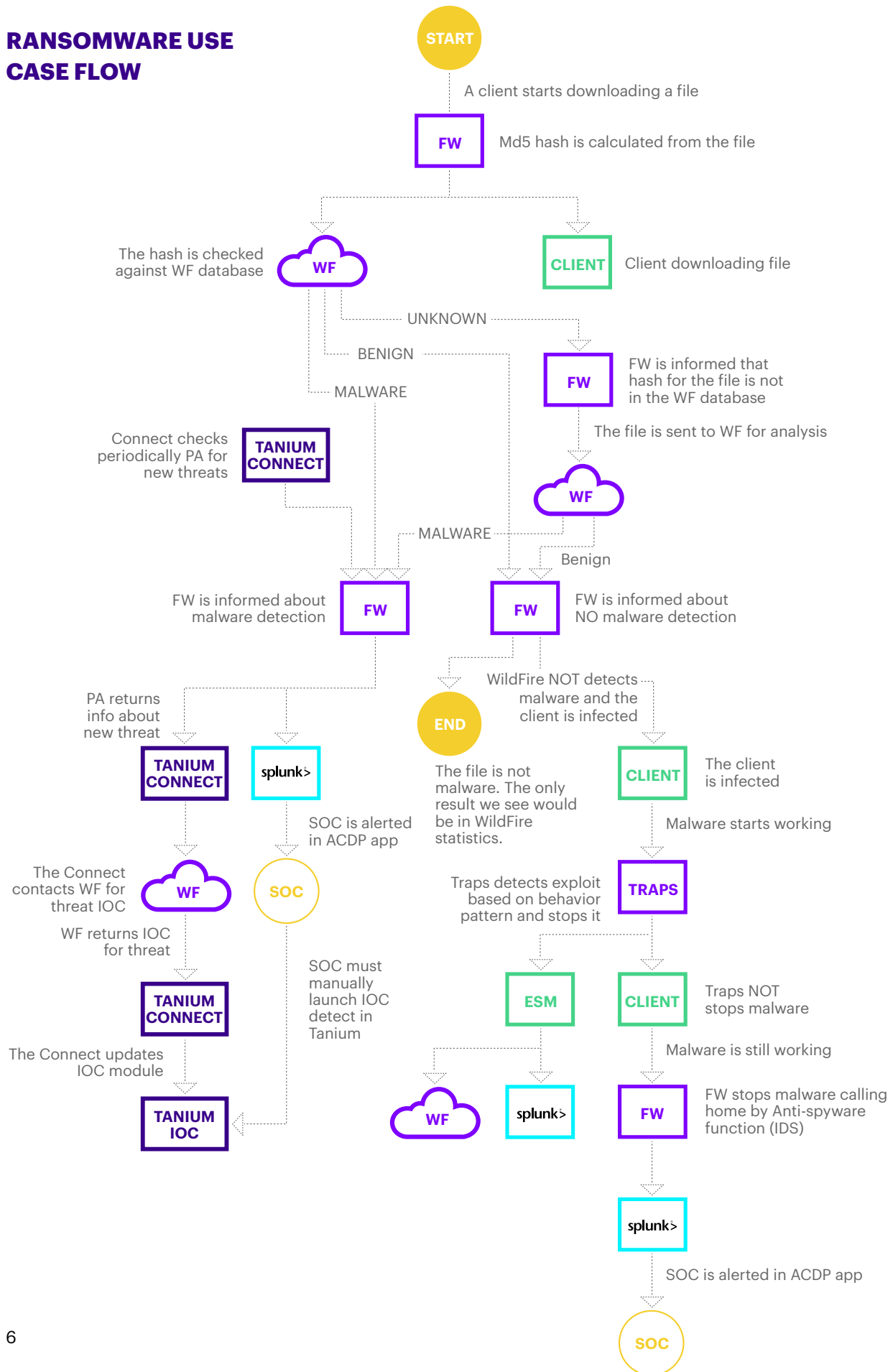
FULL AUTOMATION AVAILABLE

Organizations seeking end-to-end visibility require a new approach, based on data and analytics-driven security. Bringing together network and endpoint technologies with powerful analytics, rapid response and automation allows companies to address the full spectrum of security challenges they face.

The Accenture cyber defense solution managed service can be fully automated to detect unknown assets or malware, and then quarantine suspicious hosts on a client's firewall. Ransomware detection is automated on the Palo Alto Networks's Next Generation Firewall and on endpoints with Tanium and Palo Alto's Traps Advanced Endpoint Protection.

Splunk correlates firewall and endpoint data to automatically quarantine suspicious hosts. Any of these steps, however, can be converted to require human, manual intervention.

RANSOMWARE USE CASE FLOW



Accenture and Splunk Security Services help build cybersecurity from the inside out, managing strategy and risk, cyber defense, digital identity, application security and managed security.

For more information, contact:

JEFF CHANCEY

jeffry.t.chancey@accenture.com

JEFF PENN

jpenn@splunk.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com. Visit us at [**www.accenture.com**](http://www.accenture.com).

ABOUT SPLUNK

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable. Join hundreds of thousands of passionate users by trying Splunk solutions for free: [**http://www.splunk.com/free-trials.**](http://www.splunk.com/free-trials)

REFERENCES

1. <http://www.welivesecurity.com/2016/02/19/average-cost-cybercrime-rises-200-just-five-years/>
2. <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#421e63773bb0>