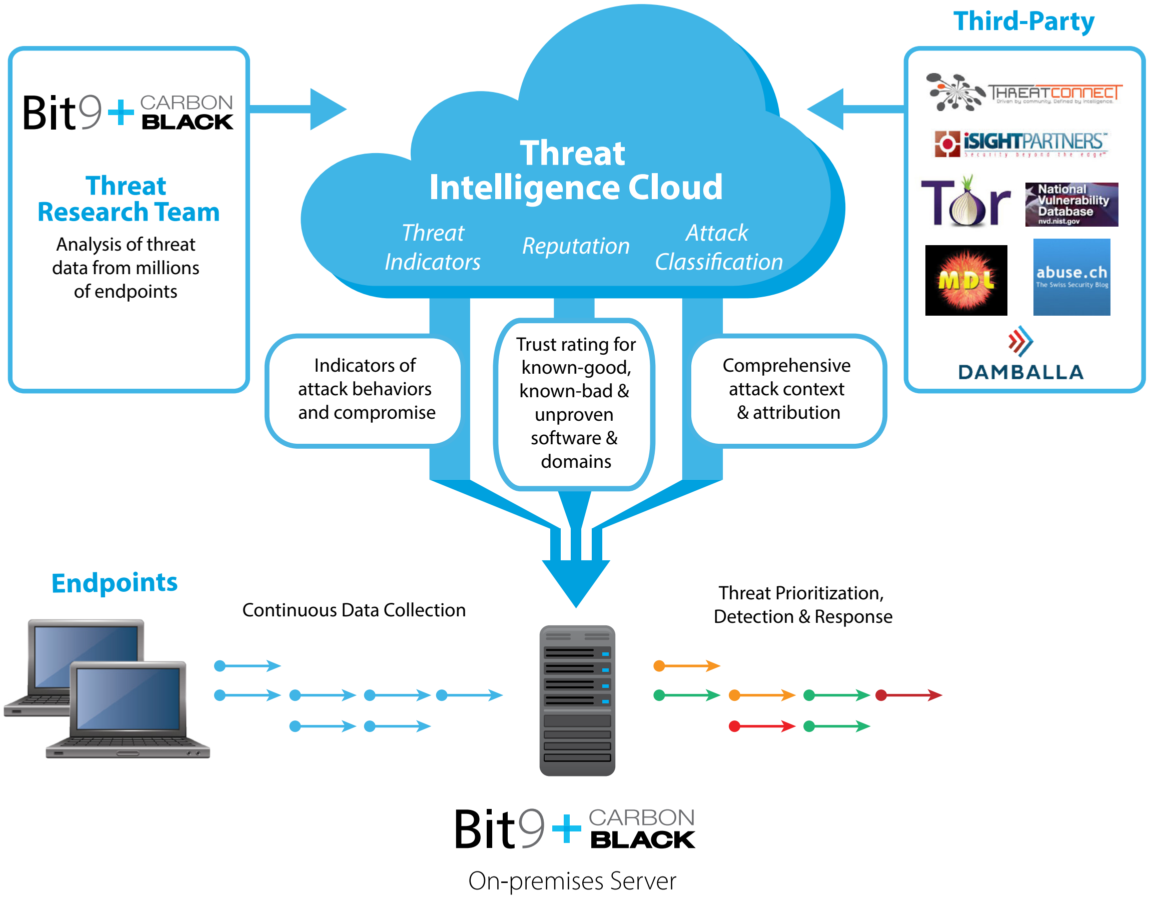
DATA SHEET

# Bit9 + Carbon Black Threat Intelligence Cloud


Bit9 + CARBON BLACK
Threat Research Team
Analysis of threat data from millions of endpoints
Threat Intelligence Cloud
Threat Indicators
Reputation
Attack Classification
Third-Party
THREATCONNECT
iSIGHTPARTNERS
Tor
National Vulnerability Database
nvd.nist.gov
MDL
abuse.ch
The Swiss Security Blog
DAMBALLA
Indicators of attack behaviors and compromise
Trust rating for known-good, known-bad & unproven software & domains
Comprehensive attack context & attribution
Endpoints
Continuous Data Collection
Threat Prioritization, Detection & Response
Bit9 + CARBON BLACK
On-premises Server

## *Single Solution for Instant, Aggregated Threat Intelligence*

**The Bit9 + Carbon Black Threat Intelligence Cloud** offers a comprehensive, aggregated advanced threat intelligence solution that combines leading software reputation, threat indicator and attack classification services to provide some of the industry's most powerful, correlated and accurate threat insight. No single vendor has a lock on the world's threat intelligence. Organizations need to combine threat intelligence from a variety of proprietary and third-party sources. Only the Threat Intelligence Cloud combines Bit9 + Carbon Black's unique threat intelligence and industry-leading third-party intelligence sources to empower security professionals to optimize and improve their prevention, detection, response and recovery capabilities.

Bit9 + Carbon Black's Threat Research Team produces threat intelligence by analyzing data from millions of endpoints, giving it unique insight into threat behaviors. This results in two cloud-delivered services: threat indicators for emerging attacks and reputation intelligence for known-good, known-bad and unproven software and domains. These two services are further complemented by the Attack Classification Service for attack context and attack attribution. The combination of this aggregated intelligence—seamlessly integrated with both the Bit9 Security Platform and Carbon Black—enables security operations and incident response professionals to define trust policies for multiple forms of advanced threat prevention, build custom detection events tailored for your business, accelerate investigations during a response, and proactively hunt for threats.

### Threat Indicator Service for detection of malicious behaviors and compromise

The Bit9 + Carbon Black Threat Research Team analyzes the data from millions of endpoints to design and publish actionable indicators of malicious attack behaviors and compromise. These threat feeds enable security teams to monitor and examine threat vectors across systems such as files executing from the recycle bin, suspicious process names or extensions, backdoor installations, ransomware, host file modifications, firewall tampering, malformed documents, suspicious attack processes, geolocation, spear-phishing attacks and more. These indicators are continuously evolving to adapt to the changing tactics of today's threat actors.

### Reputation Service for trust ratings of known-good, known-bad and unproven software and domains

The Threat Intelligence Cloud's Reputation Service delivers unmatched reputation regarding known-good, known-bad and unproven software and domains giving IT and security teams actionable intelligence about the software installed—and network connections made—within their enterprise. These trust ratings can be leveraged to define endpoint threat prevention policies, build custom detection events and prioritize investigations.

### Attack Classification Service for third-party attack context and attribution

The Threat Intelligence Cloud's Attack Classification Service provides comprehensive attack context and attribution by integrating with a robust list of industry-leading third-party sources to assist enterprises in identifying the type of malware and threat actor group behind an attack. By integrating with third-party feeds, the Threat Intelligence Cloud distributes intelligence regarding antivirus aggregation engines, malicious domain or Tor Node IP addresses, command-and-control communications, community threat intelligence and more.

## The Bit9 + Carbon Black Threat Intelligence Cloud is a critical component of both the Bit9 and Carbon Black Security Platforms

### Bit9 Security Platform

The Bit9 Security Platform is the most comprehensive endpoint threat protection solution. Bit9 continuously monitors and analyzes all endpoint activity to prevent, detect and respond to cyber threats that evade traditional security defenses.  The world's most widely deployed application control solution, Bit9 is trusted by more than 1,000 organizations worldwide.

### Carbon Black

Carbon Black is the first and only endpoint threat detection and response platform that enables SOC and IR teams to rapidly detect, respond and recover from an attack. Top IR firms and MSSPs have made Carbon Black a core component of their detection and response services.

**Threat Prevention**

**Advanced Threat Hunting**

**Customized Detection**

**Incident Response**

### ABOUT BIT9 + CARBON BLACK

Bit9 + Carbon Black provides the most complete solution against advanced threats that target organizations' endpoints and servers, making it easier to see—and immediately stop—those threats. The company enables organizations to arm their endpoints by combining continuous, real-time visibility into what's happening on every computer; real-time signature-less threat detection; incident response that combines a recorded history with live remediation; and prevention that is proactive and customizable. More than 1,000 organizations worldwide—from Fortune 100 companies to small enterprises—use Bit9 + Carbon Black to increase security, reduce operational costs and improve compliance. Leading managed security service providers (MSSP) and incident response (IR) companies have made Bit9 + Carbon Black a core component of their detection and response services.

*20150327*

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

SANS BEST OF 2014 WINNER IN End Point Protection